

Part No. 060139-10, Rev. D
March 2005

OmniSwitch® Omni Switch/Router™ User Manual

Release 4.4



www.alcatel.com

An Alcatel service agreement brings your company the assurance of 7x24 no-excuses technical support. You'll also receive regular software updates to maintain and maximize your Alcatel product's features and functionality and on-site hardware replacement through our global network of highly qualified service delivery partners. Additionally, with 24-hour-a-day access to Alcatel's Service and Support web page, you'll be able to view and update any case (open or closed) that you have reported to Alcatel's technical support, open a new case or access helpful release notes, technical bulletins, and manuals. For more information on Alcatel's Service Programs, see our web page at www.ind.alcatel.com, call us at 1-800-995-2696, or email us at support@ind.alcatel.com.

**This Manual documents Release 4.4 OmniSwitch and Omni Switch/Router hardware and software.
The functionality described in this Manual is subject to change without notice.**

Copyright © 2005 by Alcatel Internetworking, Inc. All rights reserved. This document may not be reproduced in whole or in part without the express written permission of Alcatel Internetworking, Inc.

Alcatel® and the Alcatel logo are registered trademarks of Alcatel. Xylan®, OmniSwitch®, PizzaSwitch®, OmniStack®, and Alcatel OmniVista® are registered trademarks of Alcatel Internetworking, Inc.

AutoTracker™, OmniAccess™, OmniCore™, Omni Switch/Router™, OmniVista™, PizzaPort™, PolicyView™, RouterView™, SwitchManager™, SwitchStart™, VoiceView™, WANView™, WebView™, X-Cell™, X-Vision™ and the Xylan logo are trademarks of Alcatel Internetworking, Inc.

All-In-OneSM is a service mark of Alcatel Internetworking, Inc. All other brand and product names are trademarks of their respective companies.



A L C A T E L

26801 West Agoura Road
Calabasas, CA 91301
(818) 880-3500 FAX (818) 880-3505
info@ind.alcatel.com

US Customer Support—(800) 995-2696
International Customer Support—(818) 878-4507
Internet—<http://eservice.ind.alcatel.com>

Cautions

FCC Compliance: This equipment has been tested and found to comply with the limits for Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions in this guide, may cause interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his own expense.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment. It is suggested that the user use only shielded and grounded cables to ensure compliance with FCC Rules.

This equipment does not exceed Class A limits per radio noise emissions for digital apparatus, set out in the Radio Interference Regulation of the Canadian Department of Communications.

Avis de conformité aux normes du ministère des Communications du Canada

Cet équipement ne dépasse pas les limites de Classe A d'émission de bruits radioélectriques pour les appareils numériques, telles que prescrites par le Règlement sur le brouillage radioélectrique établi par le ministère des Communications du Canada.

Lithium Batteries Caution: There is a danger of explosion if the Lithium battery in your chassis is incorrectly replaced. Replace the battery only with the same or equivalent type of battery recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions. The manufacturer's instructions are as follows:

Return the module with the Lithium battery to Alcatel. The Lithium battery will be replaced at Alcatel's factory.

Table of Contents

1	Omni Switch/Router Chassis and Power Supplies	1-1
	Omni Switch/Router User Interface (UI) Software	1-2
	Omni Switch/Router Network Management Software (NMS)	1-2
	Omni Switch/Router Distributed Switching Fabric	1-3
	Omni Switch/Router Fabric Capacity	1-4
	Omni Switch/Router Applications and Configurations	1-5
	Omni Switch/Router as the Backbone Connecting Several Networks	1-5
	Omni Switch/Router as the Central Backbone Switch/Router and in the Wiring Closet	1-6
	Omni Switch/Router Chassis and Power Supplies	1-7
	OmniS/R-3	1-8
	OmniS/R-3 Chassis Technical Specifications	1-9
	OmniS/R-5	1-10
	OmniS/R-5 Technical Specifications	1-12
	OmniS/R-9 and OmniS/R-9P	1-13
	OmniS/R-9 Technical Specifications	1-15
	OmniS/R-9P Technical Specifications	1-16
	OmniS/R-9P-48V Technical Specifications	1-17
	Omni Switch/Router Power Requirements	1-18
	Grounding a Chassis	1-25
	The Omni Switch/Router Hardware Routing Engine (HRE-X)	1-26
	Valid HRE-X Configurations	1-27
	HRE-X Router Registers versus Feature Limitations	1-27
	Connecting a DC Power Source to an OmniS/R-PS5-DC375	1-28
	Installing DC Power Source Wire Leads	1-28
	Connecting a DC Power Source to an OmniS/R-PS9-DC725	1-31
	Installation Requirements	1-31
	Installing DC Power Source Wire Leads	1-32
2	The Omni Switch/Router MPX	2-1
	Omni Switch/Router Management Processor Module (MPX) Features	2-1
	MPX Technical Specifications	2-1
	MPX Serial and Ethernet Management Ports	2-4
	Ethernet Management Port	2-5
	Configuring MPX Serial Ports	2-6
	Flash Memory and Omni Switch/Router Software	2-7
	Flash Memory Guidelines	2-8

MPX Redundancy	2-9
Change-Over Procedure	2-9
MPX Redundancy Commands	2-10
3 Omni Switch/Router Switching Modules	3-1
Required Image Files	3-3
Handling Fiber and Fiber Optic Connectors	3-5
Gigabit Ethernet Modules	3-7
GSX-FM/FS/FH-2W	3-7
GSX-FM/FS/FH-2W Technical Specifications	3-8
GSX-K-FM/FS/FH-2W	3-10
GSX-K-FM/FS/FH-2W Technical Specifications	3-11
GSX-FM/FS-4W	3-13
GSX-FM/FS-4W Technical Specifications	3-14
Auto-Sensing 10/100 Ethernet Modules	3-16
Ethernet RJ-45 Pinouts	3-16
Ethernet RJ-45 Specifications	3-16
ESX-100C-12W	3-16
ESX-100C-12W Technical Specifications	3-17
ESX-100C-32W	3-19
ESX-100C-32W Technical Specifications	3-20
ESX-K-100C-32W	3-22
ESX-K-100C-32W Technical Specifications	3-23
Fast (100 Mbps) Ethernet Modules	3-25
ESX-100FM/FS-12W	3-25
ESX-100FM/FS-12W Technical Specifications	3-26
ESX-K-100FM/FS-16W	3-28
ESX-K-100FM/FS-16W Technical Specifications	3-29
10 Mbps Ethernet Modules	3-31
ESX-FM-24W	3-31
ESX-FM-24W Technical Specifications	3-32
Token Ring Modules	3-34
Token Ring RJ-45 Pinouts	3-34
Token Ring RJ-45 Specifications	3-34
TSX-C-32W	3-35
TSX-C-32W Technical Specifications	3-35
TSX-CD-16W	3-37
TSX-CD-16W Technical Specifications	3-38
ATM Uplink Modules	3-40
ASX-155FM/FS/FH	3-42
ASX-155FM/FS/FH Technical Specifications	3-43
ASX-155RFM/RFS-1W	3-45
ASX-155RFM/RFS-1W Technical Specifications	3-46

ASX-622RFS/RFM-1W	3-48
ASX-622RFM/RFS-1W Technical Specifications	3-49
ASX-M-622RFM/RFS/RFH-1W	3-51
ASX-M-622RFM/RFS/RFH-1W Technical Specifications	3-52
ASX-DS3	3-55
ASX-DS3 Technical Specifications	3-56
ASX-E3	3-58
ASX-E3 Technical Specifications	3-59
WAN Modules	3-61
WAN Pinouts	3-61
WAN BRI Port Specifications (S/T Interface)	3-62
WAN BRI Port Specifications (U Interface)	3-62
WAN T1/E1 Port Specifications	3-63
WAN Serial Port Specifications	3-64
WSX-S-2W	3-66
WSX-S-2W Technical Specifications	3-66
WSX-SC	3-68
WSX-SC Technical Specifications	3-69
WSX-FT1/E1-SC	3-71
WSX-FT1/E1-SC Technical Specifications	3-72
WSX-FE1-SC Cabling/Jumper Settings	3-74
WSX-BRI-SC	3-75
WSX-BRI-SC Technical Specifications	3-76
4 The OmniSwitch Chassis	4-1
OmniSwitch Components	4-1
OmniSwitch Frame and Management Buses	4-1
ATM Cell Switching Matrix	4-2
OmniSwitch Chassis Types	4-2
OmniSwitch Failure-Resistant Features	4-4
Omni-3wx	4-5
Power Supply	4-5
Omni-3wx Technical Specifications	4-6
Omni-5wx	4-7
Power Supplies	4-7
Omni-5wx Technical Specifications	4-8
Omni-9wx	4-9
Power Supplies	4-10
Omni-9wx, Omni-9wx-PLUS, and Omni-9wxp Technical Specifications	4-10
Discontinued Chassis	4-11
Omni-5	4-11
Power Supplies	4-11
Omni-5 Technical Specifications	4-12

Omni-9	4-13
Power Supplies	4-13
Omni-9 Technical Specifications	4-14
Omni-5e	4-15
Power Supplies	4-15
Omni-5e Technical Specifications	4-16
Omni-9e	4-17
Power Supplies	4-17
Omni-9e Technical Specifications	4-18
Omni-5x	4-19
Power Supplies	4-19
Omni-5x Technical Specifications	4-20
Omni-9x	4-21
Power Supplies	4-21
Omni-9x Technical Specifications	4-22

5 OmniSwitch Power Supplies 5-1

Replacing Power Supplies (9-Slot Chassis)	5-2
Omni-3wx Power Supplies	5-3
Omni-3wx Power Supply Specifications	5-3
Omni-3wx Power Supply Specifications	5-4
Omni-5 Power Supplies	5-5
Omni-5 PS5 and PS5-DC-48 Specifications	5-5
Omni-5e Power Supplies	5-6
Omni-5e PS5-250 and PS5-DC250 Technical Specifications	5-6
Omni-5x Power Supplies	5-7
Omni-5x PS5-250 and PS5-DC250 Specifications	5-7
Omni-5wx Power Supplies	5-8
Omni-5wx PS5-250 and PS5-DC-250 Technical Specifications	5-8
Omni-9 Power Supply	5-9
Omni-9 PS9-350T Specifications	5-9
Omni-9e Power Supplies	5-10
Omni-9e PS9-500 and PS9-DC500 Specifications	5-10
Omni-9x Power Supplies	5-11
Omni-9wx, Omni-9wx-PLUS & Omni-9wxp Power Supplies	5-12
Omni-9wx PS9-500T Specifications	5-13
Omni-9wx PS9-500P and PS9-DC500 Specifications	5-13
Omni-9wx-PLUS PS9-650P Specifications	5-14
Omni-9wxp PS9-725 Specifications	5-14
Power Requirements	5-15
CSM-622 Modules	5-15
Omni-5, Omni-9, Omni-9e (350 watt) Chassis	5-16
Omni-5e and Omni-9e (500 watt) Chassis	5-16

FCC Class B Approvals	5-17
Removing and Installing a Power Supply	5-22
Removing a Power Supply	5-22
Installing a Power Supply	5-22
Connecting a DC Power Source	5-23
Installing DC Power Source Wire Leads	5-24
Replacing a Power Supply Fuse (older chassis models)	5-27
Grounding a Chassis	5-28
Power Cords	5-29
Backup Power System (BPS)	5-30
Operation with One Power Supply Installed in the BPS	5-30
Operation with Two Power Supplies Installed in the BPS	5-31
Front Panel	5-32
Rear Panel	5-33
Connecting a BPS to an Omni-3wx	5-34
BPS Technical Specifications	5-35
Backup Power System (BPS) Technical Specifications	5-35
BPS Power Supplies	5-36
6 The Management Processor Module (MPM)	6-1
Original MPM	6-1
MPM-II	6-1
MPM-1G	6-2
MPM-III	6-2
MPM-C	6-2
MPM Types Matrix	6-3
Serial and Ethernet Management Ports	6-7
Modem Port Jumpers	6-8
MPM-III Ethernet Management Port	6-10
Flash Memory and Switch Software	6-11
Flash Memory Guidelines	6-14
MPM Redundancy	6-15
Change-Over Procedure	6-15
MPM Redundancy Commands	6-16
Hardware Routing Engines	6-17
MPM-II and MPM-1G HRE and HRE-Plus	6-17
MPM-III HRE-VX	6-18
HRE-VX Router Registers versus Feature Limitations	6-18
7 OmniSwitch Switching Modules	7-1
Required Image Files	7-4
Installing a Switching Module	7-7
Removing a Switching Module	7-9
Hot Swapping a Switching Module	7-10

Diagnostic Tests	7-12
High-Speed Module (HSM)	7-13
Content Addressable Memory (CAM)	7-14
Module LEDs	7-16
High-Density, 10/100, and Gigabit Ethernet Modules	7-17
Ethernet Pinouts	7-17
Ethernet RJ-45 Specifications	7-17
ESM-100C-12	7-18
ESM-100C-12 Technical Specifications	7-18
ESM-100FM/FS-8	7-20
ESM-100FM/FS-8 Technical Specifications	7-20
ESM-C-16	7-22
ESM-C-16 Technical Specifications	7-22
ESM-C-32W	7-24
ESM-C-32W Technical Specifications	7-24
ESM-FM-16W	7-26
ESM-FM-16W Technical Specifications	7-26
ESM-100C-32W Ethernet Module	7-28
ESM-100C-32W Technical Specifications	7-29
ESM-T-24W	7-31
ESM-T-24W Technical Specifications	7-31
GSM-F-2W Gigabit Ethernet Module	7-33
GSM-F-2W Technical Specifications	7-34
ATM Access Modules	7-36
ATM Pinouts	7-38
ATM RJ-45 Specifications	7-38
ATM CE RJ-48C Specifications	7-38
Serial Port Specifications	7-40
ASM-155Fx (Discontinued)	7-42
ASM-155Fx Technical Specifications	7-43
ASM-155C (Discontinued)	7-45
ASM-155C Technical Specifications	7-45
ASM2-155F	7-47
ASM2-155FM/S Technical Specifications	7-48
ASM2-155RF	7-50
ASM2-155RFM/S Technical Specifications	7-51
ASM2-622F (Discontinued)	7-53
ASM2-622FM/S Technical Specifications	7-54
ASM2-622RF	7-56
ASM2-622RFM/S Technical Specifications	7-57
ASM-DS3 (Discontinued)	7-59
ASM-DS3 Technical Specifications	7-60
ASM-E3 (Discontinued)	7-62
ASM-E3 Technical Specifications	7-63
ASM-CE (Discontinued)	7-65
ASM-CE Technical Specifications	7-65

ASM2-DS3	7-68
ASM2-DS3 Technical Specifications	7-69
ASM2-E3	7-71
ASM2-E3 Technical Specifications	7-72
Token Ring Modules	7-74
Token Ring Pinouts	7-75
Token Ring RJ-45 Specifications	7-75
TSM-C-6 (Discontinued)	7-76
TSM-C-6 Technical Specifications	7-76
TSM-F-6	7-78
TSM-F-6 Technical Specifications	7-78
TSM-F-6 Port Configurations	7-80
TSM-CD-6 (Discontinued)	7-82
TSM-CD-6 Technical Specifications	7-83
TSM-CD-16W	7-85
TSM-CD-16W Technical Specifications	7-86
Original 10 Mbps Ethernet Modules	7-88
ESM-C-12 (Discontinued)	7-89
ESM-C-12 Technical Specifications	7-89
ESM-C-8 (Discontinued)	7-91
ESM-C-8 Technical Specifications	7-91
ESM-F-8	7-93
ESM-F-8 Technical Specifications	7-93
ESM-T-12 (Discontinued)	7-95
ESM-T-12 Technical Specifications	7-95
ESM-U-6	7-97
ESM-U Technical Specifications	7-98
Original Fast Ethernet (100 Mbps) Modules (Discontinued)	7-100
ESM-100C (Discontinued)	7-101
ESM-100C Technical Specifications	7-102
ESM-100C-FD (Discontinued)	7-105
ESM-100C-FD Technical Specifications	7-105
ESM-100Fx-FD (Discontinued)	7-107
ESM-100Fx-FD Technical Specifications	7-107
ESM-100C-5 (Discontinued)	7-109
ESM-100C-5 Technical Specifications	7-110
ESM-100CFx-5 (Discontinued)	7-112
ESM-100CFx-5 Technical Specifications	7-113
8 The User Interface	8-1
Overview of Command Interfaces	8-1
Changing Between the CLI and UI Modes	8-1
Exit the Command Interface	8-2

UI to CLI Command Cross Reference	8-3
Hardware Commands	8-3
Hardware Table	8-3
Basic Switch Management Commands	8-4
Basic Switch Management Table	8-4
Network Management Commands	8-5
Network Management Table	8-5
Layer II Switching Commands	8-6
Layer II Switching Table	8-6
Groups, VLANs, Policies Commands	8-7
Groups, VLANs, Policies Table	8-7
Routing Commands	8-9
Routing Table	8-9
ATM Access Commands	8-10
ATM Access Table	8-10
ATM Cell Switching (X-Cell) Commands	8-12
ATM Cell Switching (X-Cell) Table	8-12
PNNI/IISP Commands	8-13
PNNI/ISP Table	8-13
WAN Access Commands	8-14
WAN Access Table	8-14
Troubleshooting Diagnostics Commands	8-17
Troubleshooting/Diagnostics Table	8-17
User Interface Menu	8-18
Main Menu Summary	8-19
General User Interface Guidelines	8-20
Entering Command Names	8-20
Quitting a Command	8-21
Scrolling	8-21
The UI Configuration Menu	8-21
Configuring the System Prompt	8-22
Configuring More Mode for the User Interface	8-23
Setting Verbose/Terse Mode for the User Interface	8-26
Configuring the Auto Logout Time	8-28
Viewing Commands	8-29
Changing Passwords	8-29
Command History and Re-Executing Commands	8-30
Abbreviating IP Addresses	8-32
User Interface Display Options	8-34
Setting Echo/NoEcho for User Entry	8-35
Setting the Login Banner	8-35
Creating a new Banner	8-36
Permanent Banner	8-36
Banners for Different Access Methods	8-36
Login Accounts	8-37

Multiple User Sessions	8-37
Listing Other Users	8-38
Communicating with Other Users	8-39
Deleting Other Sessions	8-39
Advanced Kill Command Options	8-41
UI Table Filtering (Using Search and Filter Commands)	8-42
The Search Command	8-43
Renewing a Search	8-44
The Filter Command	8-45
Combining Search and Filter Commands	8-46
Using Wildcards with Search and Filter Commands	8-48
Wildcard Command Options	8-48
9 Installing Switch Software	9-1
Using FTP Server	9-2
Using FTP Client	9-3
Using ZMODEM	9-4
Using ZMODEM with the load Command	9-4
Using ZMODEM With the Boot Line Prompt	9-5
10 Configuring Management Processor Modules	10-1
Changing Serial Port Communication Parameters	10-2
Changing Port Speed When Communication With The Switch Lost	10-3
Configuring the Modem Port	10-3
Modem Port Mode	10-3
Configuring SLIP	10-4
Configuring the Ethernet Management Port	10-5
Ethernet Management Ports and Redundant Management Processor Modules	10-7
The MPM Command/Menu	10-9
Displaying MPM Redundancy	10-9
MPM Menu Commands	10-9
Using MPM Commands with Software Release 3.2 and Later	10-10
Listing the Secondary MPM Files	10-11
Transferring a File to the Secondary MPM	10-11
Replacing a File on the Secondary MPM	10-12
Loading a File from the Secondary MPM	10-12
Removing a File from the Secondary MPM	10-13
Giving Up Control to the Secondary MPM	10-14
Setting the Load Suffix	10-14
Setting Automatic Config Synchronization	10-15
Enabling Automatic Config Synchronization	10-15
Disabling Automatic Config Synchronization	10-15

Synchronizing Configuration Data	10-16
Synchronizing Image Files	10-16
Loading a File From the Primary MPM	10-17
Gaining Control from the Primary MPM	10-18
Resetting a Secondary MPM	10-19
Displaying and Setting the Swap State	10-20
Displaying the Swap State	10-20
Enabling the Swap Mode	10-20
Disabling the Swap Mode	10-21
11 Managing Files	11-1
File Menu	11-1
Displaying the Current Directory	11-2
Command and Image File Placement	11-2
Configuration and Log File Generation	11-2
Changing Directories	11-2
Listing Switch Files	11-3
Deleting Switch Files	11-4
Deleting Multiple Files	11-4
Deleting All Image Files	11-5
Copying System Files	11-6
Displaying Text Files	11-6
Editing Text Files	11-7
Clearing the Text Buffer	11-7
Loading an ASCII File into the Text Buffer	11-8
Listing the Contents of the Text Buffer	11-8
Adding Lines of Text to the Text Buffer	11-8
Deleting a Line of Text from the Text Buffer	11-9
Inserting a Line of Text into the Text Buffer	11-9
Editing a Line Name of Text in the Text Buffer	11-9
Creating a File Name for the Text Buffer	11-10
Creating a Text File from the Text Buffer	11-10
Real-World Examples	11-11
Real-World Example 1	11-11
Real-World Example 2	11-12
System Menu	11-13
Checking the Flash File System	11-14
Creating a New File System	11-15
12 Switch Security	12-1
Changing Passwords	12-2
Rebooting the Switch	12-3

Secure Switch Access	12-4
Configuring the Secure Switch Access Filter Database	12-4
Configuring Secure Access Filter Points	12-7
Enabling/Disabling Security Parameters	12-9
Adding Filters	12-9
Deleting Filters	12-9
Viewing Secure Access Violations Log	12-10
Managing User Login Accounts	12-11
Partition Management Requirements	12-11
Default Accounts	12-12
Adding a User Account Using the UI Command Mode	12-12
Adding a User Account Using the CLI Command Mode	12-13
Assigning Account Privileges Using the CLI Command Mode	12-13
Assigning Account Privileges Using the UI Command Mode	12-16
Command Family Table	12-18
Global Family Table	12-19
Modifying a User Account	12-20
Deleting a User	12-20
13 Configuring Switch-Wide Parameters	13-1
Summary Menu	13-1
Displaying the MIB-II System Group Variables	13-2
Displaying the Chassis Summary	13-3
Displaying Current Router Interface Status	13-4
System Menu	13-5
Displaying Basic System Information	13-6
Setting the System Date and Time	13-8
Viewing Slot Data	13-14
Viewing System Statistics	13-15
Clearing System Statistics	13-16
Viewing Task Utilization Statistics	13-17
Viewing Memory Utilization	13-19
Viewing MPM Memory Statistics	13-20
Checking the Flash File System	13-21
Checking the SIMM Files	13-21
Creating a New File System	13-22
Creating a SIMM File System	13-22
Configuring System Information	13-23
Viewing CAM Information	13-24
Configuring CAM Distribution	13-25
OmniSwitch CAM Distribution	13-25
Omni Switch/Router CAM Distribution	13-26

Configuring the HRE-X/HRE-VX Router Port	13-27
Configuring and Displaying the HRE-X/HRE-VX Hash Table	13-29
Duplicate MAC Address Support	13-30
Multicast Claiming	13-32
Disabling Flood Limits	13-32
Saving Configurations	13-33
14 Switch Logging	14-1
Logging Overview	14-1
Configuring the Syslog Parameters	14-2
Configuring Switch Logging	14-6
Displaying the Command History Entries in the MPM Log	14-9
Displaying the Connection Entries in the MPM Log	14-10
Displaying Screen (Console) Capture Entries in the MPM Log	14-11
Displaying Debug Entries in the MPM Log	14-13
Displaying Secure Access Entries in the MPM Log	14-13
15 Health Statistics	15-1
The Health Statistics Management Menu	15-1
Setting Resource Thresholds	15-2
Setting Bandwidth Thresholds	15-3
Setting Miscellaneous Thresholds	15-4
Setting the Sampling Interval	15-6
View Switch-Level Statistics	15-6
View Module-Level Statistics	15-7
View Port-Level Statistics	15-8
Reset Health Statistics	15-8
16 Network Time Protocol	16-1
Introduction	16-1
Stratum	16-2
Using NTP in a Network	16-2
NTP and Authentication	16-4
Network Time Protocol Management Menu	16-5
NTP Configuration Menu	16-6
Configuring an NTP Client	16-6
Field Descriptions	16-7
Configuring an NTP Client/Server	16-8
Field Descriptions	16-9
Configuring Client/Server Authentication	16-9
Field Descriptions	16-11
Configuring a New Peer Association	16-12

Configuring a New Server	16-13
Configuring a Broadcast Time Service	16-13
Unconfigure Existing Peer Associations	16-14
Set the Server's Advertised Precision	16-14
NTP Information Menu	16-15
Display List of Peers the Server Knows About	16-15
Display Peer Summary Information	16-16
Field Descriptions	16-17
Display Alternate Peer Summary Information	16-17
Display Detailed Information for One or More Peers	16-18
Field Descriptions	16-18
Print Version Number	16-20
Display Local Server Information	16-21
Field Descriptions	16-21
NTP Statistics Menu	16-23
Display Local Server Statistics	16-23
Field Descriptions	16-24
Display Server Statistics Associated with Particular Peer(s)	16-24
Field Descriptions	16-25
Display Loop Filter Information	16-26
Field Descriptions	16-26
Display Peer Memory Usage Statistics	16-26
Field Descriptions	16-26
Display I/O Subsystem Statistics	16-27
Field Descriptions	16-27
Display Event Timer Subsystem Statistics	16-28
Field Descriptions	16-28
Reset Various Subsystem Statistics Counters	16-28
Reset Stat Counters Associated With Particular Peer(s)	16-28
Display Packet Count Statistics from the Control Module	16-29
Field Descriptions	16-29
Display the Current Leap Second State	16-30
Field Descriptions	16-30
Turn the Server's Monitoring Facility On or Off	16-31
Display Data The Server's Monitor Routines Have Collected	16-31
Field Descriptions	16-32
NTP Administration Menu	16-33
Set the Primary Receive Timeout	16-33
Set the Delay Added to Encryption Time Stamps	16-33
Specify the Host Whose NTP Server We Talk To	16-34
Specify a Password to Use for Authenticated Requests	16-34
Set Key ID to Use for Authenticated Requests	16-34
Set Key Type to Use for Authenticated Requests (DES MD5)	16-35
Set a System Flag (Auth, Bclient, Monitor, Stats)	16-35
Clear a System Flag (Auth, Bclient, Monitor, Stats)	16-35

NTP Access Control Menu	16-36
Change the Request Message Authentication Key ID	16-36
Change the Control Message Authentication Key ID	16-37
Add One or More Key ID's to the Trusted List	16-37
Display the Trusted Key ID List	16-37
Remove One or More Key ID's from the Trusted List	16-38
Display the State of the Authentication Code	16-38
Field Descriptions	16-38
Create Restrict Entry/Add Flags to Entry	16-39
View the Server's Restrict List	16-40
Field Descriptions	16-40
Remove Flags from a Restrict Entry	16-41
Delete a Restrict Entry	16-41
Configure a Trap in the Server	16-41
Display the Traps Set in the Server	16-42
Field Descriptions	16-42
Remove a Trap (Configured or Otherwise) from the Server	16-42
17 SNMP (Simple Network Management Protocol)	17-1
Introduction	17-1
Configuring SNMP Parameters and Traps	17-2
Configuring a New Network Management Station	17-4
Viewing SNMP Statistics	17-8
Trap Tables	17-11
SNMP Standard Traps	17-15
Extended Traps	17-27
18 DNS Resolver and RMON	18-1
Introduction	18-1
Configuring the DNS Resolver	18-1
The Names Submenu	18-1
Remote Network Monitoring (RMON)	18-3
Probes and Events	18-3
Ethernet Probes	18-3
History Probes	18-3
Alarm Probes	18-3
Monitoring Probes	18-4
Monitoring Events	18-5
Configuring Router Port MAC Addresses	18-6
Restoring Router Port Mac Addresses	18-6

19	Managing Ethernet Modules	19-1
	Overview of OmniSwitch and Omni Switch/Router Ethernet Modules	19-1
	Early Generation OmniSwitch Ethernet Modules	19-3
	High-Density, 10/100, and Gigabit Ethernet (Mammoth) Modules	19-4
	Kodiak Ethernet Modules	19-5
	The Ethernet Management Menus	19-6
	Configuring 10/100 Auto-Sensing Ports (High-Density 10/100 Modules)	19-7
	Connecting High-Density 10/100 Modules to Non-Auto-Negotiating Links	19-8
	Configuring High-Density Ethernet Ports (10 Mbps and Fast Ethernet Modules)	19-9
	High-Density Modules With 10 Mbps Ports	19-9
	Viewing Configurations for High-Density and 10/100 Ethernet Modules	19-10
	OmniChannel	19-11
	The Server Channel Feature	19-12
	Server Channel Limitations	19-13
	Creating an OmniChannel	19-13
	Adding Ports to an OmniChannel	19-15
	Deleting an OmniChannel	19-15
	Deleting Ports from an OmniChannel	19-16
	Viewing OmniChannel Parameters	19-16
	Configuring Older Fast Ethernet Ports	19-18
	Viewing Fast Ethernet Configurations	19-19
	Selecting the Aggressive Ethernet Back-Off Algorithm	19-20
20	Managing 802.1Q Groups	20-1
	IEEE 802.1Q Sections Not Implemented	20-2
	Application Example	20-3
	X802.1Q vs. IEEE 802.1Q	20-4
	Single vs. Multiple Spanning Tree	20-4
	Giga I and II ASIC Modules	20-7
	Assigning an 802.1Q Group to a Port	20-8
	Configuring 802.1Q on 10/100 Ethernet Ports	20-9
	Configuring 802.1Q on Gigabit Ethernet Ports	20-12
	Modifying 802.1Q Groups	20-14
	Modifying 802.1Q Groups for 10/100 Ports	20-14
	Modifying 802.1Q Groups for Gigabit Ethernet Ports	20-16
	Viewing 802.1Q/X802.1Q Groups in a Port	20-18
	Viewing 802.1Q Statistics for 10/100 Ports	20-19
	Deleting 802.1Q/X802.1Q Groups from a Port	20-20

21	Managing Token Ring Modules	21-1
	Bigfoot and Early-Generation Token Ring Modules	21-2
	Early-Generation Modules	21-2
	Bigfoot Modules	21-3
	Source Routing	21-4
	Hop Counts	21-4
	Virtual Rings	21-6
	Local Virtual Rings	21-6
	Spanning Tree Leaf Rings	21-7
	Setting Up Virtual Rings	21-7
	Source Route Traffic Across a Backbone	21-8
	Virtual Rings Using Trunks	21-10
	Token Ring Copy Bit Stamping	21-11
	Source Routing to Transparent Bridging (SRTB)	21-12
	Token Ring UI Commands	21-13
	Token Ring Submenu	21-13
	Bridging Submenu	21-14
	Configuring Source Routing/Virtual Rings	21-15
	Source Routing/Virtual Ring Parameters	21-15
	Source Routing/Virtual Ring Configuration Steps	21-16
	Displaying Source Routing Parameters	21-18
	Configuring the Interface Type on Early-Generation Modules	21-21
	Configuring the Interface Type on a TSM-F-6	21-21
	Configuring the Interface Type on a TSM-CD-6	21-23
	Configuring Port Parameters for Early-Generation Token Ring Modules	21-24
	Configuring Auto-Sensing Ports for Bigfoot Modules	21-25
	Manually Configuring Token Ring Ports on Bigfoot Modules	21-27
	Configuring the Locally-Administered Token Ring Base MAC Address for Bigfoot Modules	21-29
	Disabling the Locally-Administered Token Ring Base MAC Address for Bigfoot Modules	21-30
	Enabling or Disabling Token Ring Switching	21-31
	Configuring Token Ring Port Switching	21-33
	Mapping Token Ring Ports	21-35
	Mapping a Token Ring Port to Another Token Ring Port	21-36
	Mapping a Token Ring Port to an ATM PTOP PVC Service	21-36
	Viewing Mapped Ports Configured Within the System	21-37
	Deleting Mapped Ports	21-38
	Displaying the Status Table for Token Ring Modules	21-39
	Displaying the Token Ring Interface Type	21-41

Displaying Token Ring Base MAC Addresses	21-42
Displaying Base MAC Addresses for Bigfoot Modules	21-42
Displaying the Base MAC Address for Early-Generation Modules	21-43
Displaying Token Ring Port Status	21-44
Displaying Token Ring Port Error Statistics	21-46
22 Configuring Bridging Parameters	22-1
Configuration Overview	22-3
Bridge Management Menu	22-4
Selecting a Default Group	22-7
Using the + or - to Change Groups	22-7
Bridging Commands	22-8
Displaying Bridge Forwarding Table	22-8
Field Descriptions	22-9
Configuring a Static Bridge Address	22-10
Field Descriptions	22-11
Modifying a Static Bridge Address	22-11
Deleting a Static Bridge Address	22-12
Displaying Static Bridge Addresses	22-13
Displaying Bridge Port Statistics	22-14
Field descriptions	22-15
Displaying Media Access Control (MAC) Information for a Specific MAC address	22-16
Field Descriptions	22-16
Displaying Media Access Control (MAC) Information for all MAC addresses	22-17
Display Statistics of Bridge MAC Addresses	22-17
Field Descriptions	22-18
Clear Statistics of Bridge MAC Addresses	22-18
Display Remote Trunking Stations	22-18
Field Descriptions	22-19
View the Domain Bridge Mapping Table	22-19
Field Descriptions	22-20
Setting Flood Limits	22-21
Setting Flood Limits for a Group	22-21
Displaying Group Flood Limits	22-22
Configuring Spanning Tree	22-23
Configuring Spanning Tree Parameters	22-25
Display Spanning Tree Bridge Parameters	22-28
Field Descriptions	22-28
Configuring Spanning Tree Port Parameters	22-30
Field Descriptions	22-31
Displaying Spanning Tree Port Parameters	22-32
Field Descriptions	22-33

Configuring Fast Spanning Tree	22-34
Truncating Tree Timing & Speedy Tree Protocol	22-35
Truncating Tree Timing	22-35
Speedy Tree Protocol	22-35
Configuring Truncating Tree Timing & Speedy Tree Protocol	22-35
Displaying Fast Spanning Tree Port Parameters	22-36
Enabling Fast Spanning Tree Port Parameters	22-38
Disabling Fast Spanning Tree Port Parameters	22-39
Configuring Source Routing	22-40
SAP Filtering	22-40
Enabling SAP Filtering	22-40
Disabling SAP filtering	22-41
Configuring SAP Filtering	22-41
Viewing SAP Filtering	22-42
Configuring Source Route to Transparent Bridging	22-43
Enabling SRTB for a Group	22-44
Disabling SRTB for a Group	22-45
Viewing the RIF Table	22-46
Field Descriptions	22-46
Clearing the RIF Table	22-47
23 Configuring Frame Translations	23-1
Any-to-Any Switching	23-1
Translating the Frame	23-2
The MAC Header	23-3
Canonical versus Non-Canonical	23-3
Abbreviated Addresses	23-3
Functional Addresses and Multicasts	23-3
The RIF Field	23-4
Source Route Termination by Proxy Not Supported	23-4
Encapsulation	23-5
Protocols other than IP and IPX	23-5
The SNAP Conversion	23-6
Other Conversions	23-6
Summary of Non-IPX Encapsulation Transformation Rules	23-6
IPX Encapsulation Transformation Rules	23-7
The Network Header	23-8
Address Mapping	23-8
Address Mapping in IP: ARP	23-8
Address Mapping in IPX	23-9
Frame Size Requirements	23-10
Insertion of Frame Padding	23-10
Stripping of Padding for all IEEE 802.3 Frames.	23-10
No stripping of non-IPX Ethertype Frames	23-10
IPX Specific Stripping	23-10

MTU Handling	23-11
IP Fragmentation	23-11
ICMP Based MTU Discovery	23-11
IPX Packet Size Negotiation	23-11
Other Protocols	23-11
Banyan Vines	23-12
Configuring Encapsulation Options	23-13
Forwarding versus Flooding	23-13
Port Based Translation Options	23-13
MAC Address Based Translation Options	23-13
“Native” versus “Non-Native” on Ethernet	23-14
“Native” versus “Non-Native” on FDDI and Token Ring	23-14
No Translation on Trunk or PTOP ports	23-14
The Proprietary Token Ring IPX Option	23-14
The User Interface	23-15
The addvp, modvp and crgp Commands	23-16
The Default Translation Option	23-16
Ethernet Factory Default Translations	23-17
FDDI Factory Default Translations	23-17
Token Ring Factory Default Translations	23-18
ATM LANE Factory Default Translations	23-18
The Ethertype Option	23-19
The SNAP Option	23-20
The LLC Option	23-22
Interaction with the new interface	23-23
The “vi” Command	23-23
The Switch Menu	23-24
Proprietary IPX Token Ring	23-24
Factory Defaults	23-24
Default Ethernet Translations	23-25
Default FDDI Translations	23-26
Default Token Ring Translations	23-27
Port Translations	23-29
Configuring Additional Ports	23-30
Displaying Ethernet Switch Statistics	23-30
Displaying Token Ring Switch Statistics	23-34
Any to Any MAC Translations	23-38
Default Autoencapsulation	23-39
Translational Bridging	23-40
Learning	23-40
Translations across Trunks	23-40
Dissimilar LAN Switching Capabilities	23-41
Switching Between Similar LANs	23-41
Switching Between Ethernet LANs Across a Trunked Backbone	23-42
Switching Between Similar LANs across a Native Backbone	23-43

24 Managing Groups and Ports	24-1
How Ports Are Assigned to Groups	24-2
Static Port Assignment	24-2
Dynamic Port Assignment (Group Mobility)	24-2
How Dynamic Port Assignment Works	24-3
Mobile Groups	24-5
Configuring Mobile Groups	24-5
Turning Group Mobility On or Off	24-6
Understanding Port Membership in Mobile Groups	24-7
How a Device Is Dropped from the Default Mobile Group (def_group) ..	24-9
How a Port's Primary Mobile Group Changes (move_from_def)	24-10
How a Port Ages Out of a Mobile Group (move_to_def)	24-11
Configuring Switch-Wide Group Mobility Variables	24-12
Viewing Ports in a Mobile Group	24-14
Viewing a Port's Mobile Group Affiliations	24-14
Dynamic LANE Services	24-15
Dynamic LANE Services and Non-Dynamic LANE Services	24-15
Creating Auto-Activated LANE Services	24-16
Deleting an Auto-Activated Service	24-16
Viewing Auto-Activated Services	24-17
Non-Mobile Groups and AutoTracker VLANs	24-18
Routing in a Non-Mobile Group	24-18
Spanning Tree and Non-Mobile Groups	24-19
Group and Port Software Commands	24-20
Creating a New Group	24-21
Step 1. Entering Basic Group Information	24-22
Step 2. Configuring the Virtual Router Port (Optional)	24-24
Step 3. Set Up Group Mobility and User Authentication	24-30
Step 4. Configuring Virtual Ports	24-31
Step 5. Configure Auto-Activated LANE Ports (Mobile Groups Only)	24-37
Step 6. Configuring AutoTracker Policies (Mobile Groups Only)	24-38
Creating a WAN Routing Group	24-39
Creating an ATM CIP Group	24-42
Creating a 1483 Group	24-44
Viewing Current Groups	24-46
Modifying a Group or VLAN	24-48
Viewing Your Changes	24-49
Saving Your Changes	24-49
Canceling Your Changes	24-49
Changing the IP Address	24-49
Changing the IP Subnet Mask	24-49
Enabling IP or IPX Routing	24-50
Deleting a Group	24-51

Adding Virtual Ports	24-52
Modifying a Virtual Port	24-53
Deleting a Virtual Port	24-54
Viewing Information on Ports in a Group	24-55
Viewing Detailed Information on Ports	24-58
Viewing Port Statistics	24-61
Viewing Port Errors	24-63
Port Mirroring	24-65
How Port Mirroring Works	24-65
What Happens to the Mirroring Port	24-65
Using Port Mirroring With External RMON Probes	24-66
Setting Up Port Mirroring	24-68
Disabling Port Mirroring	24-68
Port Monitoring	24-69
Port Monitoring Menu	24-69
RAM Disk System for Data Capture Files	24-70
Configuring RAM Drive Resources (pmcfg)	24-70
Changing the Default System Directory (cd)	24-70
Starting a Port Monitoring Session (pmon)	24-71
If You Chose Dump to Screen	24-72
If You Did Not Choose Dump to Screen	24-72
Ending a Port Monitoring Session	24-73
Viewing Port Monitoring Statistics (pmstat)	24-73
Port Mapping	24-74
Groups/VLANs and Port Mapping	24-74
The Details of Port Mapping	24-75
Who Can Talk to Whom?	24-76
Port Mapping Limitations	24-76
Creating a Port Mapping Set	24-77
Adding Ports to a Port Mapping Set	24-78
Removing Ports from a Port Mapping Set	24-79
Viewing a Port Mapping Set	24-80
Deleting a Port Mapping Set	24-80
Priority VLANs	24-81
Mammoth vs. Kodiak Priority VLANs	24-81
Configuring VLAN Priority	24-82
Viewing VLAN Priority	24-82
25 Configuring Group and VLAN Policies	25-1
AutoTracker Policy Types	25-2
Defining and Configuring AutoTracker Policies	25-4
Where These Procedures Start	25-4
Defining a Port Policy	25-5

Defining a MAC Address Policy	25-6
Defining a MAC Address Range Policy	25-7
Defining a Protocol Policy	25-8
Defining a Network Address Policy	25-11
Defining Your Own Rules	25-13
Defining a Port Binding Policy	25-15
Defining a DHCP Port Policy	25-20
Defining a DHCP MAC Address Policy	25-21
Defining a DHCP MAC Address Range Policy	25-22
Viewing Mobile Groups and AutoTracker VLANs	25-23
Viewing Policy Configurations	25-24
Viewing Virtual Ports' Group/VLAN Membership	25-25
View VLAN Membership of MAC Devices	25-26
Application Example: DHCP Policies	25-27
The VLANs	25-27
DHCP Servers and Clients	25-28
DHCP Port and MAC Rules	25-29
26 Interswitch Protocols	26-1
Interswitch Protocol Commands	26-1
XMAP	26-2
XMAP Transmission States	26-3
Discovery Transmission State	26-3
Common Transmission State	26-4
Passive Reception State	26-4
Common Transmission and Remote Switches	26-4
Configuring XMAP	26-5
Enabling or Disabling XMAP	26-5
Viewing a List of Adjacent Switches	26-5
Configuring the Discovery Transmission Time	26-6
Configuring the Common Transmission Time	26-7
VLAN Advertisement Protocol (VAP)	26-8
VAP and Port Policies	26-9
Configuring VAP	26-9
GMAP	26-10
GMAP Updating Rules	26-10
Configuring GMAP	26-11
Enabling and Disabling GMAP	26-11
Configuring the Gap Time	26-11
Configuring the Interpacket Update Time	26-12
Configuring the Hold Time	26-12
Displaying GMAP Statistics by MAC Address	26-13

27	Managing AutoTracker VLANs	27-1
	The AutoTracker Menu	27-2
	AutoTracker VLANs	27-3
	AutoTracker VLAN Policies	27-3
	The Default VLAN	27-4
	How Devices are Assigned to AutoTracker VLANs	27-5
	The defvl Command	27-5
	Devices that Generate a Secondary Traffic Type	27-6
	Router Traffic in IP and IPX Network Address VLANs	27-7
	Port Policy Functionality	27-9
	Frame Flooding in AutoTracker VLANs	27-15
	Routing Between AutoTracker VLANs	27-15
	Creating AutoTracker VLANs	27-16
	Step A. Entering Basic VLAN Information	27-16
	Step B. Defining and Configuring VLAN Policies	27-18
	Step C. Configuring the Virtual Router Port (Optional)	27-19
	Modifying an AutoTracker VLAN	27-24
	Deleting an AutoTracker VLAN	27-26
	Viewing AutoTracker VLANs	27-27
	Viewing Policy Configurations	27-28
	Viewing Virtual Ports' VLAN Membership	27-29
	View VLAN Membership of MAC Devices	27-30
	Creating a VLAN for Banyan Vines Traffic	27-31
28	Multicast VLANs	28-1
	How Devices are Assigned to Multicast VLANs	28-2
	Multicast VLANs and Multicast Claiming	28-2
	Frame Flooding in Multicast VLANs	28-3
	Creating Multicast VLANs	28-4
	Step A. Entering Basic Information	28-5
	Step B. Defining the Multicast Address	28-6
	Step C. Defining the Recipients of Multicast Traffic	28-7
	Defining Recipients By Port	28-7
	Defining Recipients By MAC Address	28-8
	Modifying Multicast VLANs	28-9
	Deleting a Multicast VLAN	28-11
	Modifying a Multicast Address Policy	28-12
	Viewing Multicast VLANs	28-13
	Viewing Multicast VLAN Policies	28-14
	Viewing the Virtual Interface of Multicast VLANs	28-15

29	AutoTracker VLAN Application Examples	29-1
	Application Example 1	29-2
	VLANs Based on Logical Policies	29-2
	Application Example 2	29-4
	VLANs in IPX Networks	29-4
	IPX VLAN Assignment at Bootup	29-5
	Application Example 3	29-7
	IPX Network Address VLANs and Translated Frames	29-7
	Application Example 4	29-8
	Routing in IPX Networks	29-8
	Application Example 5	29-10
	Traversing a Backbone	29-10
30	IP Routing	30-1
	Introduction	30-1
	IP Routing Overview	30-2
	Routing Protocols	30-2
	Transport Protocols	30-3
	Application-Layer Protocols	30-3
	Additional IP Protocols	30-3
	Setting Up IP Routing on the Switch	30-4
	The Networking Menu	30-6
	The IP Submenu	30-7
	Viewing the Address Translation (ARP) Table	30-8
	Displaying All Entries in the ARP Table	30-8
	Adding Entries to the ARP Table	30-9
	Deleting Entries from the ARP Table	30-10
	Flushing Temporary Entries from the ARP Table	30-10
	Finding a Specific IP Address in the ARP Table	30-10
	Finding a Specific MAC Address in the ARP Table	30-11
	Viewing IP Statistics and Errors	30-12
	Viewing the IP Forwarding Table	30-15
	Adding an IP Static Route	30-17
	Removing an IP Static Route	30-19
	Viewing ICMP Statistics and Errors	30-20
	Using the PING Command	30-22
	Viewing UDP Statistics and Errors	30-24
	Viewing the UDP Listener Table	30-25
	Viewing RIP Statistics and Errors	30-26
	Viewing TCP Statistics	30-27

Viewing the TCP Connection Table	30-29
Using the TELNET Command	30-30
Cancelling a Telnet request	30-30
Tracing an IP Route	30-31
Flushing the RIP Routing Tables	30-32
Configuring IP RIP Filters	30-33
Adding a “Global” IP RIP Filter	30-33
Adding an IP RIP Filter For a Specific Group or VLAN	30-34
IP RIP Filter Precedence	30-35
Deleting IP RIP Filters	30-36
Displaying IP RIP Filters	30-37
Displaying a List of All IP RIP Filters	30-37
Displaying a List of “Global” IP RIP Filters	30-38
Displaying a List of Specific IP RIP Filters	30-38
Viewing the IP-to-MAC Address Table	30-39
Displaying All Entries in the IP-to-MAC Table	30-39
Displaying Information for a Specific IP Address	30-40
Flushing Entries from the Table	30-40
Enabling/Disabling Directed Broadcasts	30-41
Path MTU Discovery	30-42
31 UDP Forwarding	31-1
UDP Relay and RIF Stripping	31-1
UDP Relay Hardware/Software Support	31-2
UDP Relay Configuration Screen	31-3
BOOTP/DHCP Relay	31-4
Overview of DHCP	31-4
DHCP and the OmniSwitch or OmniS/R	31-4
BOOTP/DHCP Relay and Source Routing	31-5
BOOTP/DHCP Relay and Authentication	31-5
External BOOTP Relay	31-6
Internal BOOTP/DHCP Relay	31-7
Example 1	31-7
Example 2	31-8
Enabling BOOTP/DHCP Relay	31-9
Configuring BOOTP/DHCP Relay Parameters	31-10
NetBIOS Relays	31-11
Overview of NetBIOS	31-11
NetBIOS Relay Application	31-12
Configuring NBNS Relay	31-13
Next-Hop Addresses for NBNS	31-14
Forwarding VLANs for NBNS Relay	31-15

Configuring NBDD Relay	31-16
Next-Hop Addresses for NBDD	31-17
Forwarding VLANs for NBDD Relay	31-18
Generic Service UDP Relay	31-19
Generic Services Menu	31-19
Adding a Generic Service	31-19
Modifying a Generic Service	31-21
Deleting a Generic Service	31-22
Viewing UDP Relay Statistics	31-23
32 IPX Routing	32-1
Introduction	32-1
IPX Routing Overview	32-2
IPX Protocols	32-2
Setting Up IPX Routing on the Switch	32-3
The IPX Submenu	32-4
Viewing the IPX Routing Table	32-5
Displaying All Entries in the IPX Routing Table	32-5
Using IPXR with Frame Relay or ISDN Boards	32-6
Displaying a List of Specific IPX Routes	32-7
Viewing IPX Statistics	32-8
Viewing the IPX SAP Bindery	32-10
Using IPXSAP with Frame Relay or ISDN Boards	32-11
Displaying a List of Specific SAP Servers	32-11
Adding an IPX Static Route	32-12
Removing an IPX Static Route	32-13
Turning the IPX Router Complex On and Off	32-14
Flushing the IPX RIP/SAP Tables	32-15
Using the IXPING Command	32-16
Configuring IPX RIP/SAP Filtering	32-18
Adding a “Global” IPX RIP/SAP Filter	32-19
Adding an IPX RIP/SAP Filter for a Specific Group or VLAN	32-20
Deleting an IPX RIP/SAP Filter	32-22
Displaying IPX RIP/SAP Filters	32-23
Displaying a List of All IPX Filters	32-23
Displaying a List of “Global” IPX Filters	32-24
Displaying a List of Specific IPX Filters	32-24
IPX RIP/SAP Filter Precedence	32-25
Configuring IPX Serialization Packet Filtering	32-26
Enabling IPX Serialization Filtering	32-26
Disabling IPX Serialization Filtering	32-27

Configuring IPX Watchdog Spoofing	32-28
Enabling IPX Watchdog Spoofing	32-28
Disabling IPX Watchdog Spoofing	32-29
Configuring SPX Keepalive Spoofing	32-30
Enabling SPX Keepalive Spoofing	32-30
Disabling SPX Keepalive Spoofing	32-31
Controlling IPX Type 20 Packet Forwarding	32-32
Configuring NetWare to Minimize WAN Connections	32-33
Configuring RIP and SAP Timers	32-35
Adding a RIP and SAP Timer	32-35
Viewing RIP and SAP Timers	32-36
Configuring Extended RIP and SAP Packets	32-37
Enabling or Disabling Extended RIP and SAP Packets	32-37
Viewing the Current Status of Extended Packets	32-37
Configuring an IPX Default Route	32-38
Adding an IPX Default Route	32-38
Viewing the Status of an IPX Default Route	32-38
Disabling an IPX Default Route	32-38
33 Managing ATM Access Modules	33-1
Early Generation OmniSwitch ATM Access Modules	33-2
SAHI-Based ATM Access Modules	33-3
Omni Switch/Router Maker-Based ATM Access Modules	33-4
FCSM ATM Access Ports	33-5
LAN Switch with ATM Uplinks	33-6
The ATM Menu	33-7
Modifying an ATM Access Port Configuration	33-8
Configuring UNI 4.0 on an ATM Access Port	33-13
Creating a Virtual Channel Connection	33-15
Traffic Shaping Parameters for the ASX-M-622RF-1W Module	33-19
Modifying a Virtual Channel Connection	33-22
Deleting a Virtual Channel Connection	33-23
Creating a Virtual ATM Address	33-24
Modifying Virtual ATM Addresses	33-25
Deleting a Virtual ATM Address	33-25
Viewing ATM Port Configuration Information	33-26
Information on the Ports for One ATM Access Module	33-29
Information on One Port	33-30

Viewing SSCOP, ILMI, and PHY	33-31
Viewing SSCOP, ILMI, and PHY Information on All Ports	33-31
Viewing SSCOP, ILMI, and PHY Information on One ATM Access Module	33-33
Viewing SSCOP, ILMI, and PHY Information on One Port	33-34
Viewing Virtual Channel Connections	33-35
Information on the Ports for One ATM Access Module	33-38
Information on One Port	33-40
Information on One Virtual Path	33-41
Information on One Virtual Channel	33-42
Viewing Virtual ATM Addresses	33-43
Viewing the ATM Layer Statistics Table	33-45
Viewing the ATM Layer Rx Error Statistics Table	33-46
ATM Layer Receive Error Statistics Table For One ATM Access Module	33-48
ATM Layer Receive Error Statistics Table For One ATM Access Port	33-49
Viewing the ATM Layer Tx Error Statistics Table	33-50
ATM Layer Transmit Error Statistics Table For One ATM Access Module	33-51
ATM Layer Transmit Error Statistics Table For One ATM Access Port	33-51
Viewing the ATM Connection Statistics Table	33-52
Information on the Ports for one ATM Access Module	33-53
Information on One Port	33-53
Information on One Virtual Channel	33-54
Viewing the ATM Connection Rx Error Statistics Table	33-55
Viewing the ATM Connection Tx Error Statistics Table	33-57
Displaying the Number of ATM Connections on a Switch	33-59
Traffic Shaping (ASM2/ASX Modules)	33-60
Traffic Shaping Overview	33-61
Values for Traffic Shaping	33-63
Configuration Guidelines	33-67
Configuring ASM2/ASX Traffic Shaping	33-68
Viewing Traffic Shaping Parameters	33-70
34 Managing Circuit Emulation Modules	34-1
The ASM-CE	34-2
The ASM-CE Ports: An Overview	34-3
The CSM-CE	34-4
Circuit Emulation T1/E1 Ports	34-5
Changes in Release 4.1.4 and Later	34-5
Configuring a Circuit Emulation Module	34-6
Circuit Emulation Services	34-7

Circuit Emulation Clocking Modes	34-8
Synchronous Clocking	34-8
Synchronous Residual Time Stamp (SRTS) Clocking	34-8
Adaptive Clocking	34-9
Application Example - ASM-CE	34-10
The Circuit Emulation Menu	34-11
Creating a Virtual Channel Connection on a T1/E1 Port	34-12
Creating a Soft Permanent Virtual Circuit (SPVC) on T1/E1 Ports	34-17
Using the SPVC Configuration Command to Configure a CE-SPVC	34-20
Creating a Virtual Channel Connection on a Serial Port	34-21
Configuring a Circuit Emulation T1/E1 Port	34-23
Configuring a Circuit Emulation Serial Port	34-25
Modifying a Virtual Channel Connection	34-27
Deleting a Virtual Circuit	34-28
Viewing Circuit Emulation Information	34-29
Viewing Information on All Circuit Emulation Boards in a Switch	34-29
Viewing Information on One Module	34-31
Viewing Information for a T1 or E1 Port	34-32
Viewing Information for a Serial Port	34-33
Viewing Information for a T1/E1 Virtual Circuit	34-34
Viewing Information for a Serial Port Virtual Circuit	34-36
Clearing ATM Circuit Emulation Statistics	34-37
35 LANE Server Configuration	35-1
Introduction	35-1
LAN Emulation Components	35-1
LANE Component Interactions	35-2
LAN-to-ATM Communication	35-3
Overview of LES/BUS and LECS Configuration	35-4
The LANE Service Menu (LSM)	35-4
Configuring LES/BUS and LECS	35-5
Making SubMenu Option Selections	35-6
Specifying a Global ELAN Name	35-7
Creating a LES/BUS Pair	35-8
Modifying a LES/BUS Pair	35-11
Deleting a LES/BUS Pair	35-12
Creating the LECS	35-13
Modifying the LECS	35-15
Deleting the LECS	35-16
Adding ELANs to the LECS	35-17
Deleting an ELAN from the LECS	35-19
Adding Policies to ELANs in the LECS	35-20

Deleting Policies from ELANs in the LECS	35-22
Displaying a List of LES/BUS Pairs	35-23
Displaying LES/BUS Pair Status	35-24
Displaying LES/BUS Pair Statistics	35-26
Displaying LES/BUS Configuration	35-32
Displaying LECs in a LES/BUS Pair	35-33
Displaying MAC Addresses for a LES/BUS Pair	35-34
Displaying Registered Route Descriptor for a LES/BUS Pair	35-35
Displaying Detailed LEC Information	35-36
Displaying LECS Status	35-38
Displaying LECS Statistics	35-39
Displaying LECS Configuration	35-41
Displaying ELANs in the LECS	35-42
Displaying ELAN Policies in the LECS	35-43
36 Configuring ATM Services	36-1
Introduction	36-1
ATM Services	36-1
PVC/SVC Support	36-3
LANE Client (LEC) Services	36-4
Token Ring vs. Ethernet Networks	36-5
Source-Routed Traffic	36-6
LANE Version 2.0	36-6
LANE Client (LEC) Enable/Disable Traps	36-6
LAN Emulated Client Start-Up and Back-Off Timers	36-7
Debugging LANE Client Problems	36-8
ATM Trunking	36-9
Groups over ATM	36-9
VLANs over ATM	36-10
Spanning Tree and Trunking	36-10
Translations Across Trunks	36-11
ATM Trunking and Older ATM Access Modules	36-11
Classical IP Routing	36-12
LLC Header Encapsulation	36-12
IP to ATM Address Resolution	36-12
IP Over ATM Signaling	36-12
Typical CIP over ATM Configuration	36-13
Point-to-Point Bridging	36-14
VLAN Clusters	36-15
Method 1	36-16
Method 2	36-16

1483 Scaling Services	36-17
1483 Routed Format Services	36-19
Configuring ATM Services	36-20
Services Menu	36-20
Creating a Service	36-21
Creating a LANE Client Service	36-23
Setting LANE Client Parameters	36-26
Using the WKA as the Primary Source for the LECS Address	36-28
Setting the LECS Manually	36-29
Creating a Trunking Service	36-31
Creating a Classical IP Service	36-33
Creating a PTOp Bridging Service	36-36
Creating a VLAN Cluster Service	36-38
Creating a 1483 Scaling Service	36-40
Editing and Displaying 1483 Mapping Parameters	36-43
Creating a 1483 Routed Format Service	36-47
Modifying a Service	36-49
Modifying a LANE Client Service	36-49
Modifying a Trunking Service	36-50
Modifying a Classical IP Service	36-51
Adding Static ARP Entries for CIP	36-53
Modifying a PTOp Bridging Service	36-54
Modifying a VLAN Cluster Service	36-55
Modifying VLAN Cluster Parameters	36-56
Modifying a 1483 Scaling Service	36-57
Modifying a 1483 Routed Format Service	36-59
Deleting a Service	36-60
Deleting Static ATM ARP Entries for CIP	36-61
Viewing ATM Access Port Services	36-62
Viewing General Service Statistics on a Port	36-63
Viewing Service Statistics for a LANE Client	36-64
Viewing the LANE LE_ARP Table	36-67
Viewing ATM Service Statistics for Classical IP	36-68
Viewing the CIP ARP Table	36-70
Viewing Service Statistics for VLAN Clusters	36-71
Viewing 1483 Scaling Service Parameters	36-72
Viewing 1483 Routed Format Services Statistics	36-74
Debugging LANE Client Problems	36-75

37	Multi-Protocol Over ATM (MPOA)	37-1
	Introduction	37-1
	Network Functionality and MPOA	37-1
	MPOA Requirements	37-4
	The MPOA Client (MPC)	37-4
	The MPOA Network	37-7
	The MPOA Management Menu	37-10
	Configuring an MPOA Client Service	37-11
	Field Descriptions	37-12
	Viewing Client Service Status	37-14
	Field descriptions	37-14
	Viewing Client Service Statistics	37-15
	Field descriptions	37-16
	Viewing Entries in the Ingress Cache Table	37-19
	Field descriptions	37-19
	Viewing Entries in the Egress Cache Table	37-20
	Viewing MPOA Servers	37-21
	Field descriptions	37-21
38	Frame Relay/ATM Internetworking	38-1
	Frame Relay/ATM Internetworking Overview	38-2
	ATM as a Backbone for Frame Relay Users (FRF.5)	38-2
	How to Set Up This FR/ATM IWF Network	38-3
	ATM and Frame Relay Interworking Services (FRF.8)	38-9
	How to Set Up This FR/ATM IWF Service	38-10
	Configuring an FR/ATM IWF on an FCSM-II	38-15
	Sample WSM/FCSM-II Frame Relay/ATM IWF	38-15
	Dynamically Loading the FR/ATM Image File	38-19
	Enabling and Disabling FR/ATM Internetworking Software	38-20
	Displaying the Status of FR/ATM Internetworking	38-20
	Enabling FR/ATM Internetworking	38-20
	Disabling FR/ATM Internetworking	38-20
	The Frame Relay/ATM Internetworking Submenu	38-21
	Creating an FR/ATM Internetworking Function	38-23
	Enabling/Disabling the Frame Relay PVC on an FR/ATM IWF	38-27
	Modifying an FR/ATM Internetworking Function	38-28
	Modifying ATM Parameters on a FR/ATM Internetworking Function	38-32
	Deleting the FR/ATM Internetworking Function on a Port	38-35
	Deleting FR/ATM PVCs on a Port	38-36
	Deleting All FR/ATM PVCs on a Port	38-36
	Deleting One FR/ATM PVC on a Port	38-36

Displaying FR/ATM IWF Configurations	38-37
Displaying the Configurations of All FR/ATM IWFs on a Switch	38-37
Displaying the Configurations of All FR/ATM IWFs on a Port	38-38
Displaying the Detailed Configuration of a Single FR/ATM IWF	38-39
Displaying FR/ATM IWF Statistics	38-42
Displaying the Statistics for All FR/ATM IWFs on a Switch	38-42
Displaying the Statistics for All FR/ATM IWFs on an ATM Switching Module	38-43
Displaying the Statistics for All FR/ATM IWFs on a Port	38-43
Displaying the Statistics for a Single FR/ATM IWF on a Port	38-44
Displaying FR/ATM IWF Statistics for FRF.5 Networks	38-44
Displaying FR/ATM IWF Statistics for FRF.8 Services	38-45
39 SONET Error Collection	39-1
SONET Overview	39-3
SONET Error Collection Intervals	39-3
SONET Protocol Layers	39-3
Path Layer	39-3
Line Layer	39-4
Section Layer	39-4
Medium Layer	39-4
SONET Connections	39-4
Enabling and Disabling SONET Error Collection	39-5
Displaying SONET Error Collection Status	39-5
Enabling SONET Error Collection	39-5
Disabling SONET Error Collection	39-5
The SONET Error Collection Menu	39-6
Enabling SONET Error Collection on ATM Ports	39-7
Enabling SONET Error Collection on a Single Port	39-7
Enabling SONET Error Collection on all ATM Ports on a Switching Module	39-8
Enabling SONET Error Collection on all ATM Ports in a Switch	39-8
Viewing the SONET Medium Table	39-9
Viewing the SONET Medium Table for a Single ATM Port	39-9
Viewing the SONET Medium Table for All ATM Ports on a Switching Module	39-10
Viewing the SONET Medium Table for all ATM Ports	39-10
Viewing SONET Error Statistics Tables	39-11
Viewing SONET Error Statistics for the Current Interval	39-11
Section Table Statistics	39-13
Line Table Statistics	39-14
Path Table Statistics	39-15
Viewing SONET Error Statistics for a Single Interval	39-17
Viewing SONET Error Statistics for All Intervals	39-19
Viewing Individual SONET Error Statistics Tables	39-21

Clearing SONET Error Statistics Tables for the Current Interval	39-22
Clearing Error Statistics for All Tables	39-22
Clearing Error Statistics for a Single Table	39-23
Viewing the Summary of SONET Error Statistics	39-24
40 Cell Switching Modules (CSMs)	40-1
Virtual Circuits	40-1
Dynamic Input Buffering With Output Control	40-1
Quality of Service (QoS)	40-2
Partial Packet Discard (PPD) and Early Packet Discard (EPD)	40-2
Dual Leaky Buckets	40-2
Available Bit Rate Traffic	40-2
MPM-C and MPM-III Signaling Performance	40-2
Required Image Files	40-3
ATM Switching Applications and Configurations	40-6
Frame-Based LAN Switch With ATM Uplinks	40-6
Hybrid LAN/ATM Switch	40-7
Pure ATM Campus Switch	40-8
Distributed Cell Switching Fabric	40-9
Buffer Management	40-10
Cell Buffers	40-11
Module Mix for OmniSwitch Configurations	40-12
Pure LAN Switch	40-12
Hybrid LAN/ATM Switch	40-13
Pure ATM Switch	40-14
Cell Switching Modules	40-15
CSM Pinouts	40-16
CSM RJ-45 Specifications	40-16
CSM-CE RJ-48C Specifications	40-16
Frame-to-Cell Switching Module (FCSM)	40-17
FCSM I (FCSM-155)	40-19
FCSM I Redundancy	40-19
FCSM II	40-22
FCSM II Technical Specifications	40-22
The Cell Switching Management Processor Module (MPM-C)	40-23
MPM-C Technical Specifications	40-24
MPM-C Serial and Ethernet Management Ports	40-27
Ethernet Management Port	40-27
Configuring MPM-C Serial Ports	40-28
Flash Memory and OmniSwitch Software	40-28
MPM-C Redundancy	40-28
Redundancy for MPM Functions	40-28
Redundancy for FCSM Functions	40-28
ATM Services on the MPM-C	40-29

CSM-155F	40-30
CSM-155 Technical Specifications	40-31
Jumper Settings	40-33
CSM-622	40-34
CSM-622 Technical Specifications	40-35
Jumper Settings	40-37
CSM-155C-8	40-38
CSM-155C-8 Technical Specifications	40-39
Jumper Settings	40-41
CSM-A25-12	40-42
CSM-A25-12 Technical Specifications	40-42
CSM-A25-24W	40-44
CSM-A25-24 Technical Specifications	40-44
CSM-U/CSM-U+	40-46
CSM-U+	40-46
CSM-U/CSM-U+ Technical Specifications	40-47
CSM-AB-155F	40-49
CSM-AB-155F Technical Specifications	40-50
Jumper Settings	40-51
CSM-AB-155C	40-52
CSM-AB-155C Technical Specifications	40-53
Jumper Settings	40-54
CSM-AB-DS1/E1-4W	40-55
CSM-AB-DS1/E1 Technical Specifications	40-56
CSM-AB-DS3/E3-2W	40-57
CSM-AB-DS3/E3 Technical Specifications	40-58
CSM-AB-CE-T1/E1-4W	40-59
CSM-AB-CE Technical Specifications	40-60
CSM-AB-CE-E1-4W Impedance Jumper Numbers	40-60
CSM-AB-CE-E1-4W Grounding Jumper Numbers	40-61
CSM-AB-CM	40-62
CSM-AB-CM Technical Specifications	40-63
CSM-AB-CM Port Type Jumper Settings	40-64
CSM-AB-CM Port Shield Jumper Settings	40-64
CSM-AB-IMA-DS1/E1-8W	40-65
CSM-AB-IMA-DS1-8W/CSM-AB-IMA-E1-8W Technical Specifications	40-66
CSM-AB-IMA-E1-8W Jumpers	40-67
CSM-AB-IMA-E1-8W Impedance Jumper Numbers	40-67
CSM-AB-IMA-E1-8W Grounding Jumper Numbers	40-68
CSM-ABT-155F	40-69
Installing a CSM-ABT-155F in a CSM-U/CSM-U+	40-69
CSM-ABT-155F Technical Specifications	40-71

41 Managing Cell Switching Modules (CSMs)	41-1
Virtual Circuits	41-4
VPs and VCs	41-5
Point-to-Point Virtual Circuits	41-6
Point-to-Multipoint Virtual Circuits	41-6
PVCs, SVCs, and Soft PVCs	41-7
ATM Traffic Types	41-8
Quality of Service (QoS)	41-10
Flow Control	41-12
Resource Management	41-12
Explicit Forward Congestion Indication (EFCI)	41-12
Traffic Management	41-13
Cell Loss Priority (CLP) and Policing	41-14
Traffic Contract Descriptors	41-16
Understanding Traffic Descriptor Names	41-17
Traffic Contract Enforcement	41-18
Traffic Policing and Leaky Bucket Algorithms	41-19
Dual Leaky Buckets	41-21
Leaky Buckets and Class of Service	41-22
Class of Service Profiles	41-23
Constant Bit Rate (CBR)	41-23
Variable Bit Rate, Real Time (rt_VBR)	41-24
Variable Bit Rate, Non-Real Time (nrt_VBR)	41-24
Available Bit Rate (ABR)	41-25
Unspecified Bit Rate (UBR)	41-25
The ATM Menu	41-26
FCSM Modules in ATM Menu Commands	41-28
Modifying a Port Configuration	41-29
Creating a Permanent Virtual Circuit	41-33
Setting Up Basic VC Parameters	41-33
Configuring Point-to-Multipoint Virtual Circuits	41-38
Configuring Traffic Parameters	41-40
Configuring Statistics and Priority Parameters	41-45
Configuring a Cell Switch for Switched Virtual Circuits (SVCs)	41-46
Configuring VP Switching	41-51
Modifying a Virtual Circuit	41-53
Deleting a Virtual Circuit	41-53

CSM Port Auto Configuration	41-54
Modifying CSM Port Auto Configuration	41-54
Modifying One or More CSM Boards	41-56
Modifying One or More Ports	41-57
Viewing CSM Port Auto Configuration	41-58
Information on the Ports for One or More CSM Boards	41-60
Information on One or More Single Ports	41-61
Information on One Virtual Instance	41-62
Viewing Port Configurations	41-63
Information on the Ports for One CSM Board	41-71
Information of One Port	41-74
Viewing SSCOP, ILMI, and PHY	41-75
Viewing SSCOP, ILMI, and PHY Information on All Ports	41-75
Viewing SSCOP, ILMI, and PHY Information on One CSM Board	41-78
Viewing SSCOP, ILMI, and PHY Information on One Port	41-80
Viewing Virtual Connections	41-82
Information on All Virtual Circuits in a Switch	41-82
Information on the Ports for One CSM Virtual Circuit	41-89
Information on One Port	41-92
Information on One Virtual Path	41-95
Information on One Virtual Channel	41-98
Displaying the Number of ATM Connections on a Switch	41-100
42 Advanced CSM Management	42-1
Soft PVCs	42-3
Creating a Soft PVC	42-3
Configuring Traffic Parameters	42-8
Configuring Statistics and Priority Parameters	42-14
Configuring Point-to-Multipoint Soft PVCs	42-15
Modifying a Point-to-Multipoint Soft PVC	42-17
Configuring Soft PVC Retry Parameters	42-18
Configuring Broadband Bearer Capability Parameters	42-18
Configuring Transport Priority with the Multiple-Peer Group Software	42-19
Viewing Soft PVCs	42-21
Virtual UNI/NNI Using Virtual Path (VP) Tunneling	42-24
Extending PNNI Over Public Networks	42-24
Virtual Path Mux	42-25
Signaling Hop Reduction	42-25
Creating a VP Tunnel	42-26
Displaying VP Tunnel Information	42-30
Viewing SSCOP, ILMI, and PHY	42-32
Modifying a VP Tunnel	42-35
Deleting a VP Tunnel	42-35
Configuring a LECS ATM Address	42-36

Mapping Service Registry Table Addresses to the Well-Known Address	42-37
Modifying Existing Addresses in the Service Registry Table	42-38
Viewing ATM Layer Statistics	42-39
Viewing ATM Layer Receive Error Statistics	42-41
Information on the Ports for One CSM Board	42-44
Information on One Port	42-45
Viewing ATM Connection Statistics Table	42-46
Information on All ATM Boards in a Switch	42-46
Information on the Ports for one CSM Board	42-48
Information on One Port	42-49
Information on One Virtual Path	42-50
Information on One Virtual Channel	42-50
Viewing CSM Port and Connection Statistics	42-51
Displaying Port Statistics	42-51
Displaying Connection Statistics	42-53
Viewing Connection Receive Error Statistics	42-54
Intelligent Multicast Replication	42-56
Multicast Replication Trees	42-58
Enabling Intelligent Multicast Replication	42-59
Disabling Intelligent Multicast Replication	42-59
Displaying Intelligent Multicast Replication Performance Gain	42-60
Displaying Intelligent Multicast Replication Trees	42-61
CSM-ABT Traffic Shaping	42-64
Using the CLI to Configure CSM Traffic Shaping	42-65
Software Requirements	42-65
CLI Conventions	42-66
Global Definitions	42-66
Traffic Shaping Configuration Examples	42-67
Activating CSM Traffic Shaping	42-67
Enabling/Disabling CSM Traffic Shaping	42-67
Viewing CSM Traffic Shaping	42-69
Disabling CSM Traffic Shaping	42-70
Switching from CLI Mode to UI Mode	42-70
43 Inverse Multiplexing Over ATM (IMA)	43-1
IMA Hardware	43-2
IMA Software	43-2
IMA Configuration Overview	43-3
IMA Process Overview	43-4
Adding and Deleting Links in an IMA Group	43-4
Cell Switching Module (CSM) Ports and IMA Groups (CSM-AB-IMA-DS1/E1-8W Submodule)	43-5
Sample IMA Network	43-6

IMA Application Example	43-8
How to Set Up this Network	43-9
IMA Theory of Operation	43-11
IMA Link State Machine (LSM)	43-11
IMA Synchronization Process	43-12
The IMA Submenu	43-13
User Interface Command Syntax	43-14
Creating IMA Groups	43-15
Adding and Modifying IMA Group Membership	43-18
Adding IMA Group Membership	43-18
Modifying IMA Group Membership	43-20
Modifying IMA Groups	43-21
Modifying IMA Groups with T1 Ports (Short-Haul Line)	43-21
Modifying IMA Groups with T1 Ports (Long-Haul Line)	43-24
Modifying IMA Groups with E1 Ports	43-25
Configuring IMA Link Parameters	43-28
Conducting an IMA Test	43-29
Starting an IMA Test	43-29
Ending an IMA Test	43-31
Restarting an IMA Group	43-32
Deleting IMA Groups	43-32
Upgrading Flash Memory on CSM-AB-IMA-DS1/E1-8W Submodules	43-33
Displaying the Summary Status of IMA Groups	43-35
Displaying the Summary Status of All IMA Groups	43-35
Displaying the Summary Status of a Single IMA Group	43-38
Displaying the Detailed Status of a Single IMA Group with Link Status	43-41
Displaying the Summary Status of IMA Links	43-44
Displaying the Summary Status of All IMA Links	43-44
Displaying the Detailed Status of a Single IMA Link	43-46
Displaying the Statistics for an IMA Group	43-48
Displaying Summary Statistics for an IMA Group	43-48
Displaying Detailed Statistics for an IMA Group	43-50
Displaying 24-Hour Performance Statistics on a Local Group	43-54
Displaying Current Performance Statistics on a Local Group	43-55
Displaying Performance Statistics Intervals on a Local Group	43-56
Displaying Detailed Statistics for IMA Links	43-57
Displaying 24-Hour Performance Statistics on a Local Link	43-60
Displaying Current Performance Statistics on a Local Link	43-63
Displaying Performance Statistics Intervals on a Local Link	43-64
Clearing IMA Group Statistics	43-67

Clearing IMA Link Statistics	43-67
Troubleshooting IMA Networks	43-68
44 ATM Accounting	44-1
Accounting Overview	44-2
CDRs and the Concept of “Charging”	44-4
Terminated CDRs and Intermediate CDRs	44-5
Periodic Collection of CDRs	44-6
The Benefits of Using Periodic Collection	44-6
Collection Interval	44-6
Tariff Period	44-6
How Periodic Collection is Computed	44-6
Combining A Collection Interval With Tariff Periods	44-7
Maximum Number of Collects	44-8
How CDRs Are Stored	44-9
Storage Strategy	44-9
Size of Temporary Storage	44-9
Congestion Strategy	44-10
Establishing Threshold Levels for Temporary Storage	44-10
Accept Calls, Refuse Calls	44-11
Traps	44-11
CDR Parameters	44-12
Enabling the Accounting Function	44-18
Using the CLI to Configure ATM Call Accounting	44-20
Software Requirements	44-20
CLI Conventions	44-21
Global Definitions	44-21
Configuration Examples	44-22
Node-Level Configuration	44-22
Enabling Accounting at the Node Level	44-22
Disabling Accounting	44-24
Forcing a Switchover to the Alternate Collection Device	44-24
Collecting CDRs From All Established Connections	44-24
Defining a Congestion Strategy	44-25
Port-Level Configuration	44-26
Enabling Accounting at the Port Level and Defining Its Congestion Strategy	44-26
Disabling Accounting	44-26
PVC- and Soft PVC-Level Configuration	44-27
Enabling Accounting at the PVC and Soft PVC Level	44-27
Disabling Accounting at the PVC and Soft PVC Level	44-27

Collection Interval and Tariff Periods	44-28
Define a Collection Interval	44-28
Define a Tariff Period	44-28
Configuration Queries	44-29
45 Clocking ATM Networks	45-1
Introduction	45-1
ATM Data Traffic	45-1
Selecting Clocking Sources	45-2
Configuring Transmit Clocking (Port-Level Clocking)	45-2
Modules that Require 8 kHz Timing	45-2
Modules that Require 19.44 MHz Timing	45-3
Timing Considerations for DS3/E3 and PLCP	45-3
Timing Modes	45-3
Bus-Level Clocking	45-4
Bus Lines	45-4
Clocking Summary	45-5
Viewing/Configuring Clocking	45-7
Viewing the Clocking Configuration	45-8
Viewing Configured Ports	45-8
Viewing Clocking on All Ports	45-9
Field Descriptions	45-9
Configuring Clocking	45-10
Modifying the Clocking Configuration (CSM Ports)	45-10
Field Descriptions	45-10
Examples	45-11
Modifying the Clock Switching Time (CSM Ports)	45-11
Modifying the Transmit Clocking Source	45-12
Modifying the Transmit Clocking Source (T1/E1 Ports)	45-13
Clock Backup	45-14
Backup Design	45-14
46 Configuring and Monitoring PNNI	46-1
PNNI Configuration	46-4
PNNI Port Type Configuration	46-4
Running PNNI Software	46-4
Loading the PNNI Module	46-5
Default ATM Address	46-5
Static Routes/IISP	46-5
Elements of a PNNI Network	46-6
Multiple Peer Group Networks	46-7
Peer Group Leader (PGL) Election Algorithm	46-9
Complex Representation	46-10

PNNI Identifiers	46-12
Level Identifier	46-12
Node ID	46-12
Port ID	46-13
Peer Group ID	46-13
Summary Addresses	46-14
PNNI Packet Types	46-15
Hello packets	46-15
Database Summary packets	46-15
PNNI Topology State Element (PTSE) Request packets	46-15
PNNI Topology State Packets (PTSPs)	46-15
PNNI Topology State Element (PTSE) Acknowledgment packets	46-15
Metrics and Attributes	46-16
Summarization and Reachability	46-18
PNNI Network Initialization	46-19
Step 1. Discover Attached ATM End Stations	46-19
Step 2. Discover Neighbor Nodes	46-20
Step 3. Send Topology Information for Updating Other Nodes	46-21
Step 4. Compute the Topology of the Peer Group	46-21
Establishing a Connection	46-22
Step 1. Receive a Call Request	46-22
Step 2. Locate Called Parties	46-23
Step 3. Path Selection	46-24
Step 4. Send Setup Message	46-25
Step 5. Process Setup Message	46-26
Step 6. Send Call Proceeding Message	46-27
Step 7. Send Connect Message	46-27
Step 8. Data Flow	46-27
The PNNI Menu and Submenus	46-28
Pconfig	46-28
Proute	46-29
Pinfo	46-29
Pstats	46-30
Padmin	46-30
Summary Form of PNNI Commands	46-31
Displaying PNNI Command Help (Multi-Peer Group PNNI Only)	46-31
Configuring General PNNI Parameters	46-32
Configuring PNNI Operation Limits	46-35
Selecting Metrics Used in Path Computations	46-38
Configuring Multi-Peer Group Operation	46-39
Configuring Node-Specific Parameters	46-40
Configuring Single-Peer Group Nodes	46-40
Configuring PTSE and Hello Timers	46-42
Configuring Multiple-Peer Group Nodes	46-45

Configuring Peer Group Leader Nodes	46-46
Configuring the Peer Group Leader Election Process on All Node Levels	46-48
Configuring Port Parameters	46-50
Viewing General PNNI Information	46-53
Viewing Node-Specific Information	46-56
Viewing Timer Information	46-60
Viewing PNNI Neighbor Information	46-62
Summary Form of pnbrs	46-63
Viewing Port Information	46-64
Summary Form of ppinfo	46-65
Viewing Link Information	46-66
Summary Form of plink	46-68
Viewing the PTSE Database	46-69
Standard Output	46-69
Verbose Mode Output	46-70
Summary Mode Output	46-72
Viewing End-Point Adjacencies	46-73
Configuring PNNI Scope Mapping Parameters	46-74
Viewing the PNNI Map Table	46-77
Summary Form of pmap	46-78
Network Diagram of pmap Summary Display	46-79
Viewing the PNNI Nodal Map Table	46-80
Summary Form of pnmap	46-82
Viewing Current PNNI Calls	46-83
Viewing Current DTLs	46-84
Summary Form of pdtl	46-84
Viewing Basic Port Statistics	46-85
Viewing Port Error Statistics	46-86
Viewing Port PTSE Statistics	46-87
Halting PNNI Operations	46-88
Restarting PNNI	46-89
Resetting PNNI Statistics Counters	46-90
Viewing PNNI Configuration Information	46-91
Removing PNNI Configuration Information	46-91
Verifying Routes	46-92
Operating PNNI with Redundant MPMs	46-93
Configuring Node Information on Redundant MPMs	46-93
Verifying PNNI Node Information on Redundant MPMs	46-94
FCSM I PNNI Frame Size Guidelines	46-96

47	Managing IISP and PNNI Routes	47-1
	Setting Up Static Routes	47-1
	The PNNI/IISP Route Management Menu	47-2
	Configuring a PNNI/IISP Static Route Property	47-3
	Configuring QoS and Metrics for Inbound and Outbound Routes	47-5
	Configuring the Associated Transit Network	47-6
	Deleting a PNNI/IISP Static Route Property	47-8
	Adding a PNNI/IISP Static Route Address	47-9
	Deleting a PNNI/IISP Static Route Address	47-11
	Viewing PNNI/IISP Static Route Properties	47-13
	Viewing PNNI/IISP Static Route Prefixes	47-14
	Viewing Learned PNNI/IISP Routes to Reachable Addresses	47-15
	Summary Output for proutea	47-16
	Viewing PNNI/IISP Learned Routes to Other Nodes	47-17
	Summary Output for prouten	47-18
48	Managing WAN Switching Modules	48-1
	Introduction	48-1
	Type of Service (ToS)	48-2
	Supported Physical Interfaces	48-4
	Universal Serial Port	48-4
	ISDN Basic Rate Interface Port	48-4
	Fractional T1 Port	48-4
	Fractional E1 Port	48-4
	Supported Protocols	48-5
	Application Examples	48-5
	Frame Relay WSM/WSX Using Serial Ports	48-5
	Back-to-Back WSM/WSX Using T1 Ports	48-6
	Combined Frame Relay with ISDN Backup	48-7
	OmniSwitch WAN Modules	48-8
	WAN Pinouts	48-8
	WAN BRI Port Specifications (S/T Interface)	48-9
	WAN BRI Port Specifications (U Interface)	48-9
	WAN T1/E1 Port Specifications	48-10
	WAN Serial Port Specifications	48-11
	WSM-S/SC	48-13
	WSM Technical Specifications	48-13
	WSM-FT1/FE1	48-15
	WSM-FT1/E1 Technical Specifications	48-15
	Cabling/Jumper Settings	48-17
	WSM-BRI	48-18
	WSM-BRI Technical Specifications	48-18

Cable Interfaces for Universal Serial Ports	48-21
DTE/DCE Type and Transmit/Receive Pins	48-21
Data Compression	48-22
Loopback Detection	48-23
The WAN Port Software Menu	48-24
Setting Configuration Parameters	48-24
Modifying a Port	48-24
Serial Port Example	48-25
ISDN-BRI Port Example	48-30
Fractional T1 Port Example	48-33
Viewing Configuration Parameters for the WSM	48-36
Viewing Parameters for all Submodules in the Chassis	48-36
Viewing Parameters for all Ports in a Single Submodule	48-37
Viewing Port Parameters	48-38
Deleting Ports	48-45
Obtaining Status and Statistical Information	48-46
Obtaining Information on All Boards in a Switch	48-46
Field Descriptions	48-46
Obtaining Information on the Ports for a Single WSM Board	48-48
Field Descriptions	48-50
Viewing Information on a Single Port	48-50
Configuring 31 Timeslots on a WAN E1 Port	48-53
49 Managing Frame Relay	49-1
Back-to-Back Frame Relay Configurations	49-3
Universal Serial Port Cable Interfaces	49-4
“Physical” and “Logical” Devices	49-4
Compression	49-5
Virtual Circuits and DLCIs	49-6
WSM Self-Configuration and Virtual Circuits	49-7
Congestion Control	49-8
Regulation Parameters	49-8
Discard Eligibility (DE) Flag	49-9
Interaction Among Congestion Parameters	49-9
Notification By BECN	49-11
Notification By FECN	49-12
Frame Formats Supported	49-13
Bridging Services	49-14
Frame Relay IP Routing	49-15
The Frame Relay Subnet and “Split Horizon”	49-16
Frame Relay IPX Routing	49-18
Trunking	49-19

The Frame Relay Software Menu	49-20
Setting Configuration Parameters	49-21
Modifying a Port	49-21
Modifying a Virtual Circuit	49-28
Adding a Virtual Circuit	49-31
Viewing Configuration Parameters for the WSM	49-32
Viewing Parameters for all WSMs in the Chassis	49-32
Viewing Port Parameters	49-33
Viewing Virtual Circuit Parameters	49-34
Deleting Ports and Virtual Circuits	49-35
Deleting a Virtual Circuit	49-35
Deleting a Port and Its Virtual Circuits	49-36
Obtaining Status and Statistical Information	49-37
Information on All Boards in a Switch	49-37
Information on the Ports for One WSM Board	49-41
Information on One Port	49-42
Information on One Virtual Circuit	49-48
Resetting Statistics Counters	49-51
Resetting Statistics for a WSM Board	49-51
Resetting Statistics for a WSM Port	49-51
Resetting Statistics for a Virtual Circuit (DLCI)	49-51
Managing Frame Relay Services	49-52
Configuring a Bridging Service	49-54
Configuring a WAN Routing Service	49-56
Step 1. Set Up a Frame Relay Routing Group	49-56
Step 2. Set Up a Frame Relay Routing Service	49-57
Configuring a Trunking Service	49-59
Viewing Frame Relay Services	49-61
Modifying a Frame Relay Service	49-62
Deleting a Frame Relay Service	49-63
50 Point-to-Point Protocol	50-1
PPP Connection Phases	50-1
Data Compression	50-2
Multi-Link PPP	50-2
Multilink Modes of Operation	50-3
PPP Fragmentation Interleaving	50-3
Overview of PPP Configuration Procedures	50-4
The PPP Submenu	50-6
PPP Configuration Overview	50-6
Setting Global PPP Parameters	50-7
Adding a PPP Entity	50-9

Modifying a PPP Entity	50-14
Viewing PPP Entity Configurations	50-15
Displaying the Configuration of All PPP Entities	50-15
Displaying the Configuration of a Specific PPP Entity	50-16
Displaying PPP Entity Status	50-17
Displaying the Status of All PPP Entities	50-17
Displaying the Status of a Specific PPP Entity	50-18
Deleting a PPP Entity	50-20
51 WAN Links	51-1
Introduction	51-1
Configuring WAN Interfaces	51-1
The Link Submenu	51-2
Adding a WAN Link	51-3
Adding WSM Port Links	51-3
Adding ISDN Call Links	51-4
Modifying a WAN Link	51-9
Modifying ISDN Links	51-9
Modifying WSM Links	51-10
Deleting WAN Links	51-11
Viewing WAN Links	51-12
Displaying All Existing WAN Links	51-12
Displaying Information for a Specific WAN Link	51-13
Displaying Link Status	51-15
Displaying Status for All WAN Links	51-15
Displaying Status for a Specific WAN Link	51-16
52 Managing ISDN Ports	52-1
Overview of ISDN	52-1
Basic Rate Interface (BRI) Versus Primary Rate Interface (PRI)	52-1
“U”, “S/T”, and “R” Interfaces	52-2
The “B,” “D,” and “H” Channels	52-2
The ISDN Submenu	52-3
Switch Configuration	52-3
Modifying an ISDN Configuration Entry	52-4
Deleting an ISDN Configuration Entry	52-5
Viewing an ISDN Configuration Entry	52-6
Displaying ISDN Configuration Entry Status	52-7
Displaying Status of All ISDN Ports	52-7
Displaying Status of a Specific ISDN Slot	52-8
Displaying Status of a Specific ISDN Port	52-9

53	Managing T1 and E1 Ports	53-1
	T1 and E1 Overview	53-2
	The T1/E1 Menu	53-3
	Configuring a T1 Port	53-4
	Configuring an E1 Port	53-8
	Viewing T1/E1 Configuration and Alarm Information	53-11
	Viewing Information for all T1/E1 Ports in the Switch	53-11
	Viewing Information for T1/E1 Ports on One Module	53-12
	Viewing Information For a T1 Port	53-13
	Viewing Information For an E1 Port	53-15
	Viewing T1/E1 Local Statistics	53-17
	Viewing Total Local Statistics	53-17
	Viewing Current Local Statistics	53-18
	Viewing Local Historical Statistics	53-19
	Viewing T1 Remote Statistics	53-20
	Viewing Total Remote Statistics	53-20
	Viewing Current Remote Statistics	53-21
	Viewing Remote Historical Statistics	53-21
	Clearing the Framer Statistics for a T1/E1 Port	53-22
54	Managing DS3/E3 Modules	54-1
	DS3/E3 Overview	54-1
	DS3 Framing	54-1
	E3 Framing	54-1
	DS3/E3 Port Management Menu	54-2
	Configuring a DS3 Port	54-2
	Field Descriptions	54-3
	Configuring an E3 Port	54-4
	Field Descriptions	54-5
	Viewing DS3/E3 Configuration and Alarm Information	54-7
	Viewing Information for all DS3/E3 Ports in the Switch	54-7
	Field Descriptions	54-7
	Viewing Information for DS3/E3 Ports on a Board	54-8
	Viewing Information for a DS3 Port	54-9
	Field Descriptions	54-9
	Viewing Information for an E3 Port	54-10
	Field Descriptions	54-12
	Viewing DS3/E3 Local Statistics	54-13
	Viewing DS3/E3 Local Total Statistics	54-13
	Field Descriptions	54-14
	Displayed Statistics	54-14
	Viewing DS3/E3 Local Current Statistics	54-15
	Viewing DS3/E3 Local Interval (Historical) Statistics	54-16

Viewing ATM Physical Layer Statistics for DS3 (CbitParity PLCP Sublayer) . . .	54-17
Status Definitions for DS3	54-18
Statistics Definitions for DS3	54-19
Viewing ATM Physical Layer Statistics for DS3 (CbitParity ADM Sublayer)	54-20
Viewing ATM Physical Layer Statistics for DS3 (M23 Type PLCP Sublayer)	54-21
Viewing ATM Physical Layer Statistics for DS3 (M23 Type ADM Sublayer)	54-22
Viewing ATM Physical Layer Statistics for E3 (G.751 PLCP Sublayer)	54-23
Status Definitions for E3 G.751 PLCP	54-24
Statistics Definitions for E3, PLCP G.751	54-24
Viewing ATM Physical Layer Statistics for E3 (G.751 ADM Sublayer)	54-25
Statistics Definitions for E3, ADM G.751	54-25
Viewing ATM Physical Layer Statistics for E3 (G.832 ADM Sublayer)	54-26
Status Definitions for G.832 ADM	54-26
Statistics definitions for E3, ADM G.832	54-27
Viewing ATM Physical Layer Interval Statistics for DS3 (CbitParity PLCP Sublayer)	54-28
Viewing ATM Physical Layer Interval Statistics for DS3 (CbitParity ADM Sublayer)	54-29
Viewing ATM Physical Layer Interval Statistics for DS3 (M23 Type PLCP Sublayer)	54-30
Viewing ATM Physical Layer Interval Statistics for DS3 (M23 Type ADM Sublayer)	54-31
Viewing ATM Physical Layer Interval Statistics for E3 (G.832 PLCP Sublayer)	54-32
Viewing ATM Physical Layer Interval Statistics for E3 (G.751 ADM Sublayer)	54-33
Clearing Interval Statistics	54-33
55 Backup Services	55-1
Introduction	55-1
Backup Services Commands	55-2
Accessing the Backup Services Menu	55-2
Adding a Backup Service	55-3
Adding a backup for a Physical Port	55-3
Field Descriptions	55-4
Backing Up a Frame Relay PVC	55-6
Modifying a Backup Service	55-9
Modifying a backup for a Physical Port	55-9
Modifying a Frame Relay PVC Backup Service	55-10
Viewing Backup Service(s) Configurations	55-11
Viewing the Configurations of All Backup Services	55-11
Viewing the Configuration of a Single Backup Service (bview Command)	55-11

Deleting a Backup Service	55-11
Viewing Backup Service Statistics	55-12
Clearing Backup Service Statistics	55-13
56 Managing Channelized DS3 Modules	56-1
Introduction	56-1
Digital Signal Level X (DSX)	56-2
Supported Physical Interfaces	56-3
BNC	56-3
Balanced T1	56-3
Supported Protocols	56-3
Application Examples	56-4
Internet Services Provider Point-of-Presence	56-4
Local Exchange Carrier's Central Office	56-5
Channelized DS3 Module	56-6
Channelized DS3 Module Technical Specifications	56-6
Channelized DS3 Module Configuration Overview	56-8
The Channelized DS3 Module Management Menu	56-10
Physical Configuration Commands	56-11
Logical Configuration Commands	56-12
Configuring a DS3 Port	56-14
Field Descriptions	56-14
Viewing Cumulative Statistics and Errors of a Local DS3 Port	56-17
Viewing Current 15-Minute Statistics and Errors of a Local DS3 Port	56-19
Viewing 15-Minute Interval (Historical) Statistics and Errors of a Local DS3 Port	56-20
Clearing Interval Statistics and Errors of a Local DS3 Port	56-22
Viewing Configuration and Statistical Parameters for a DS3 Port	56-22
Configuring a DS1 Channel	56-24
Field Descriptions	56-25
Setting DS1 Collection Statistics for a DS3 Port	56-26
Viewing Cumulative Statistics and Errors of a Local DS1 Channel	56-26
Field Descriptions	56-27
Viewing Current 15-Minute Statistics of a Local DS1 Channel	56-28
Viewing 15-Minute Interval Statistics and Errors of a Local DS1 Channel	56-29
Clearing Interval Statistics of a Local DS1 Channel	56-31
Viewing Configuration and Statistical Parameters for a DS1 Channel	56-32
Adding a Logical Port Configuration	56-33
Field Descriptions	56-34
Adding a Logical Port Configuration to a Clear Channel DS3 Port	56-36
Modifying a Logical Port Configuration	56-36
Field Descriptions	56-38
Deleting a Logical Port	56-39

Viewing Logical Port Configuration and Statistics	56-40
Field Descriptions	56-40
Clear Statistics for a Logical Port	56-42
Modify the Protocol Configuration of a Logical Port using PPP	56-43
Field Descriptions for Logical Port using PPP	56-44
Modify the Protocol Configuration of a Logical Port using Frame Relay	56-46
Field Descriptions for Logical Port using Frame Relay	56-47
Display Protocol Configuration and Statistics of a Logical Port using PPP	56-50
Field Descriptions for Logical Port Protocol using PPP	56-51
Display Protocol Configuration and Statistics of a Logical Port using Frame Relay	56-54
Field Descriptions for Logical Port Protocol using Frame Relay	56-55
Clear Protocol Statistics of a Logical Port	56-59
Add Frame Relay DLCI on a Logical Port	56-60
Field Descriptions	56-60
Delete Frame Relay DLCI on a Logical Port	56-61
Adding a Router Interface	56-62
Field Descriptions	56-62
Modifying a Router Interface Configuration	56-63
Deleting a Router Interface	56-63
Viewing Router Interfaces	56-64
Clearing Statistics for a Router Interface	56-64
Creating a Bridging or Trunking Service	56-65
Deleting Services	56-67
Viewing Service Configurations	56-67
Field descriptions	56-68
Modifying Service Configurations	56-69
Deleting the Module Configuration	56-70
57 Troubleshooting	57-1
Detecting Problems	57-1
Reporting Problems	57-3
Report Hardware Details	57-3
Report Software Details	57-4
Understanding Problems	57-5
Software Installation Problems	57-5
Operational Problems	57-6
Deadlocked VLAN	57-6
Probable Cause	57-7
Solution	57-7

Problems with IP Applications	57-7
Probable Cause	57-7
Solution	57-7
Protocol Problems	57-8
Probable Cause	57-8
Solution	57-8
Hardware Problems	57-9
LEDs Do Not Light on All Modules	57-9
Probable Cause	57-9
Solution	57-9
Amber Color in LEDs	57-9
Probable Cause	57-9
Solution	57-9
Non-Blinking OK2 LED	57-9
Probable Cause	57-9
Solution	57-9
TEMP LED is Amber	57-10
Solution	57-10
STA LED Is Off	57-10
Probable Cause	57-10
Solution	57-10
Cannot Use SLIP Line on an MPM	57-10
Probable Cause	57-10
Solution	57-10
Switch Does Not Boot When Flash File System Is Full and Trying To Create the mpm.cnf File	57-11
Probable Cause	57-11
Solution	57-11
Error Messages	57-12
Understanding Error Messages	57-12
Correcting Errors	57-12
Module Startup/Shutdown Error Messages	57-12
Serial Port Configuration Errors	57-13
Module Connection Errors	57-13
Chassis Error Messages	57-14
Chassis Error Messages Table	57-14
58 Running Hardware Diagnostics	58-1
Running Diagnostics	58-3
Login to Run Diagnostics	58-5
Resetting a Switching Module	58-6
Disabling a Switching Module	58-6
Temperature Masking	58-7

Running Hardware Diagnostics	58-8
Sample Command Lines	58-13
Halting Diagnostic Tests in Progress	58-13
Port Tests	58-13
OmniSwitch Port Test Wrap Cable/Plug Requirements	58-14
Sample Test Session: Ethernet Module	58-26
Displaying Available Diagnostic Tests	58-29
Configuring the Diagnostic Test Environment	58-30
Configuring Tests for Ethernet Modules	58-31
Configuring Tests for Token Ring Modules	58-32
Running Cell Fabric Tests on OmniSwitch CSMs	58-33
Running Frame Fabric Tests on Omni Switch/Routers	58-35
Running Diagnostics on an Entire Chassis	58-37
Diagnostic Test Cable Schematics	58-39
A The Boot Line Prompt	A-1
Entering the Boot Prompt	A-2
Boot Prompt Basics	A-3
Resuming Switch Boot (@)	A-3
Displaying Current Configuration (p)	A-4
Loading the Last Configured Boot File (l)	A-4
Listing Available Files in the Flash Memory (L)	A-5
Deleting All Files in the Flash Memory (P)	A-5
Deleting Specific Files in the Flash Memory (R)	A-5
Saving Configuration Changes (S)	A-6
Viewing Version Number (V)	A-6
Configuring a Switch with an MPX/MPM-C/MPM-III	A-7
Configuring a Switch with an MPM/MPM-II/MPM-1G	A-10
B Custom Cables	B-1
V.35 DTE Cable (For WSM-to-DCE Device Connection)	B-2
V.35 DCE Cable (For WSM-to-DTE Device Connection)	B-3
RS232 DTE Cable (For WSM-to-DCE Device Connection)	B-4
RS232 DCE Cable (For WSM-to-DTE Device Connection)	B-5
RS530 DTE Cable (For WSM-to-DCE Device Connection)	B-6
RS530 DCE Cable (For WSM-to-DTE Device Connection)	B-7
X.21 DTE Cable (For WSM-to-DCE Device Connection)	B-8
X.21 DCE Cable (For WSM-to-DTE Device Connection)	B-9
RS449 DTE Cable (For WSM-to-DCE Device Connection)	B-10
RS-449 DCE Cable Assembly (For WSM-to-DTE Device 75W Connection) . . .	B-11
RJ-45 to DB15F Cable Assembly (For T1/E1 Port 120W Connections)	B-12
RJ-45 to BNC Cable Assembly (For E1 75W Port Connections)	B-13

IndexI-1

1 Omni Switch/Router Chassis and Power Supplies

Alcatel's Omni Switch/Router (OmniS/R) is an advanced, multi-layer switching platform (Layer 2 and 3) that supports the most demanding switch requirements. With Omni Switch/Router, network administrators can replace aging FDDI or Fast Ethernet backbones with high capacity Gigabit Ethernet backbones.

◆ Important Notes ◆

Beginning with Release 4.4, FDDI is no longer supported.

Omni Switch/Router modules can be distinguished from older OmniSwitch modules by the **X** in the module name. For example, the ESM-100C-32W is an OmniSwitch module whereas the ES**X**-100C-32W is an Omni Switch/Router module.

Omni Switch/Router has a distributed switching fabric. In a 9-slot chassis operating at full duplex, Omni Switch/Router offers an aggregate 22 Gigabit per second (Gbps) distributed switching fabric. In addition, Omni Switch/Router offers new high density switching modules, including auto-sensing 10/100 Ethernet modules that offer high speed network connections to servers and desktops. (See *Omni Switch/Router Applications and Configurations* on page 1-5 for examples.)

The Omni Switch/Router Management Processor Module (MPX) module provides the core routing, VLAN MAC learning, SNMP, and file management functions for the entire Omni Switch/Router. In addition, the MPX has an Ethernet plug-in port for managing the switch. Only one MPX is required per Omni Switch/Router, but you can add another MPX for redundancy. See Chapter 2, "The Omni Switch/Router MPX," for more information on the MPX.

◆ Important Note ◆

Omni Switch/Router switching modules require an MPX. You cannot install any version of the MPM (i.e., MPM-C, MPM 1G, MPM II, or original MPM) in a chassis with an MPX.

An Omni Switch/Router Hardware Routing Engine (HRE-X). The HRE-X offers high-speed Layer 3 switching from 1.5 to 12.0 million packets per second (Mpps) in a fully loaded chassis. See *The Omni Switch/Router Hardware Routing Engine (HRE-X)* on page 1-26 for more information on the HRE-X.

Omni Switch/Router switching modules perform software filtering, translations between dissimilar network interfaces, and hardware-based switching. Omni Switch/Router switching modules have an additional on-board interface connector for the HRE-X.

Currently, Omni Switch/Router switching modules consist of Gigabit Ethernet modules, auto-sensing Ethernet modules, Fast 10/100 Ethernet modules, 10 Mbps Ethernet modules, Token Ring modules, ATM uplink modules, WAN modules, Packets Over SONET, and Voice Over IP (VOIP) modules. See Chapter 3, “Omni Switch/Router Switching Modules,” for documentation.

◆ **Important Note** ◆

Omni Switch/Router modules require the use of an Omni Switch/Router chassis (see *Omni Switch/Router Chassis and Power Supplies* on page 1-7). Do *not* install an Omni Switch/Router module in an OmniSwitch chassis and do *not* install an OmniSwitch module in an Omni Switch/Router chassis.

Omni Switch/Router User Interface (UI) Software

Omni Switch/Router hardware uses the same User Interface (UI) commands and Network Management Software (NMS) as OmniSwitch hardware. Omni Switch/Router modules support broadcast management, multicast management, any-to-any switching, virtual LANs (VLANs), firewalls, user authentication, WAN access, and policy-based configuration.

◆ **Important Note** ◆

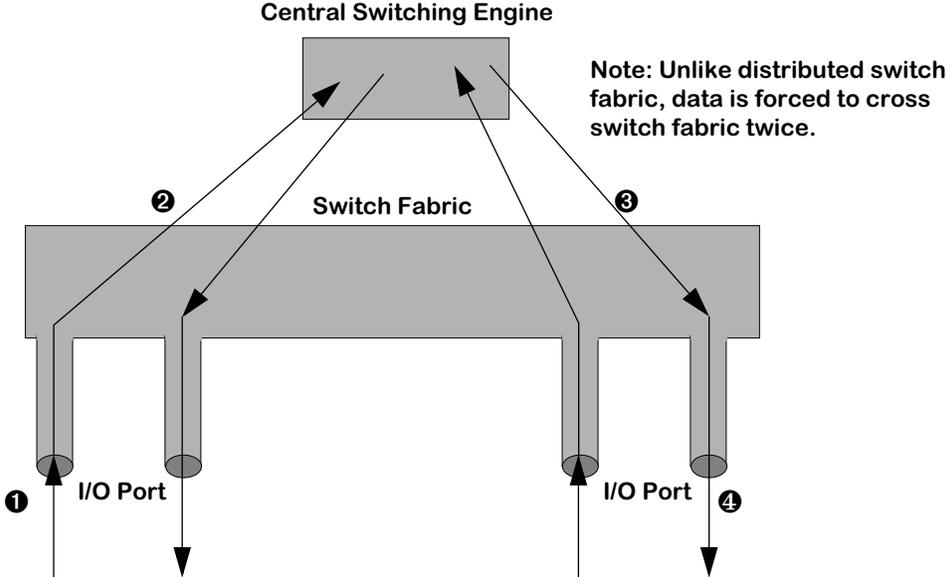
In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. Chapter 8, “The User Interface,” includes documentation on changing from CLI mode to UI mode.

Omni Switch/Router Network Management Software (NMS)

You need Release 3.4, or higher, of Alcatel’s X-Vision Network Management Software (NMS) to operate with Omni Switch/Router hardware.

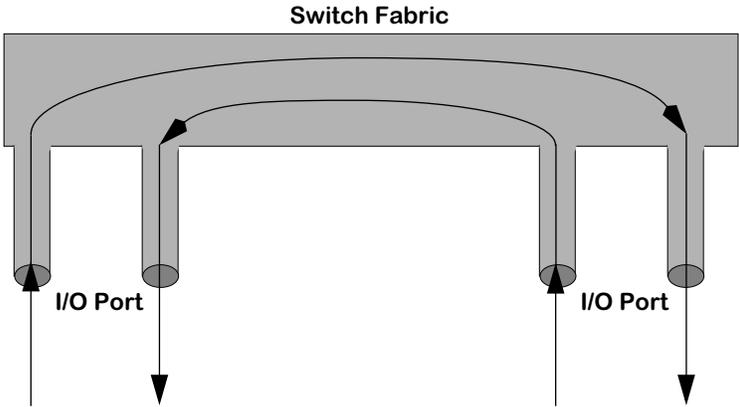
Omni Switch/Router Distributed Switching Fabric

Many switches in the market employ a shared memory architecture, which uses a central switching engine to send data to the appropriate port. As shown in the figure below, data enters the input port (1 below), crosses the switching fabric on its way to the central switching engine(2 below), and *again* crosses the switching fabric (3 below) before exiting the appropriate output port (4 below).



Traditional Shared Memory Architecture

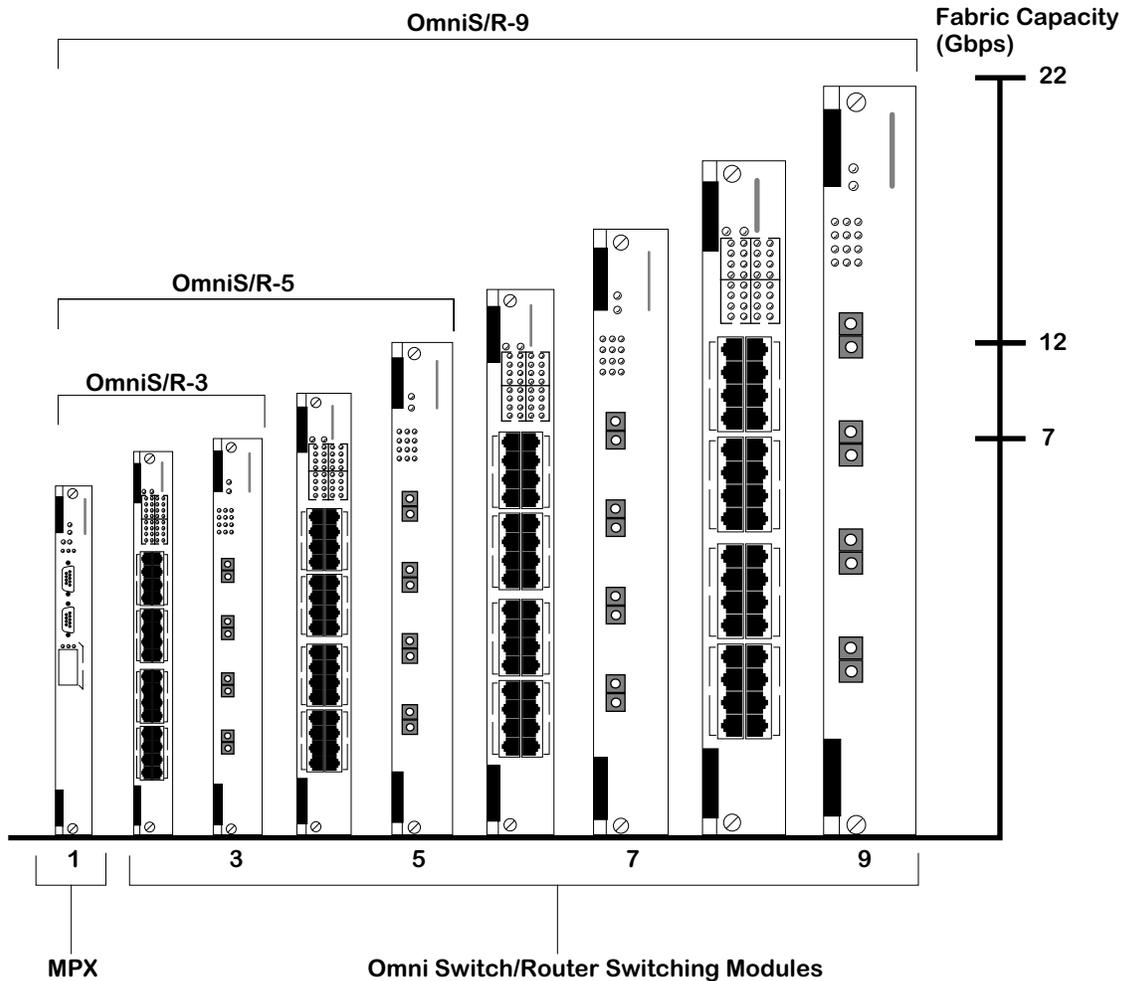
In contrast, Omni Switch/Router switches use a distributed switching fabric. As shown in the figure below, data enters the input port and crosses the switching fabric *only once* before exiting the appropriate output port. Compared to the shared memory architecture, only half as much bandwidth is required since data just crosses the switching fabric once.



Omni Switch/Router Distributed Switching Fabric

Omni Switch/Router Fabric Capacity

In a chassis with Omni Switch/Router modules only, each Omni Switch/Router module provides 2.4 Gbps of switching capacity in full-duplex mode. In a chassis with all Omni Switch/Router modules, the Omni Switch/Router architecture provides up to a 22 Gbps distributed switching fabric. As shown in the figure below, an OmniS/R-9 with an MPX and eight (8) Omni Switch/Router switching modules provides 22 Gbps of switching capacity. An OmniS/R-5 with an MPX and four (4) Omni Switch/Router switching modules provides 12 Gbps of switching capacity, while an OmniS/R-3 with an MPX and two (2) Omni Switch/Router switching modules provides 7 Gbps of switching capacity.



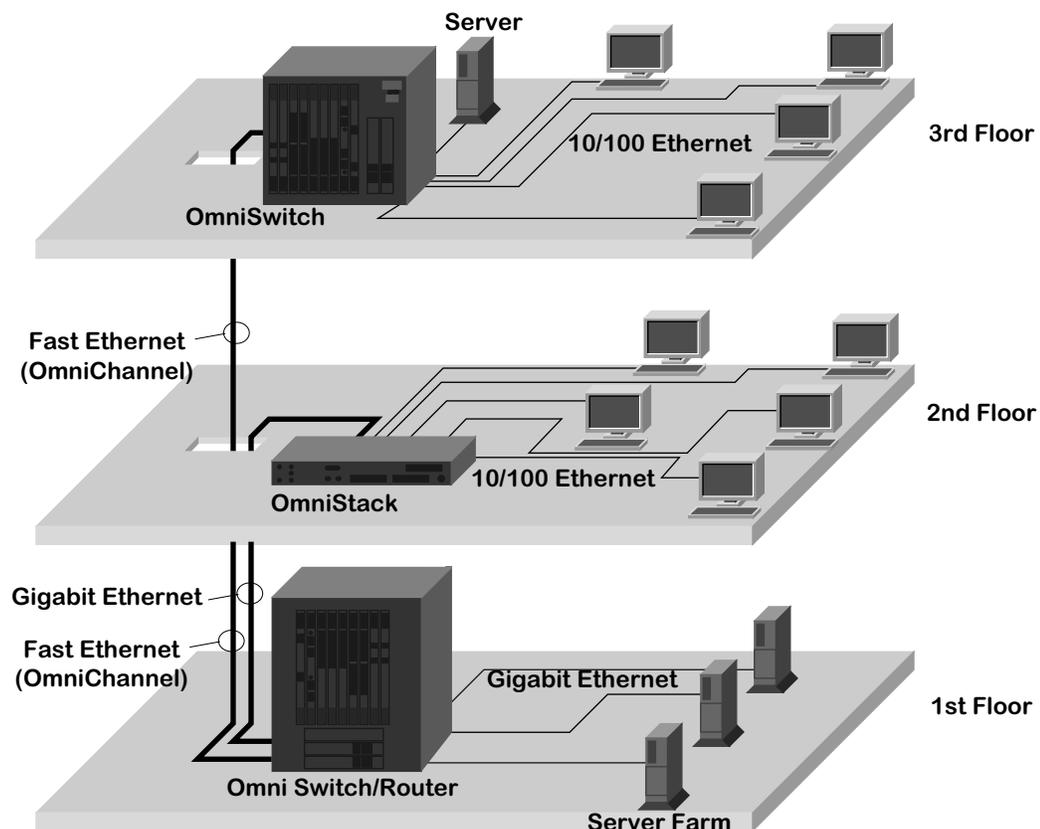
Omni Switch/Router Fabric Capacity in OmniS/R-3, OmniS/R-5 and OmniS/R-9 Chassis

Omni Switch/Router Applications and Configurations

Omni Switch/Router hardware is ideally suited to meet the most demanding server and backbone needs. In addition, Omni Switch/Router hardware can be integrated easily with OmniSwitches and with OmniStack workgroup switches. The examples that follow show how the Omni Switch/Router can be used as a network backbone and as the central switch/router in a wiring closet.

Omni Switch/Router as the Backbone Connecting Several Networks

The figure below shows how Omni Switch/Router Gigabit Ethernet and 10/100 Ethernet modules can be used as a network backbone. In this example, two networks on two different floors need high speed access to a server farm on the first floor.

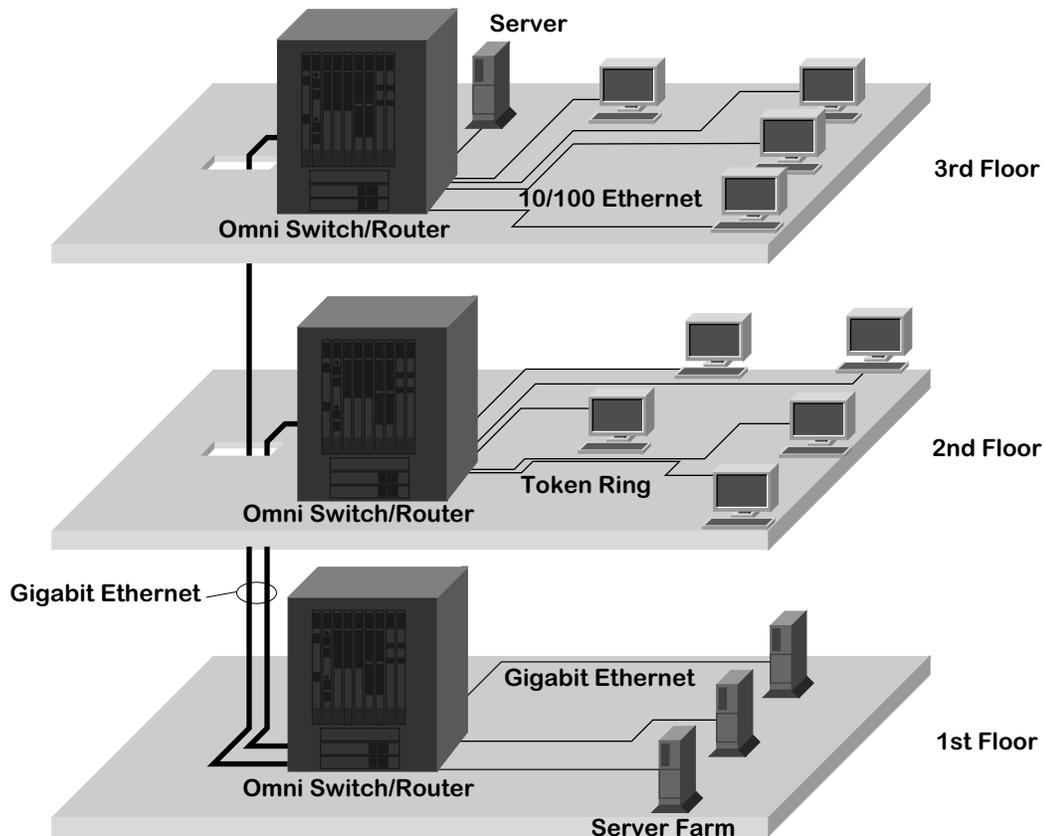


Using Omni Switch/Router in a Network Backbone

The servers each have dedicated Gigabit Ethernet connections to Omni Switch/Router modules on the first floor. The Omni Switch/Router chassis on the first floor is connected to the network on the second floor via a Gigabit Ethernet link to the OmniStack on the second floor. The Omni Switch/Router chassis on the first floor is connected via a 10/100 Ethernet link, using OmniChannel, to the OmniSwitch chassis on the third floor containing a Fast Ethernet module, such as the ESM-100C-12. See Chapter 19, “Managing Ethernet Modules,” for more information on OmniChannel.

Omni Switch/Router as the Central Backbone Switch/Router and in the Wiring Closet

The figure below shows Omni Switch/Router chassis used in the wiring closet and as a network backbone switch/router connecting the wiring closets and server farm. On the third floor, an Omni Switch/Router chassis connects a mixture of 10BaseT and 100BaseTx workstations with an auto-sensing Ethernet module. In addition, this Omni Switch/Router chassis connects the workstations to a local server with a Gigabit Ethernet module. On the second floor, an Omni Switch/Router connects legacy Token Ring workstations. On the first floor, the Omni Switch/Router connects the networks on the upper floors to the server farm using a Gigabit Ethernet module.



Using Omni Switch/Router in the Wiring Closet

Omni Switch/Router Chassis and Power Supplies

The Omni Switch/Router chassis houses the MPX, switching modules, and one or two power supplies. The modular design of the chassis provides the ability to configure your Omni Switch/Router to meet your networking needs. The Omni Switch/Router chassis also offer such failure resistant features as redundant MPXs, redundant power supplies, and hot swapping of switching modules. (See Chapter 7, “OmniSwitch Switching Modules,” for more information on hot swapping switching modules.)

There are three (3) different versions of the Omni Switch/Router chassis. The OmniS/R-3, a three-slot version, is documented in *OmniS/R-3* on page 1-8. The OmniS/R-5, a five-slot version, is documented in *OmniS/R-5* on page 1-10. A nine-slot version called the OmniS/R-9 is documented in *OmniS/R-9 and OmniS/R-9P* on page 1-13. The OmniS/R-3, OmniS/R-5 and OmniS/R-9 chassis, the MPX module, and several switching modules have met FCC Class B requirements.

◆ Note ◆

In the current release, a maximum of seven (7) 32-port switching modules (e.g., ESX-100C-32W) is supported in 9-slot Omni Switch/Router chassis.

Slot 1 is reserved for the MPX; you *cannot* install a switching module in Slot 1. You can install a switching module in Slot 2 (if an MPX is installed in Slot 1) or an MPX. When dual-redundant MPXs are installed, one of them must be installed in Slot 1 and the other in Slot 2. On the OmniS/R-3, Slot 3 is reserved for a switching module. On the OmniS/R-5, Slots 3 through 5 are reserved for switching modules. On the OmniS/R-9, Slots 3 through 9 are reserved for switching modules.

◆ Important Note ◆

You *must* have an MPX acting as the management module; you cannot use any version of the MPM.

Warning

If you have any empty switching module slots in either an OmniS/R-3 (3-slot) or OmniS/R-5 (5-slot) chassis, you *must* cover them with blank panels (available from Alcatel) to prevent your chassis from overheating.

Covering empty slots forces air to flow directly over the power supplies, thereby cooling them. If the power supplies are not properly cooled, they will overheat and shut down.

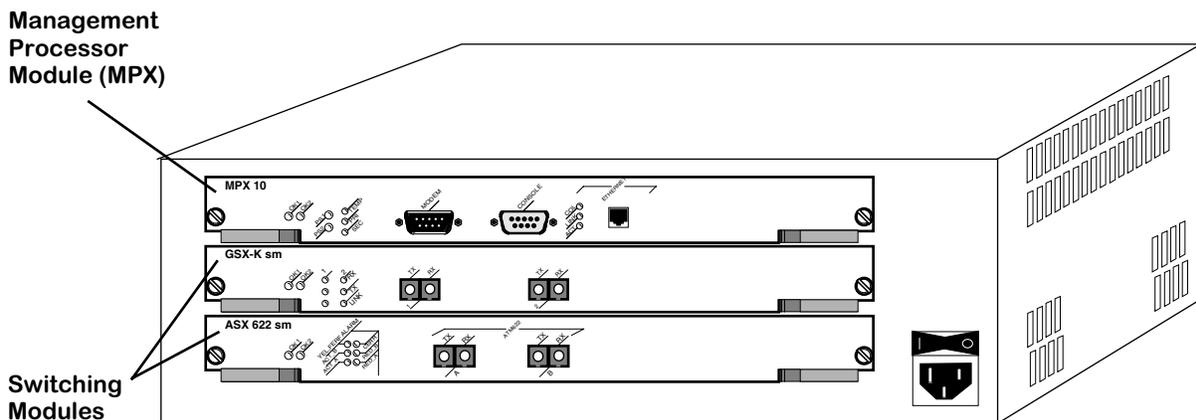
OmniS/R-3

The OmniS/R-3 chassis features three slots for an MPX and specific switching modules (contact your Alcatel sales representative for information on module availability). Slots are numbered from 1 to 3 starting with the topmost slot. A built-in power supply is located on the right side of the chassis, and a fan cooling system is located on the left side of the chassis. The chassis can be rack-mounted. You can view all cabling, power supplies, module interfaces, and LEDs at the front of the chassis.

The OmniS/R-3 uses a built-in AC power supply that has a capacity of 32.8 Amps at 5 volts and 3 amps at 12 volts for 200 Watts of output power. The OmniS/R-3 does not support a Backup Power Supply (BPS).

◆ Caution ◆

Do not connect the power connector on the back of the OmniS/R-3 to data communication equipment.



OmniS/R-3 Chassis

◆ Important Note ◆

Slot 1 (the top slot) on the OmniS/R-3 is reserved for an MPX module. Slot 2 can accommodate either a second (optional) MPX module or a Switching module. Slot 3 (the bottom slot) is reserved for a Switching module. Contact your Alcatel sales representative for information regarding module availability.

OmniS/R-3 Chassis Technical Specifications	
Total Module Slots	3
Total Slots for Switching Modules	2
Physical Dimensions	5.25" (13.34 cm) high, 17.13" (43.51 cm) wide, 13.00" (33.02 cm) deep
Weight	18 lb. (8.18 kg), fully populated with modules and power supplies.
Switching Backplane	Up to 7 Gbps (aggregate) switching fabric capacity
Voltage Range	85-270 VAC, 47 to 63 Hz, auto-ranging and auto-sensing
Current Draw	3.8 Amps at 100/115 VAC 1.7 Amps at 230 VAC
Watts (Output)	200
Current Provided	32.8 Amps at +5 Volts 3 Amps at +12 Volts
Heat Generation	Approximately 1020 BTUs per hour
Temperature Operating Range	0 to 45 degrees Celsius 32 to 113 degrees Fahrenheit
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Altitude	Sea level to 10,000 feet (3 km)
Agency Listings	UL 1950 CSA-C22.2 EN60950 FCC Part 15, Subpart B (Class A) EN55022, 1987/EN50081 FCC Class B C.I.S.P.R. 22: 1985 EN50082-1, 1992 IEC 801-2, 1991 IEC 801-3, 1984 IEC 801-4, 1988 VCCI V-3/94.04 (Class A & Class B) EN 61000-4-2: 1995 EN 61000-4-3: 1995 EN 61000-4-4: 1995 EN 61000-4-5: 1995 EN 61000-4-6: 1996 EN 61000-4-8: 1993 EN 61000-4-11: 1994 ENV 50204: 1996

OmniS/R-5

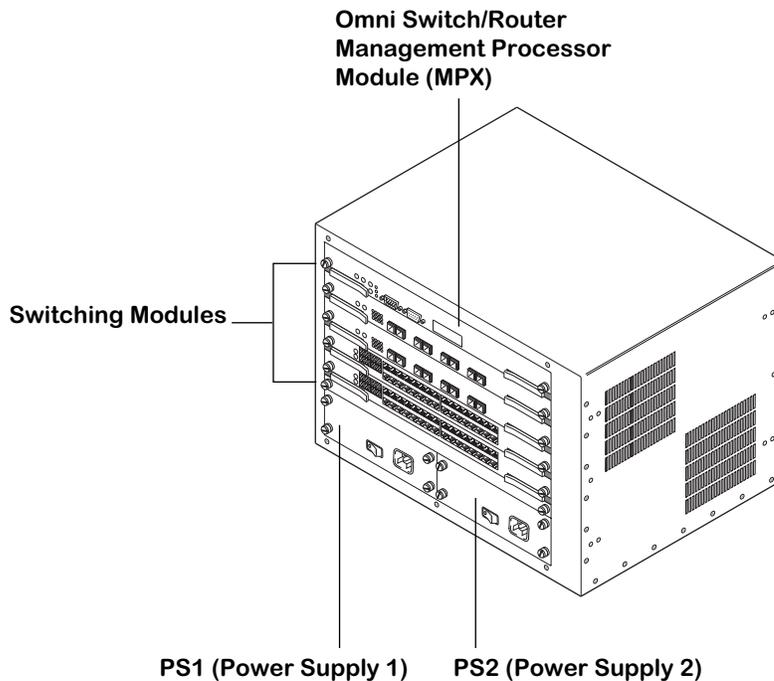
The OmniS/R-5 chassis has five slots for an MPX and switching modules (see figure below). Slots are numbered from 1 to 5 starting with the topmost slot. Slots for two power supplies are located at the bottom of the chassis.

◆ Warning ◆

If you have an OmniS/R-5 with a single power supply, do *not* remove the cover on the empty power supply slot. In addition, if you have any empty switching module slots in an OmniS/R-5, you *must* cover them with blank panels (available from Alcatel) to prevent your chassis from overheating.

Covering empty slots forces air to flow directly over the power supplies, thereby cooling them. If the power supplies are not properly cooled, they will overheat and shut down.

The entire chassis can be wall-mounted or rack-mounted. You can view all cabling, power supplies, module interfaces, and LEDs at the front of the chassis.



The OmniS/R-5

The OmniS/R-5 uses the MPX. Slot 1 is reserved for the MPX; you *cannot* install a switching module in Slot 1. You can install a switching module in Slot 2 (if an MPX is installed in Slot 1) or an MPX. When dual-redundant MPXs are installed, one of them must be installed in Slot 1 and the other in Slot 2. Slots 3 through 5 are reserved for switching modules.

The OmniS/R-5 provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to the operation. See Chapter 5, “OmniSwitch Power Supplies,” for more information on installing and removing power supplies. See *OmniS/R-5 Technical Specifications* on page 1-12 for more information.

The OmniS/R-5 uses one of the following power supplies:

OmniS/R-PS5-375 The standard power supply. It can provide 375 Watts of power.

OmniS/R-PS5-DC375 A -48 volt (input voltage) DC version of the OmniS/R-PS5-375 power supply. This power supply can provide 375 Watts of power. It requires the use of 12 to 14 gauge wire for connections to the DC power source. See *Connecting a DC Power Source to an OmniS/R-PS5-DC375* on page 1-28 for more information.

◆ Caution ◆

This unit may be equipped with two power connections. To reduce the risk of electrical shock, disconnect both power connections before servicing the unit.

◆ VORSICHT ◆

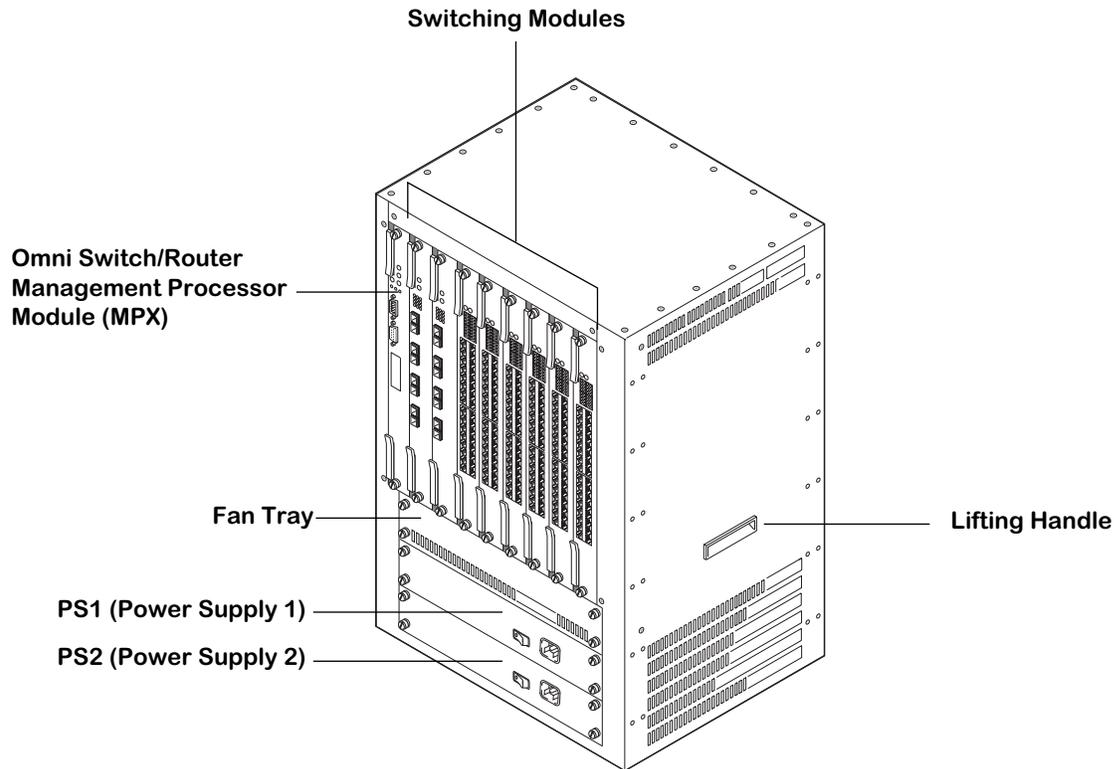
Das Gerät kann mit zwei Netzanschlüssen ausgestattet sein. Um einen elektrischen Schlag zu vermeiden, immer beide Anschlüsse vor der Wartung vom Netz trennen.

Omni Switch/Router Chassis and Power Supplies

OmniS/R-5 Technical Specifications	
Total Module Slots	5
Total Slots for Switching Modules	4
Physical Dimensions	12.25" (31.12 cm) high, 17.14" (43.54 cm) wide, 13" (33.02 cm) deep
Weight	approximately 55 lb. (24.09 kg), fully populated with modules and power supplies.
Switching Backplane	Up to 12 Gbps (aggregate) switching fabric capacity
Voltage Range	90-265 VAC, 47 to 63 Hz auto-ranging and auto-sensing.
Current Draw	6 Amps at 100/115 VAC; 3 Amps at 230 VAC
Watts (Output)	375
Current Provided	60 Amps at 5 Volts (V1) 5 Amps at 12 Volts (V2) 3 Amps at 3.3 Volts (V3) 5.1 Amps at 1.5 Volts (V4)
Temperature Operating Range	0 to 45 degrees Celsius 32 to 113 degrees Fahrenheit
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Altitude	Sea level to 10,000 feet (3 km)
Heat Generation	1280 BTUs per hour (one power supply)
Agency Listings	UL 1950 CSA-C22.2 EN60950 FCC Part 15, Subpart B (Class A) EN55022, 1987/EN50081 FCC Class B C.I.S.P.R. 22: 1985 EN50082-1, 1992 IEC 801-2, 1991 IEC 801-3, 1984 IEC 801-4, 1988 VCCI V-3/94.04 (Class A & Class B) EN 61000-4-2: 1995 EN 61000-4-3: 1995 EN 61000-4-4: 1995 EN 61000-4-5: 1995 EN 61000-4-6: 1996 EN 61000-4-8: 1993 EN 61000-4-11: 1994 ENV 50204: 1996

OmniS/R-9 and OmniS/R-9P

The OmniS/R-9 and OmniS/R-9P chassis have nine slots for an MPX and switching modules (see figure below). Slots are numbered from 1 to 9 starting with the left-most slot. Slots for two power supplies are located at the bottom of the chassis. A separate, removable fan tray containing four fans is located above the power supply module bays.



The OmniS/R-9

A fully loaded OmniS/R-9 weighs nearly 100 lbs. Therefore, it is recommended that if you are rack-mounting the chassis you use a rack mount shelf instead of just brackets. Using a shelf will ensure that the weight of the chassis can be supported. In addition, the OmniS/R-9 contains side handles to make lifting and installation easier.

The OmniS/R-9 uses the MPX. Slot 1 is reserved for the MPX; you *cannot* install a switching module in Slot 1. You can install a switching module in Slot 2 (if an MPX is installed in Slot 1) or an MPX. When dual-redundant MPXs are installed, one of them must be installed in Slot 1 and the other in Slot 2. Slots 3 through 9 are reserved for switching modules.

◆ Important Note ◆

You *must* have an MPX acting as the management module; you cannot use any version of the MPM. See Chapter 2, “The Omni Switch/Router MPX,” for more information on the MPX.

The OmniS/R-9 and OmniS/R-9P provide bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to the operation. See Chapter 5, “OmniSwitch Power Supplies,” for additional information on installing and removing power supplies.

The OmniS/R-9 uses the following power supply:

OmniS/R-PS9-650 The standard power supply. It can provide 650 Watts of power.

The OmniS/R-9P uses the following power supply:

OmniS/R-PS9-725 This power supply can provide 725 Watts of power.

The OmniS/R-9P-48V uses the following power supply:

OmniS/R-PS9-DC725 A -48 Volt (input voltage) DC version of the OmniS/R-PS9-725 power supply. This power supply can provide 725 Watts of power. It requires the use of 12 to 14 gauge wire for connections to the DC power source. See *Connecting a DC Power Source to an OmniS/R-PS9-DC725* on page 1-31 for more information.

For additional information, see *OmniS/R-9 Technical Specifications* on page 1-15, *OmniS/R-9P Technical Specifications* on page 1-16 and *OmniS/R-9P-48V Technical Specifications* on page 1-17.

◆ Caution ◆

This unit may be equipped with two power connections. To reduce the risk of electrical shock, disconnect both power connections before servicing the unit.

◆ VORSICHT ◆

Das Gerät kann mit zwei Netzanschlüssen ausgestattet sein. Um einen elektrischen Schlag zu vermeiden, immer beide Anschlüsse vor der Wartung vom Netz trennen.

OmniS/R-9 Technical Specifications	
Total Module Slots	9
Total Slots for Switching Modules	8
Physical Dimensions	24.50" (62.23 cm) high, 16.60" (42.16 cm) wide, 13.25" (36.66 cm) deep
Weight	96 lb. (43.55 kg), fully populated with modules and power supplies.
Switching Backplane	Up to 22 Gbps (aggregate) switching fabric capacity
Voltage Range	90-264 VAC, 47 to 63 Hz
Current Draw	12 Amps at 100/115 VAC; 6 Amps at 230 VAC
Watts (Output)	650
Current Provided	120 Amps at 5 Volts 4 Amps at 12 Volts 6 Amps at 3.3 Volts 8 Amps at 1.5 Volts
Temperature Operating Range	0 to 45 degrees Celsius 32 to 113 degrees Fahrenheit
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Altitude	Sea level to 10,000 feet (3 km)
Heat Generation	2219 BTUs per hour (one power supply)
Agency Listings	UL 1950 CSA-C22.2 EN60950 FCC Part 15, Subpart B (Class A) EN55022, 1987/EN50081 FCC Class B C.I.S.P.R. 22: 1985 EN50082-1, 1992 IEC 801-2, 1991 IEC 801-3, 1984 IEC 801-4, 1988 VCCI V-3/94.04 (Class A & Class B) EN 61000-4-2: 1995 EN 61000-4-3: 1995 EN 61000-4-4: 1995 EN 61000-4-5: 1995 EN 61000-4-6: 1996 EN 61000-4-8: 1993 EN 61000-4-11: 1994 ENV 50204: 1996

OmniS/R-9P Technical Specifications	
Total Module Slots	9
Total Slots for Switching Modules	8
Physical Dimensions	24.50" (62.23 cm) high, 16.60" (42.16 cm) wide, 13.25" (36.66 cm) deep
Weight	96 lb. (43.55 kg), fully populated with modules and power supplies.
Switching Backplane	Up to 22 Gbps (aggregate) switching fabric capacity
Voltage Range	85-270 VAC, 47 to 63 Hz
Current Draw	12 Amps at 100/115 VAC; 6 Amps at 230 VAC
Watts (Output)	725
Current Provided	120 Amps at 5 Volts 6 Amps at 12 Volts 6 Amps at 3.3 Volts 8 Amps at 1.5 Volts
Temperature Operating Range	0 to 70 degrees Celsius 32 to 158 degrees Fahrenheit
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Altitude	Sea level to 10,000 feet (3 km)
Heat Generation	2219 BTUs per hour (one power supply)
Agency Listings	UL 1950; CSA-C22.2 #950-M90; TUV EN60950; CB Certification IEC 950; FCC Title 47 CRF Part 15, Subpart B (Class A & Class B); IEC EN55022, 1995 (Class A & Class B) CISPR 22, 1995; IEC 1000-3-2; IEC 1000-3-3 (EN60555-2); IEC 1000-4-2 (EN61000-4-2, per EN50082-1, 1992); IEC 1000-4-3 (EN61000-4-3, per EN50082-1, 1992); IEC 1000-4-4 (EN61000-4-4) Level 4; IEC 1000-4-5 (EN61000-4-5) Level 4; IEC 1000-4-6 (EN61000-4-6); IEC 1000-4-8 (EN61000-4-8); IEC 1000-4-11 (EN61000-4-11); EN50204: 1996.

OmniS/R-9P-48V Technical Specifications	
Total Module Slots	9
Total Slots for Switching Modules	8
Physical Dimensions	24.50" (62.23 cm) high, 16.60" (42.16 cm) wide, 13.25" (36.66 cm) deep
Weight	96 lb. (43.55 kg), fully populated with modules and power supplies.
Switching Backplane	Up to 22 Gbps (aggregate) switching fabric capacity
Voltage Range	40-60 VDC
Current Draw	23 Amps
Watts (Output)	725
Current Provided	120 Amps at 5.15 VDC 6 Amps at 12 VDC 6 Amps at 3.3 VDC 8 Amps at 1.5 VDC
Temperature Operating Range	0 to 70 degrees Celsius 32 to 158 degrees Fahrenheit
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Altitude	Sea level to 10,000 feet (3 km)
Heat Generation	2219 BTUs per hour (one power supply)
Agency Listings	UL 1950; CSA-C22.2 #950-M90; TUV EN60950; CB Certification IEC 950; FCC Title 47 CRF Part 15, Subpart B (Class A & Class B); IEC EN55022, 1995 (Class A & Class B) CISPR 22, 1995; IEC 1000-3-2; IEC 1000-3-3 (EN60555-2); IEC 1000-4-2 (EN61000-4-2, per EN50082-1, 1992); EN55024 IEC 1000-4-3 (EN61000-4-3, per EN50082-1, 1992); IEC 1000-4-4 (EN61000-4-4) Level 4; IEC 1000-4-5 (EN61000-4-5) Level 4; IEC 1000-4-6 (EN61000-4-6); IEC 1000-4-8 (EN61000-4-8); IEC 1000-4-11 (EN61000-4-11); ENV 50204: 1996.

Omni Switch/Router Power Requirements

Always make sure that the total power requirements of the modules in your chassis do not exceed the limits of your power supply. To check the power consumption of your configuration, refer to the tables on the following pages and add up the **DC Current Draw** of all modules in your switch. The tables beginning on page 1-19 list modules *without* an HRE-X and the tables beginning on page 1-22 list modules *with* an HRE-X.

The total power consumption of all your modules should be below the current provided by your power supply, which is listed in *OmniS/R-3* on page 1-8 for the OmniS/R-3, *OmniS/R-5* on page 1-10 for the OmniS/R-5 and *OmniS/R-9 and OmniS/R-9P* on page 1-13 for the OmniS/R-9 and OmniS/R-9P. For power consumption and FCC compliance information for Omni Switch/Router VoIP modules, consult your *VoIP User Manual*.

◆ Caution ◆

It is possible, but *not recommended*, to have a configuration in which the current draw of the installed modules exceeds the power provided by a single power supply. However, such a configuration would *require two power supplies and would not allow you to have power redundancy*.

Module Power Requirements *without* an HRE-X

Module	Description	DC Current Draw (Amps)	FCC Class Approval
MPX	Management Processor Module.	3.75	B
ASX-155FM/FS/FH-1W	ATM 155 Mbps (OC-3) with one (1) fiber SC port.	5.25	B
ASX-155FM/FS/FH-2W	ATM 155 Mbps (OC-3) with two (2) fiber SC ports.	6.25	B
ASX-155RFM/RFS-1W	ATM 155 Mbps (OC-3) with one (1) redundant fiber SC port.	5.75	B
ASX-622RFM/RFS-1W	ATM 622 Mbps (OC-12) with one (1) redundant fiber SC port.	11.0	B
ASX-D3-1W	ATM with one (1) DS3 port	5.75	B
ASX-D3-2W	ATM with two (2) DS3 ports.	7.25	B
ASX-E3-1W	ATM with one (1) E3 port	5.75	B
ASX-E3-2W	ATM with two (2) E3 port	7.25	B
ESX-100C-12W	Auto-Sensing 10/100 Ethernet module with twelve (12) copper RJ-45 ports.	5.75	B (STP cable) A (UTP cable)
ESX-100C-32W	Auto-Sensing 10/100 Ethernet module with thirty-two (32) RJ-45 ports.	11.25	B (STP cable) A (UTP cable)
ESX-K-100C-32W	Advanced auto-Sensing 10/100 Ethernet module with thirty-two (32) RJ-45 ports.	10.25	B
ESX-100FM/FS-12W	Fast Ethernet (100 Mbps) module with twelve (12) fiber MT-RJ ports.	10.0	B
ESX-K-100FM/FS-16W	Advanced Fast Ethernet (100 Mbps) module with sixteen (16) fiber MT-RJ ports.	9.75	B
ESX-FM-24W	10 Mbps Ethernet module with twenty-four (24) fiber VF-45 ports	13.0	B

continued on next page...

Module Power Requirements *without* an HRE-X (continued)

Module	Description	DC Current Draw (Amps)	FCC Class Approval
GSX-FM/FS/FH-2W	Gigabit Ethernet module with two (2) fiber SC ports.	6.75	B
GSX-K-FM/FS-2W	Advanced Gigabit Ethernet module with two (2) fiber SC ports.	5.25	B (STP cable) A (UTP cable)
GSX-FM/FS-4W	Gigabit Ethernet module with four (4) fiber SC ports.	10.0	B
TSX-C-32W	Token Ring (Lobe Only) with thirty-two (32) copper RJ-45 ports.	9.25	B (STP cable) A (UTP cable)
TSX-CD-16W	Token Ring (Station/Lobe) with sixteen (16) copper RJ-45 ports.	7.0	B (STP cable) A (UTP cable)

continued on next page...

Module Power Requirements *without* an HRE-X (continued)

Module	Description	DC Current Draw (Amps)	FCC Class Approval
WSX-S-2W	WAN module with 2 serial ports	4.75	B
WSX-SC-4W	WAN module with 4 serial ports	6.25	B
WSX-SC-8W	WAN module with 8 serial ports	8.25	B
WSX-BRI-SC-1W	WAN ISDN module with 1 serial and 1 BRI port	5.75	B
WSX-BRI-SC-2W	WAN ISDN module with 2 serial and 2 BRI ports	7.25	B
WSX-FT1-SC-1W	WAN module with 1 serial and 1 T1 or E1 port	5.75	A
WSX-FE1-SC-1W	WAN module with 1 serial and 1 T1 or E1 port	5.75	B
WSX-FT1-SC-2W	WAN module with 2 serial and 2 T1 or E1 ports	7.25	B
WSX-FE1-SC-2W	WAN module with 2 serial and 2 T1 or E1 ports	7.25	B
WSX-M013-2W	WAN module with 2 channelized DS3 ports.	6.5	B
WSX-M013-4W	WAN module with 4 channelized DS3 ports.	8.5	B

Module Power Requirements *with* an HRE-X

Module	Description	DC Current Draw (Amps)	FCC Class Approval
MPX-L3	Management Processor Module.	5.25	B
ASX-155FM/FS/FH-1W-L3	ATM 155 Mbps (OC-3) with one (1) fiber SC port.	6.75	B
ASX-155FM/FS/FH-2W-L3	ATM 155 Mbps (OC-3) with two (1) fiber SC ports.	7.75	B
ASX-155RFM/RFS-1W-L3	ATM 155 Mbps (OC-3) with one (1) redundant fiber SC port.	7.25	B
ASX-155RFM/RFS-2W-L3	ATM 155 Mbps (OC-3) with two (2) redundant fiber SC port.	8.75	B
ASX-622RFM/RFS-1W-L3	ATM 622 Mbps (OC-12) with one (1) redundant fiber SC port.	12.5	B
ASX-D3-1W-L3	ATM with one (1) DS3 port	7.25	B
ASX-D3-2W-L3	ATM with two (2) DS3 port	8.75	B
ASX-E3-1W-L3	ATM with one (1) E3 port	7.25	B
ASX-E3-1W-L3	ATM with one (1) E3 port	8.75	B
ESX-100C-12W-L3	Auto-Sensing 10/100 Ethernet module with twelve (12) copper RJ-45 ports.	7.25	B (STP cable) A (UTP cable)
ESX-100C-32W-L3	Auto-Sensing 10/100 Ethernet module with thirty-two (32) RJ-45 ports.	12.75	B (STP cable) A (UTP cable)
ESX-K-100C-32W-L3	Advanced auto-Sensing 10/100 Ethernet module with thirty-two (32) RJ-45 ports.	11.75	B
ESX-100FM/FS-12W-L3	Fast Ethernet (100 Mbps) module with twelve (12) fiber MT-RJ ports.	11.5	B
ESX-FM-24W-L3	10 Mbps Ethernet module with twenty-four (24) fiber VF-45 ports	14.5	B
ESX-K-100FM/FS-16W-L3	Advanced Fast Ethernet (100 Mbps) module with sixteen (16) fiber MT-RJ ports.	11.25	B

continued on next page...

Module Power Requirements *with* an HRE-X (continued)

Module	Description	DC Current Draw (Amps)	FCC Class Approval
GSX-FM/FS/FH-2W-L3	Gigabit Ethernet module with two (2) fiber SC ports.	8.25	B
GSX-K-FM/FS-2W-L3	Advanced Gigabit Ethernet module with two (2) fiber SC ports.	6.75	B (STP cable) A (UTP cable)
GSX-FM/FS-4W-L3	Gigabit Ethernet module with four (4) fiber SC ports.	11.5	B
TSX-C-32W-L3	Token Ring (Lobe Only) with thirty-two (32) copper RJ-45 ports.	10.75	B (STP cable) A (UTP cable)
TSX-CD-16W-L3	Token Ring (Station/Lobe) with sixteen (16) copper RJ-45 ports.	8.5	A

continued on next page...

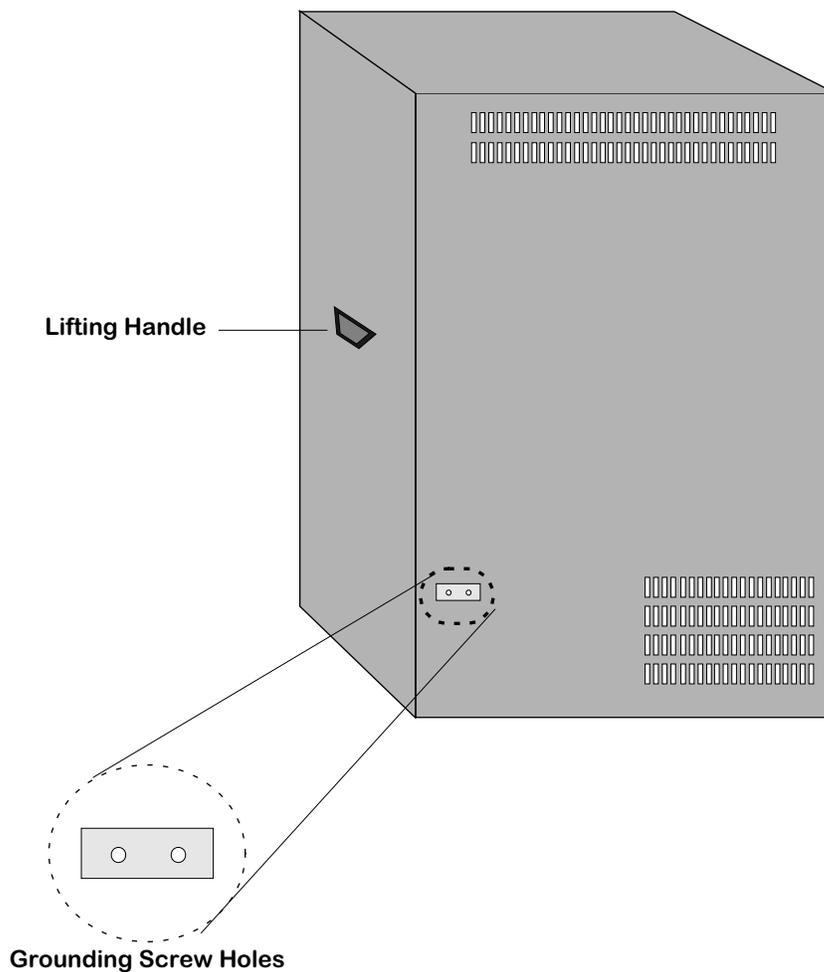
Module Power Requirements *with* an HRE-X (continued)

Module	Description	DC Current Draw (Amps)	FCC Class Approval
WSX-S-2W-L3	WAN module with 2 serial ports	6.25	B (STP cable) A (UTP cable)
WSX-SC-4W-L3	WAN module with 4 serial ports	7.75	B (STP cable) A (UTP cable)
WSX-SC-8W-L3	WAN module with 8 serial ports	9.75	B (STP cable) A (UTP cable)
WSX-BRI-SC-1W-L3	WAN ISDN module with 1 serial and 1 BRI port	7.25	B (STP cable) A (UTP cable)
WSX-BRI-SC-2W-L3	WAN ISDN module with 2 serial and 2 BRI ports	8.75	B (STP cable) A (UTP cable)
WSX-FT1-SC-1W-L3	WAN module with 1 serial and 1 T1 or E1 port	7.25	B (STP cable) A (UTP cable)
WSX-FE1-SC-1W-L3	WAN module with 1 serial and 1 T1 or E1 port	7.25	B (STP cable) A (UTP cable)
WSX-FT1-SC-2W-L3	WAN module with 2 serial and 2 T1 or E1 ports	8.75	B (STP cable) A (UTP cable)
WSX-FE1-SC-2W-L3	WAN module with 2 serial and 2 T1 or E1 ports	8.75	B (STP cable) A (UTP cable)
WSX-M013-2W-L3	WAN module with 2 channelized DS3 ports.	8.0	B (STP cable) A (UTP cable)
WSX-M013-4W-L3	WAN module with 4 channelized DS3 ports	10.0	B (STP cable) A (UTP cable)

Grounding a Chassis

Omni Switch/Routers have two grounding screw holes on the back of the chassis. These holes use 10-32 screws and are approximately 1 inch apart. In addition, these holes do not have paint and are surrounded by a small paint-free rectangular section, which provides for a good connection contact.

The figure below shows the location of the grounding screw holes on the back of an OmniS/R-9. They are located approximately four (4) inches from the bottom of the chassis and approximately one (1) inch from the left-hand side of the rear of the chassis.



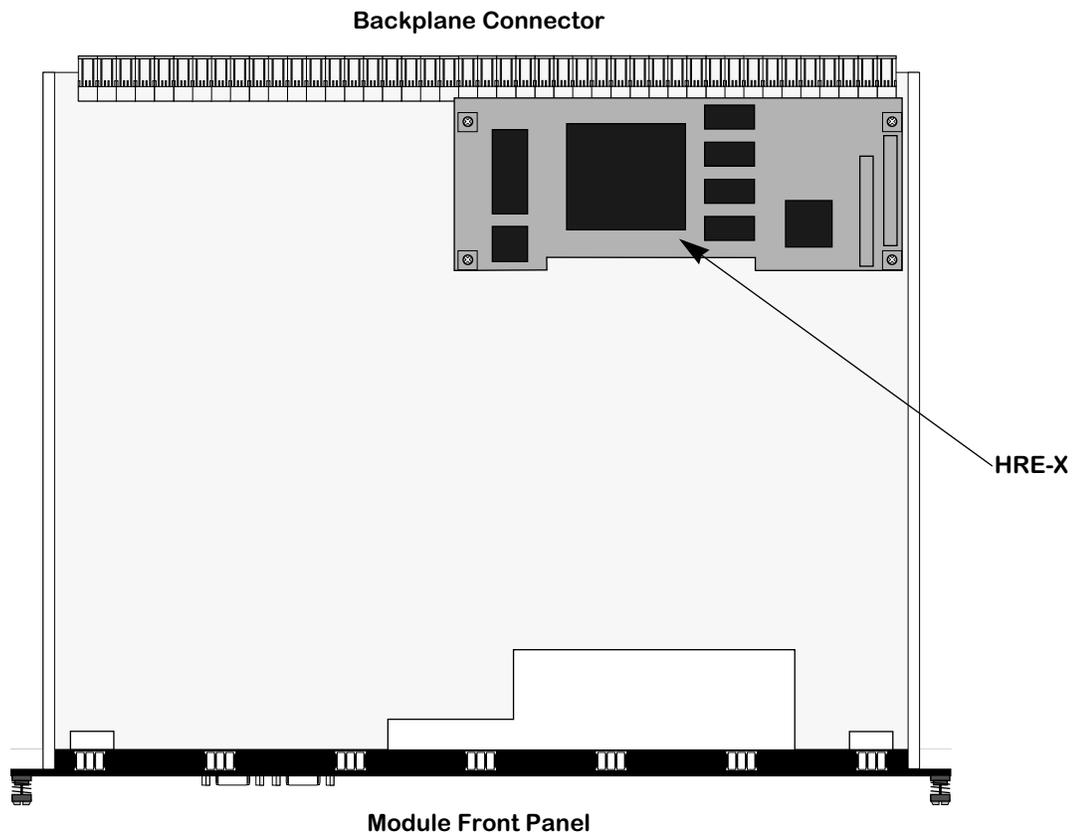
Grounding Screw Holes on an OmniS/R-9

On an OmniS/R-5, the grounding screw holes are located approximately one (1) inch from the bottom of the chassis and approximately one (1) inch from the left-hand side of the rear of the chassis.

On an OmniS/R-3, they are located approximately four (4) inches from the bottom of the chassis and approximately one (1) inch from the left-hand side of the rear of the chassis.

The Omni Switch/Router Hardware Routing Engine (HRE-X)

The Omni Switch/Router Hardware Routing Engine (HRE-X) is available for the MPX and all Omni Switch/Router switching modules. The HRE-X is a submodule, which plugs into an Omni Switch/Router module, that provides high speed Layer 3 distributed routing for IP and IPX traffic. The HRE-X intercepts frames from the switching logic and determines if a frame should be switched or routed. If a frame needs to be routed, the HRE-X will automatically add the appropriate routing information.



MPX with an HRE-X

The HRE-X has the following restrictions:

- You *must* have Release 3.4.4 software, or later, on your Omni Switch/Router.
- Do *not* install an HRE-X on an MPX unless it is Revision A10, or later.
- Do *not* install an HRE-X on a GSX-FM/FS-4W unless it is Revision B04, or later.

Each HRE-X routes up to 1.5 million packets per second. In an OmniS/R-9 with an HRE-X on every switching module, for example, you could have up to 12 Mpps routed throughput. On a per switch basis, the HRE-X also supports over 256,000 route entries and 64,000 Next Hop destinations.

Valid HRE-X Configurations

You can configure an Omni Switch/Router chassis in one of two ways: with an HRE-X on every single Omni Switch/Router switching module (distributed routing) or a single HRE-X on the MPX (centralized routing).

Distributed Routing. In this configuration, you *must* install an HRE-X on every single switching module in the chassis. In addition, you *cannot* install an HRE-X on the MPX. For example, in an OmniS/R-9 with a single MPX, you would need eight (8) HRE-Xs for all the switching modules. As a general rule, this configuration is recommended in networks of more than four subnets from any one switch.

Centralized Routing. In this configuration, you *must* install the HRE-X on the MPX but not on any Omni Switch/Router switching modules. The HRE-X will perform routing for all Omni Switch/Router switching modules in the chassis. As a general rule, this configuration is recommended for networks of two to four subnets from any one switch.

HRE-X Router Registers versus Feature Limitations

The HRE-X has three (3) registers that can be programmed with a MAC address and mask that allows it to recognize which destination MAC addresses it should act as a router for. IP Routing, Virtual Router Redundancy Protocol (VRRP), ATM Classical IP (CIP), and Channelized DS3 (i.e., M013) utilize at least one of these registers for their operation. This leads to a restriction of the combination of these features that can be supported on an Omni Switch/Router at any given time.

The HRE-X registers are programmed on a first come, first served basis. Any attempt to program more than three registers fails. In current release, the order which these features program the HRE-X is as follows:

1. ATM CIP
2. IP Routing (**Note:** If there is a second base MAC configured on the MPX, then it will also take a second register.)
3. M013
4. VRRP

For example, if a switch has two base MACs and a CIP group, then no other features can be configured. Any combination of the above features will work given the available HRE-X registers. IP routing always takes one register (two in the dual base MAC case), leaving the other features to compete for the remaining two (one in the dual base MAC case). The other features attempt to program a register only if they are enabled.

◆ Note ◆

ATM CIP is limited to 128 end node route cache entries.

Connecting a DC Power Source to an OmniS/R-PS5-DC375

The OmniS/R-5 can use a DC power supply called the OmniS/R-5-DC375. This power supply contains a female power connector as shown in the figure below. This supply requires the use of 12 gauge wire. A clamp inside each connector keeps the power wire tightly in place during operation. This connector has side screws that can be used to remove the connector.

OmniS/R-PS5-DC375

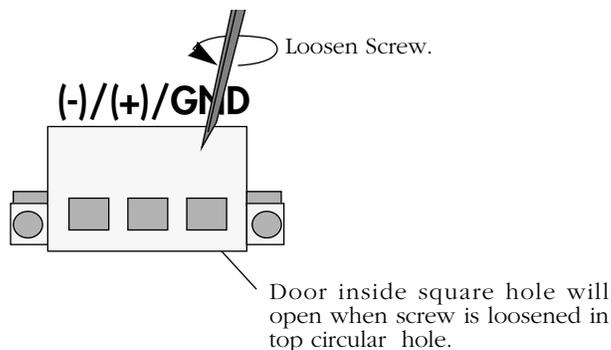


OmniS/R-5 DC Power Supply Connector Style

Installing DC Power Source Wire Leads

These instructions describe how to connect your 3-wire DC power source to the power connector on your DC power supply. A small flat-tip screwdriver and a wire stripper are required for this procedure.

1. Prepare the three (3) wires—12 gauge—that will plug into the power supply. First, **make sure they are not plugged into the 48-volt power source.**
2. Next, use a wire stripper to carefully strip about a half-inch off the end of each wire, removing the outer insulation to expose the copper core.
3. Twist the loose strands of copper wire together so that they form a tight braid. If possible, solder the entire braid of wire together for better conductivity.
4. Open the wire bay door for one of the three (3) power connector holes. The front of this connector contains a row of square holes. It also contains three (3) circular holes on top that contain screws; you loosen the screws in these holes to open the wire bay doors (square holes) on the connector front so that you can insert the wire lead.
 - a. Insert a small flat-tip screwdriver into one of the top three (3) screw holes.
 - b. Loosen the screw so that the door for the wire bay on the connector front opens.



Opening Wire Bay on Screw-Style Connector

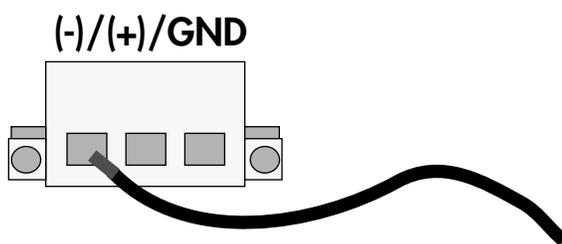
5. Insert the appropriate wire lead into the open circular hole. The silkscreen above each hole indicates which power lead—negative (-), positive (+), or ground (GND)—to plug into which hole. The lead you insert *must* match the lead attached to the 48-volt power source (i.e., negative to negative, positive to positive, ground to ground).

◆ Warning ◆

You must plug DC wire leads into the correct holes in the DC power connector. Use the labels above the DC power connector as a guide to positive, negative, and ground connections.

If you plug wire leads into wrong holes the power supply will not work and could result in damage.

Push the wire in far enough such that it reaches the back wall of the connector, about a half inch inside.



This end would plug into the negative (-) power source. The middle lead would plug into the positive (+) power source and the rightmost lead would plug into the ground (GND).

Inserting the Wire Lead Into the Circular Hole

6. Close the wire bay. Use the small screwdriver (from Step 4a) to tighten the screw above the wire bay into which you inserted the wire lead. The wire lead should be securely attached inside the connector. You should be able to pull on the wire and not dislodge it.

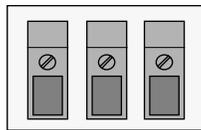
7. Repeat Steps 4 through 6 for the remaining two wire leads. Be sure that the end of each lead attaches to the same power source that you connected to on the power supply (i.e., negative to negative, positive to positive, ground to ground).

Connecting a DC Power Source to an OmniS/R-PS9-DC725

The OmniS/R-9P can use a DC power supply called the OmniS/R-PS9-DC725. This power supply contains a female power connector as shown in the figure below. This supply requires the use of 10 gauge wire. A clamp inside each connector keeps the power wire tightly in place during operation.

OmniS/R-PS9-DC725

GND/(+)/(-)



GND = 

OmniS/R-9P DC Power Supply Connector Style

Installation Requirements

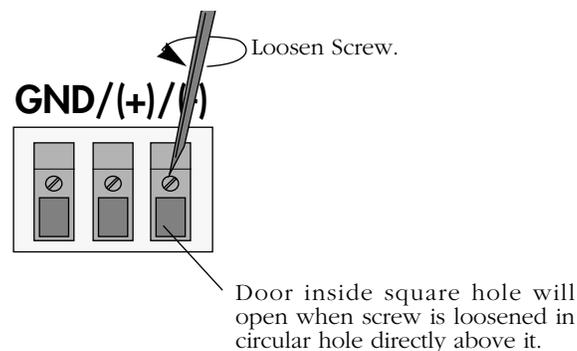
Caution: To reduce the risk of electric shock or energy hazards:

- The branch circuit overcurrent protection must be rated at a minimum of 30 A (amperes) for the OmniS/R-9P PS9-DC725.
- Use 10 gauge (AWG - American Wire Gauge) solid copper conductors only for the OmniS/R-9P PS9-DC725.
- A readily-accessible disconnect device that is suitably approved and rated shall be incorporated in the field wiring.
- This device is to be installed in a restricted access area in accordance with the NEC (National Electrical Code) or the authority having jurisdiction.
- Connect this device to a reliably grounded SELV (Safety Extra Low Voltage) or a centralized DC source.

Installing DC Power Source Wire Leads

These instructions describe how to connect your 3-wire DC power source to the power connector on your DC power supply. A small flat-tip screwdriver and a wire stripper are required for this procedure.

1. Prepare the three (3) wires—10 gauge—that will plug into the power supply. First, **make sure they are not plugged into the 48-volt power source.**
2. Next, use a wire stripper to carefully strip about a half-inch off the end of each wire, removing the outer insulation to expose the copper core.
3. Twist the loose strands of copper wire together so that they form a tight braid. If possible, solder the entire braid of wire together for better conductivity.
4. Open the wire bay door for one of the three (3) power connector holes. The front of the power connector contains a row of square holes. It also contains three (3) circular holes (located directly above the square holes) that contain screws; you loosen the screws in these holes to open the wire bay doors (square holes) on the connector front so that you can insert the wire leads into the power connector.
 - a. Insert a small flat-tip screwdriver into one of the three (3) screw holes.
 - b. Loosen the screw so that the door for the wire bay on the connector front opens.



Opening Wire Bay on DC Power Supply Connector

5. Insert the appropriate wire lead into the open circular hole. The silkscreen above each hole indicates which power lead—ground (GND), positive (+), or negative (−)—to plug into which hole. The lead you insert *must* match the lead attached to the 48-volt power source (i.e., ground to ground, positive to positive, negative to negative).

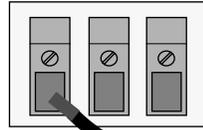
◆ Warning ◆

You *must* plug DC wire leads into the correct holes in the DC power connector. Use the labels above the DC power connector as a guide to ground, positive and negative connections.

If you plug wire leads into the wrong holes, the power supply will not work and could result in damage.

Push the wire in far enough so that it reaches the back wall of the connector, about a half inch inside.

GND/(+)/(-)



This end would plug into the ground (GND). The middle lead would plug into the positive (+) power source and the rightmost lead would plug into the negative (-) power source.

Inserting the Wire Lead Into the Circular Hole

6. Close the wire bay door. Use the small screwdriver (from Step 4a) to tighten the screw above the wire bay into which you inserted the wire lead. The wire lead should be securely attached inside the connector. You should be able to pull on the wire and not dislodge it.
7. Repeat Steps 4 through 6 for the remaining two wire leads. Be sure that the end of each lead attaches to the same power source that you connected to on the power supply (i.e., ground to ground, positive to positive, negative to negative).

2 The Omni Switch/Router MPX

Omni Switch/Router Management Processor Module (MPX) Features

The MPX provides such system services as maintenance of user configuration information, downloading of switching module software, basic bridge management functions, basic routing functions, the SNMP management agent, access to the User Interface software, and Advanced Routing. In addition, the MPX can operate in a redundant configuration with another MPX.

◆ Important Note ◆

If you have a single MPX in your chassis, it *must* be installed in Slot 1.

With the optional HRE-X, which is described in Chapter 1, “Omni Switch/Router Chassis and Power Supplies,” you can increase routing performance to 1.5 million packets per second.

MPX Technical Specifications	
Flash Memory	8 MB (16 MB maximum); 16 MB required for Release 4.4 and later
SIMM (DRAM) Memory	32 MB (64 MB maximum); 64 MB required for Release 4.4 and later
SDRAM Memory	16 MB
MAC Addresses Supported	4096
Switching Backplane	Up to 22 Gbps (aggregate) switching fabric capacity
Serial Ports	2 (1 male DB9 modem connector and 1 female DB9 console connector)
Ethernet (10 Mbps) Switch Management Ports	1 copper RJ-45 or fiber (ST) port for switch management functions.
Current Draw	3.75 amps without an HRE-X 5.25 amps with an HRE-X

◆ Warning ◆

Do *not* install any version of the MPM (i.e., MPM-C, MPM-1G, MPM-II, MPM-III, or original MPM) in a chassis with an MPX or any OmniSwitch switching module. Installing an MPM in a chassis with an MPX can cause physical damage.

Omni Switch/Router Management Processor Module (MPX) Features

Warning Label. This label indicates that the module contains an optical transceiver (on the MPXs with fiber ST Ethernet ports only).

OK1 (Hardware Status). This dual-state LED is on Green when the MPX has passed power-on hardware diagnostics successfully. On Amber when the hardware has failed diagnostic tests. If the **OK1** LED is alternating Green and Amber, then file system compaction is in progress.

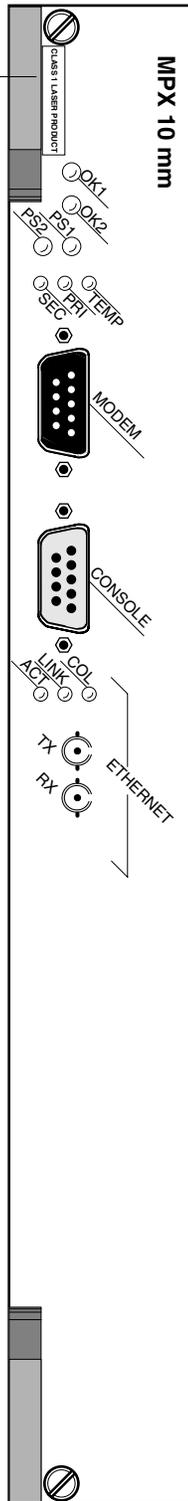
Caution

Do not power down the Omni Switch/Router or insert any modules while the **OK1** LED is alternating Green and Amber. If you do, file corruption may result and you will not be able to restart the switch.

OK2 (Software Status). Blinking Green when the MPX has successfully loaded software to the switching modules. Blinking Amber when the MPX is in a transitional state, such as when it first boots up. If the **OK2** LED blinks Amber for an extended period of time (i.e., more than a minute), then you should reboot the switch.

Caution

Do not insert or remove any modules while the MPX **OK2** LED is blinking Amber. If you do, file corruption may result and you will not be able to restart the switch.



Label. This label will indicate the Ethernet management port type. It will read either **MPX 10 mm** (multimode fiber Ethernet port) or **MPX 10** (copper RJ-45 Ethernet port).

Module Status LEDs

Module Status LEDs

PS1 (Power Supply 1 Status). This dual-state LED is on Green when the switch is receiving the proper voltage from Power Supply 1. It is on Amber when Power Supply 1 is on, but not supplying the correct amount of voltage to power the switch, or is installed and turned off. The **PS1** LED is Off when the Power Supply 1 is not present.

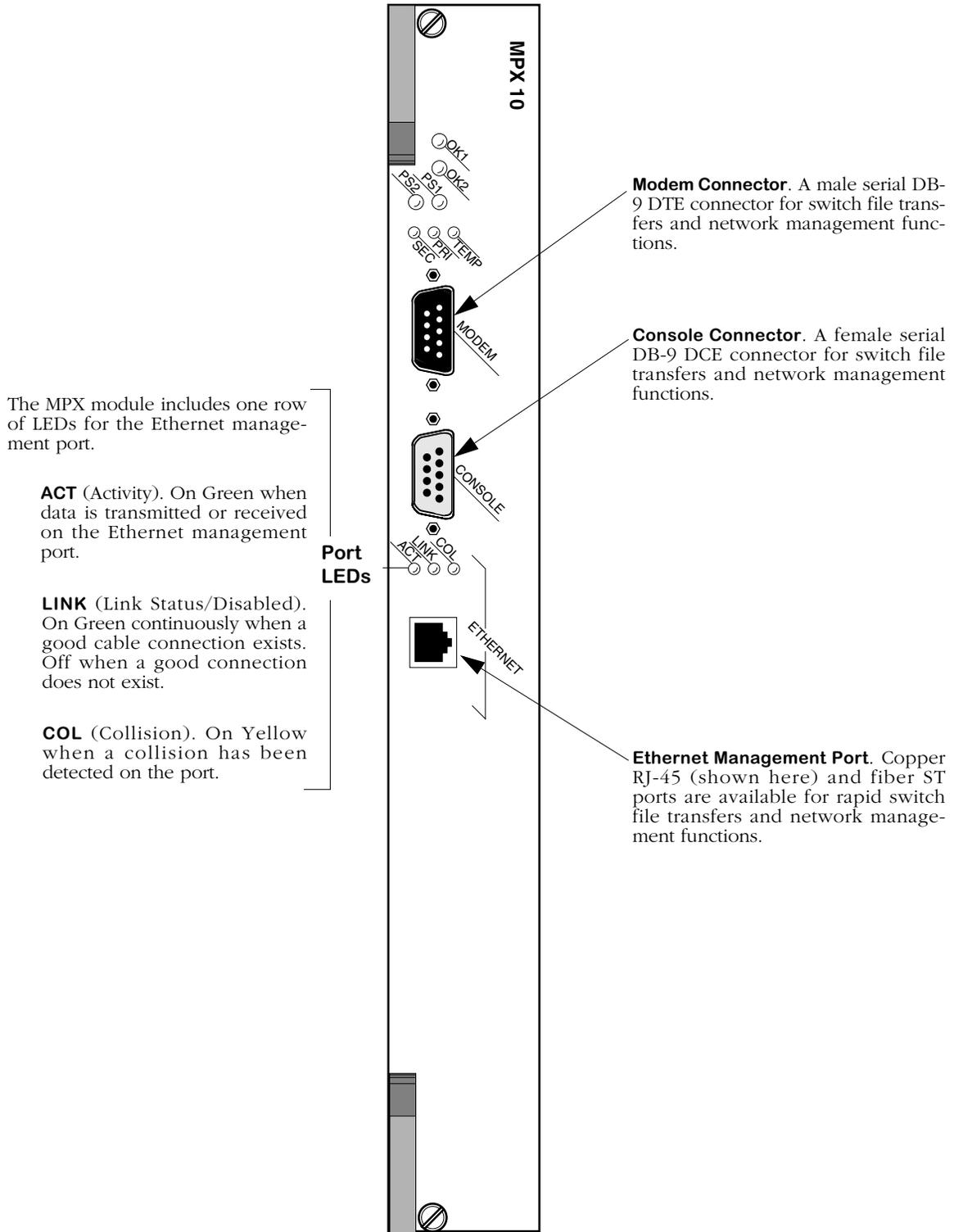
PS2 (Power Supply 2 Status). This dual-state LED is on Green when the Omni Switch/Router is receiving the proper voltage from Power Supply 2. It is on Amber when Power Supply 2 is on, but not supplying the correct amount of voltage to power the switch, or is installed and turned off. The **PS2** LED is Off when Power Supply 2 is not present.

TEMP (Temperature). On Yellow to warn that the internal switch temperature is approaching maximum operating limits. Note that this LED comes on *before* the temperature limit is reached.

PRI (Primary MPX). On Green when this MPX is the active, or controlling, MPX. It is also on Green when this is the only MPX installed in the switch.

SEC (Secondary MPX). On Green when this MPX is the secondary MPX in a redundant MPX configuration. As the secondary MPX, this module is in hot standby mode.

Omni Switch/Router Management Processor Module (MPX) Status LEDs



MPX Management Connectors

MPX Serial and Ethernet Management Ports

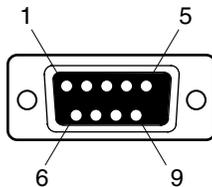
You can gain access to switch management software through one of the two serial (RS-232) ports on the MPX or the Ethernet management port. The two serial ports are configured with 9-pin “D” connectors (DB-9) per the IBM AT serial port specification. One port, called the “modem” port, is male and the other, called the “console” port, is female. See *MPX Management Connectors* on page 2-3 for illustrations of these ports.

The modem port is a Data Terminal Equipment (DTE) connector, which is typically connected to a modem. You can also connect directly from this port to a PC or terminal with a standard null-modem cable available in most computer equipment stores.

◆ **Note** ◆

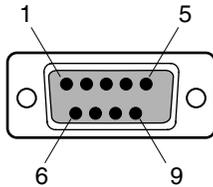
The modem port is hard-wired for DTE communication; you do not need to set any jumpers.

The console port is a Data Communication Equipment (DCE) connector, which can be directly connected to a PC, terminal, or printer.



MPX Console Port Specifications		
Pin Number	Standard Signal Name	Direction
1	Not Used	
2	RD	From MPX
3	TD	To MPX
4	Not Used	
5	GND	
6	Not Used	
7	Not Used	
8	Not Used	
9	Not Used	
Shell	Shield GND	

MPX Console Port



MPX Modem Port Specifications		
Pin Number	Standard Signal Name	Direction
1	Not Used	
2	RD	To MPX
3	TD	From MPX
4,	DTR	From MPX
5	GND	
6	DSR	To MPX
7	RTS	From MPX
8	CTS	To MPX
9	Not used	
Shell	Shield GND	

MPX Modem Port

Ethernet Management Port

The MPX also supports an out-of-band Ethernet port for high-speed uploads and switch management functions. With this port, you can access the Omni Switch/Router over a network via Telnet or FTP.

You can use the Boot prompt to configure an IP address for the Ethernet management port or you can use the **ethernetc** command, which is described in Chapter 10, “Configuring Management Processor Modules.” After you have assigned an IP address to the Ethernet management port, you can use it to Telnet into the UI.

See Appendix A, “The Boot Line Prompt,” for documentation on configuring the Ethernet management port with the boot prompt.

◆ Important Note ◆

On some revisions of the MPX, you *must* configure the Ethernet management port with the boot prompt before you can use the **ethernetc** command.

See the table on the following page for available Ethernet management port types.

MPX Model	Ethernet Management Port Type (Cable Type)	Max. Cable Distance
MPX-T	RJ-45 (UTP)	100 meters
MPX-FL	ST (Multimode fiber)	2 kilometers

Configuring MPX Serial Ports

The serial communications parameters for the two MPX serial ports are set by default to the following:

- 9600 bits per second (bps)
- 8 data bits
- 1 stop bit
- no parity
- no hardware flow control (Windows 95)

Each serial port supports serial data rates of 1200, 9600, 19200, and 38400 bps. However, you must remove the default baud rate shunt (E1), which fixes the baud rate at 9600 bps, before you can change the baud rate. This shunt is located near the front end of the MPX's circuit board, just to the right of the Ethernet management port.

To change the serial port configuration parameters, use the **ser** command, which is described in detail in Chapter 10, "Configuring Management Processor Modules."

Flash Memory and Omni Switch/Router Software

Flash memory on the MPX holds the Omni Switch/Router's executable images and configuration data. When a switching module comes online, the MPX downloads the appropriate image file for that module to that module's memory. Image files (those with the **img** extension) contain executable code for different switching modules and software features.

The following table lists Omni Switch/Router image files that may be present in MPX flash memory along with the module(s) or feature with which the file is used.

File Name	Modules/Function Used With
mpx.img mpx.cmd mpm.cfg mpm.cnf	MPX
asm.img	All ASX modules
desx.img	Ethernet port stress test software
diagx.img	Diagnostics software
ds3e3drv.img	ASX-DS3, ASX-E3
esx.img	All GSX and ESX modules
fpx.img	IP Fastpath and Firewall software
frlmi.img	FRF/FR-LMI software
fwdx.img	IP Fastpath and Firewall software
gated.img	Advanced Routing software
ipcntrl.img	IP control software
ipms.img	IPMS software
isdn.img	WSX-BRI-SC
m013x.img	WSX-M013
maker.img	ASX-M-622RF-1W
mpcx.img	Multi-Protocol Over ATM (MPOA) software
mrd.img	Advanced Routing software
ntp.img	Network Time Protocol (NTP) software

continued on next page...

File Name	Modules/Function Used With (cont.)
policy.img	PolicyView software
qos.img	Quality of Service (QOS) software
rav.img	RADIUS authentication software
sonet.img	SONET error collection software (required on ASX-M-622RF-1W)
t1e1drv.img	WSX-FT1/E1-SC
text_cfg.img	Text-based configuration software
tsx.img	TSX-C-32W, TSX-CD-16W
vrrp.img	VRRP software
vsmboot.asc	Boot file for Voice Over IP (VOIP) modules
vsx.img	Voice Over IP (VOIP) modules
web.img	HTTP browser client software
wsx.img	WSX-S-2W, WSX-SC-4W, WSX-SC-8W (Frame Relay and PPP software)

Flash Memory Guidelines

The switch alters flash memory contents when a software command requests a configuration change, when a remote administrator downloads a new executable image, or when the switch fails and a record of the failure is written to flash memory. These operations require available space in flash memory.

In general the flash memory on the switch should always have at least 75000 bytes available at all times. In a switch with 8 MB of flash memory, for example, the images in flash should never exceed 7.45 MB. (You can view how much flash memory is available through the **ls** command.) This will allow enough room in flash for booting and configuration file expansions. If your flash memory exceeds this amount, then you need to delete some images from flash.

In addition, the flash file system has a limit of 256 files, including configuration, logging, and other files. When this 256-file limit is reached, configuration file expansions will cease and new files will not be able to be loaded. This file limit applies even if there is enough memory available in flash.

Not all image files in flash memory are required—only those that must be used with the switching modules in your Omni Switch/Router. You can remove any files that are not required for your Omni Switch/Router configuration by using the **rm** command. For example, if you did not have any Token Ring modules, you could remove the **tsx.img** file.

MPX Redundancy

In order to provide greater reliability, Omni Switch/Router supports two MPXs in a primary/secondary redundant configuration. If the primary MPX fails, the secondary MPX takes over without any operator intervention.

◆ Warning ◆

Do *not* install any version of the MPM (i.e, MPM-C, MPM 1G, MPM II, or original MPM) in a chassis with an MPX. Installing an MPM in a chassis with an MPX can cause physical damage. If you want to configure an Omni Switch/Router chassis in a redundant configuration, you *must* use two MPXs.

When you have two MPXs in one chassis, they must be installed in Slots 1 and 2, and only one can be active. MPXs will assume one of the following roles.

- Primary - The MPX that is currently active and processing commands. It is also the MPX that is communicating via Telnet, FTP, etc.
- Secondary - An MPX that is currently not the primary. It has sufficient software to communicate with the primary MPX. (For full redundancy, the secondary MPX should also have the same software version as the primary and its configuration should be in sync with the primary.) In this state, it is capable at any time of assuming the primary role.

The LEDs on each MPX reflect the same status with the exception that the primary's **PRI** LED is on whereas the secondary's **SEC** LED is on. Also, the secondary MPX's **OK2** LED will not flash amber during board transitions. See *Omni Switch/Router Management Processor Module (MPX) Status LEDs* on page 2-2 for locations of the LEDs.

◆ Important Note ◆

To support redundancy, your MPX *must* be Revision A14 or higher.

Change-Over Procedure

The secondary MPX continuously monitors the primary MPX. This monitoring serves two purposes: 1) to notify the secondary MPX that the primary is alive and processing, and 2) to update the configuration and thus keep the two MPXs in sync. If the secondary MPX detects that the primary is no longer operational, it will begin to take over as primary. When a secondary MPX becomes primary it resets all the other modules in the chassis and performs a primary MPX initialization.

There are four states for an MPX configuration. You can view the current MPX state through the **slot** command. These states are described in the table below. Note that for a primary/secondary configuration to be in a “redundant” state, the relationship between the two MPXs must meet the conditions shown in the table.

MPX State	Requirement for State
Redundant	Both MPXs are running the same version of software and the configurations are in sync.
Configuration Fallback	Both MPXs are running the same version of software but the configurations are different.
Software Fallback	The MPXs are running different versions of software, and their configurations may be the same or different.
None	There is only one MPX installed in the chassis.

The primary MPX has the ability to transfer files to and from the secondary MPX. In the condition where the secondary MPX has an older version of software (Software Fallback), it is not desirable to update the configuration file of the secondary. It is therefore the default not to update the configuration file on the secondary if the secondary is running an earlier version of software. You can force the update using appropriate commands in the **mpm** menu. (See Chapter 10, “Configuring Management Processor Modules,” for more information on commands in the mpm menu.)

◆ **Note** ◆

Do *not* remove a primary MPX without performing a **renounce** command (described in Chapter 10, “Configuring Management Processor Modules”) first.

MPX Redundancy Commands

A set of commands exists to monitor the primary and secondary MPXs. These commands are covered in detail in Chapter 10, “Configuring Management Processor Modules.” Note that you can attach a terminal to both MPXs in a chassis; however, you will see a different responses depending on which is primary and which is secondary. You should execute all UI commands from the primary MPX except for those commands specifically addressing the secondary MPX. For example, commands are available to control and monitor the secondary MPX from the primary MPX (e.g., the **sls** command lists files on the secondary MPX from the primary MPX).

3 Omni Switch/Router Switching Modules

Omni Switch/Router switching modules perform software filtering, translations between dissimilar network interfaces, and hardware-based switching. Omni Switch/Router switching modules have an additional on-board interface connector for the HRE-X.

Currently, Omni Switch/Router switching modules consist of Gigabit Ethernet modules, auto-sensing 10/100 Ethernet modules, Fast (100 Mbps) Ethernet modules, 10 Mbps Ethernet modules, Token Ring modules, ATM uplink modules, Voice Over IP (VOIP) modules, and WAN modules.

◆ Important Note ◆

Omni Switch/Router modules require the use of an Omni Switch/Router chassis (see Chapter 1, “Omni Switch/Router Chassis and Power Supplies”). Do *not* install an Omni Switch/Router module in an OmniSwitch chassis and do *not* install an OmniSwitch module in an Omni Switch/Router chassis.

Gigabit Ethernet Modules

- GSX-FM/FS/FH-2W 2-port Gigabit Ethernet switching module
- GSX-K-FM/FS/FH-2W Advanced 2-port Gigabit Ethernet switching module
- GSX-FM/FS-4W 4-port Gigabit Ethernet switching module

10/100 Ethernet Modules

- ESX-100C-12W 12-port auto-sensing 10/100 Ethernet switching module
- ESX-100C-32W 32-port auto-sensing 10/100 Ethernet switching module
- ESX-K-100C-32W Advanced 32-port auto-sensing 10/100 Ethernet switching module

Fast (100 Mbps) Ethernet Modules

- ESX-100FM/FS-12W 12-port Fast Ethernet (100 Mbps) switching module
- ESX-K-100FM/FS-16W Advanced 16-port Fast Ethernet (100 Mbps) switching module

10 Mbps Ethernet Modules

- ESX-FM-24W 24-port 10 Mbps Ethernet switching module with fiber ports

Token Ring Modules

- TSX-C-32W 32-port Token Ring (Lobe only) switching module
- TSX-CD-16W 16-port Token Ring (Lobe and Station) switching module

ATM Uplink Modules

- ASX-155FM/FS/FH-1W/2W 1- or 2-port ATM uplink (155 Mbps) switching modules
- ASX-155RFM/RFS-1W 1-port (redundant) ATM uplink (155 Mbps) switching module
- ASX-622RFM/RFS-1W 1-port (redundant) ATM uplink (622 Mbps) switching module
- ASX-M-622RFM/RFS/RFH-1W Advanced 1-port (redundant) ATM uplink (622 Mbps) switching module
- ASX-DS3-1W/2W 1- or 2-port ATM DS3 uplink modules
- ASX-E3-1W/2W 1- or 2-port ATM E3 uplink modules

WAN Modules

- WSX-S-2W 2 serial ports that support the frame relay or PPP protocol.
- WSX-SC-4W/8W 4 or 8 serial ports that support the frame relay or PPP protocol.
- WSX-FT1/E1-SC-1W/2W 1 or 2 T1/E1 ports and one or two serial ports that support the frame relay or PPP protocol
- WSX-BRI-SC-1W/2W 1 or 2 UPS (Universal Serial Port) and 1 or 2 ISDN-BRI ports that support Frame Relay or PPP
- WSX-M013-2W/4W 2 or 4 channelized DS3 ports (described in Chapter 56, “Managing Channelized DS3 Modules”)

Voice Over IP Modules

Voice Over IP (VOIP) modules for the Omni Switch/Router are listed below and are documented in the *VoIP User Manual*.

- VSX-VSA 4, 6, 8, 14, or 16 analog RJ-11 ports supporting FXS and FXO interfaces, including T.38 FAX
- VSX-VSD 2 or 4 digital T1 or E1 (Euro PRI and Qsig) ports, including T.38 FAX

Omni Switch/Router Hardware Routing Engine

The HRE-X offers high-speed Layer 3 switching from 1.5 to 12.0 million packets per second (Mpps) in a fully loaded chassis. See Chapter 1, “Omni Switch/Router Chassis and Power Supplies,” for more information on the HRE-X.

◆ Important Note ◆

Omni Switch/Router switching modules require an MPX. You cannot install any version of the MPM (i.e., MPM-III, MPM-C, MPM-1G, MPM-II, or original MPM) in a chassis with an MPX. See Chapter 2, “The Omni Switch/Router MPX,” for more information on the MPX.

Required Image Files

See the table below for the required images files for the MPX and switching modules. You *must* load the image file (or files) listed for the corresponding module or it will not run.

◆ **Note** ◆

You must load the **sonet.img** file to run SONET error collection on ASX modules. However, this image file is only required on the ASX-M-622RF-1W modules and not other ASX modules.

Required Image Files

Module	Image File(s)
MPX	mpx.img, fpx.img
ASX-155FM/FS/FH-1W/2W	asm.img
ASX-155RFM/RFS-1W	asm.img
ASX-622RFM/RFS-1W	asm.img
ASX-D3-1W/2W	asm.img, ds3e3drv.img
ASX-E3-1W/2W	asm.img, ds3e3drv.img
ASX-M-622RF-1W	asm.img, sonet.img, maker.img
ESX-100C-12W	esx.img
ESX-100C-32W	esx.img
ESX-K-100C-32W	esx.img
ESX-100FM/FS-12W	esx.img
ESX-K-100FM/FS-16W	esx.img
ESX-FM-24W	esx.img

continued on next page...

Required Image Files (continued)

Module	Image File(s)
GSX-FM/FS/FH-2W	esx.img
GSX-K-FM/FS/FH-2W	esx.img
GSX-FM/FS-4W	esx.img
TSX-C-32W	tsx.img
TSX-CD-16W	tsx.img
VSX-VSA	vsx.img, text_cfg.img, vsmboot.asc
VSX-VSD	vsx.img, text_cfg.img, vsmboot.asc
WSX-S-2W	wsx.img
WSX-SC-4W	wsx.img
WSX-SC-8W	wsx.img
WSX-BRI-SC-1W/2W	wsx.img, isdn.img
WSX-FT1-SC-1W/2W	wsx.img, t1e1drv.img
WSX-FE1-SC-1W/2W	wsx.img, t1e1drv.img
WSX-M013-2W/4W	m013x.img

Handling Fiber and Fiber Optic Connectors

Using fiber is extremely simple, but a few important rules should always be followed:

Step 1. Use Premium Grade Jumper Cables with Duplex SC Connectors

There are many brands of fiber optic jumper cables, with a wide range of quality between each manufacturer. Premium cables do three things well:

- They provide a good polish on the fiber optic connector endface (where the light exits the cable). Endface geometries must be exceptionally precise and aligned to extremely tight tolerances. The better the endface geometry, the lower the loss and more consistent the connection. Poor connector interfaces will reflect light back into the laser, causing an increase in laser noise.
- They mate well with other connector interfaces. Chances are the manufacturer of the jumper cable will not be the same as the manufacturer of the transceiver connector interface. Premium jumper cables mechanically align themselves well into most transceiver interfaces. This provides both better performance as well as better repeatability. You will always see a variance in transceiver power due to connector alignment, often as much as 0.3 to 0.7 dB. Good jumper cables help reduce this variance.
- They continue to mate well after many insertions and removals. Premium grade jumper use premium grade connectors that maintain their mechanical integrity up to and beyond 2000 insertion cycles.

For better repeatability, always use duplex (two connectors fused together and terminated to two cables) SC connectors on your jumper cables when connecting to a fiber-optic transceiver. Two simplex connectors inserted into a transceiver interface will often have up to 3 dB greater variation in repeatability compared to duplex connectors.

Never bend the fiber optic cable beyond its recommended minimum bend radius (1.2 inches minimum). This introduces bend losses and reflections that will degrade the performance of your system. It can also damage the fiber, although fiber is much tougher than most would assume. Still, it is highly recommended to buy only jumper cables with 3mm Kevlar jacketing, which offer superior protection and longer life.

Step 2. Keep Your Fiber Optic Connectors Clean

Unlike electrical connectors, fiber-optic connectors need to be extremely clean to ensure good system performance. Microscopic particles on the connector endface (where the light exits the connector) can degrade the performance of your system, often to the point of failure. If you have low-power output from a fiber-optic transceiver or a fault signal from your equipment, cleaning your fiber-optic connectors should always be done before trouble shooting.

Follow the steps below to clean your fiber optic connector:

1. Hold the connector cleaner tool in the palm of your left hand and, with the silver shutter upwards, rotate the cloth-forwarding lever (located on the right side of the tool) with your thumb away from your body. As the lever winds the cleaning cloth inside the case, it simultaneously opens the silver shutter located at the top of the unit.

2. Keeping your thumb pressed on the cloth-forwarding lever, press the optical plug ferrule endface against the cleaning cloth and drag the plug down toward your body (there should be arrows on the top of the tool that indicate the proper wiping direction). The connector is now clean.
3. Release the cloth-forwarding lever, allowing it to return to its initial position.

A cleaning cloth reel can enable over 400 cleanings and is replaceable. When cables are not being used, always put the plastic or rubber endcaps back on the connector to ensure cleanliness.

Step 3. Keep the Transceiver Interface Clean

If you have cleaned your connectors, but still experience low-power output from a fiber-optic transceiver or a fault signal from your equipment, you should clean the transceiver interface by blowing inert dusting gas inside the transceiver interface. This removes dust and other small particles that may block the optical path between the optics of the transceiver and the connector's endface.

Step 4. Attenuate Properly

Often equipment using laser-based transceivers need to have the optical path attenuated when performing loop-back testing or testing between two pieces of equipment. Too much optical power launched into the receiver will cause saturation and result in system failure. If you are using single mode fiber and you do not know the power output of the laser, it is always best to use a 10 dB attenuator when testing. Using the wrong type of attenuator will introduce problems, most notably reflection of light back into the laser, often resulting in excess noise and causing system failure.

Inline attenuators eliminate the need for additional jumper cables and thus reduce the number of connection interfaces. This increases the integrity of the optical path resulting in a more accurate test.

Gigabit Ethernet Modules

Gigabit Ethernet connections can be used as network backbones or in a wiring closet. The following Omni Switch/Router Gigabit Ethernet modules are available:

- **GSX-FM/FS/FH-2W** Two (2) Gigabit Ethernet backbone connections using fiber (SC) connectors.
- **GSX-K-FM/FS/FH-2W** Advanced switching module with two (2) Gigabit Ethernet backbone connections using fiber (SC) connectors.
- **GSX-FM/FS-4W** Four (4) Gigabit Ethernet server connections using fiber (SC) connectors.

These modules are described and illustrated in the following sections.

◆ Note ◆

Wait at least five (5) seconds after a cable is pulled from a GSX module before reinserting it. This will prevent packets from being dropped.

GSX-FM/FS/FH-2W

The GSX-FM/FS/FH-2W Gigabit Ethernet backbone switching module contains two fiber SC connectors that support two fully switched 1000Base-LX (long-distance fiber transmissions) or 1000Base-SX (short-distance fiber transmission ports). The GSX-FM/FS/FH-2W can be factory configured with long-reach single mode, intermediate-reach single mode, or multimode fiber ports (see *GSX-FM/FS/FH-2W Technical Specifications* on page 3-8 for more information). The long-reach single mode version is referred to as the GSX-FH-2W; the intermediate-reach single mode version is referred to as the GSX-FS-2W; and the multimode version is referred to as the GSX-FM-2W.

The ports are color coded to differentiate the mode: multimode connectors are black, long-haul single mode connectors are yellow, and intermediate-reach single mode connectors are blue. (See *Handling Fiber and Fiber Optic Connectors* on page 3-5 for proper handling of SC connectors and fiber-optic cable.)

The GSX-FM/FS/FH-2W can be used as a backbone connection in networks where Gigabit Ethernet is used as the backbone media.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

GSX-FM/FS/FH-2W Technical Specifications	
Number of ports	2
Connector Type	SC
Standards Supported	802-3z, 1000Base-LX, and 1000Base-SX
Data Rate	1 Gigabit per second (full duplex)
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	4,096
Connections Supported	1000Base-LX or 1000Base-SX connection to backbone or server
Cable Supported	Multimode and single mode
Output Optical Power	-9.5 to -4 dBm (Multimode) -9.5 to -3 dBm (Intermediate-reach single mode) 0 to +5 dBm (Long-reach single mode)
Input Optical Power	-17 to 0 dBm (Multimode) -20 to -3 dBm (Intermediate-reach single mode) -24 to -3 dBm (Long-reach single mode)
Cable Distance	Multimode fiber: \approx 220 m Intermediate-reach single mode fiber: \approx 10 km Long-reach single mode fiber: \approx 70 km
Current Draw	6.75 amps without an HRE-X 8.25 amps with an HRE-X

◆ Special Note ◆

The single mode version of this module has been deemed:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

Warning Label. This label indicates that the module contains an optical transceiver.

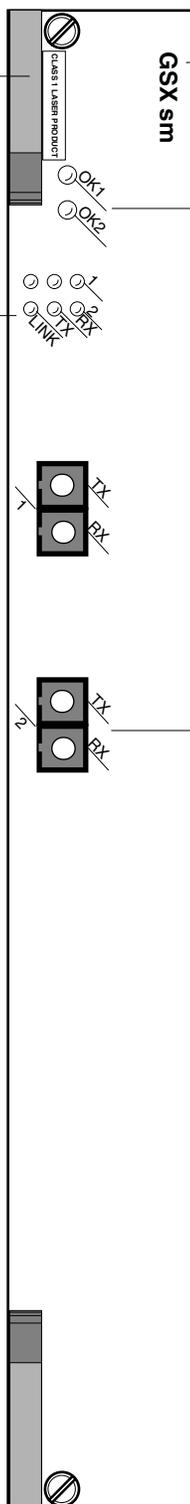
This Gigabit Ethernet module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number. Definitions for the LEDs are given below.

RX (Receive). On Green when the corresponding port is receiving data.

TX (Transmit). On Green when the corresponding port is transmitting data.

LINK (Link Status/Disabled). On Green when the corresponding port has a valid physical link and a signal is present. Under normal conditions, this LED should always be on when a cable is connected.

Port LEDs



Module Label. This label will indicate the GSX-FM/FS/FH-2W type. It will read either **GSX mm** (multimode cable), **GSX sm** (intermediate-reach single mode cable), or **GSX sm long reach** (long-reach single-mode cable).

Module LEDs **OK1 (Hardware Status).** On Green when the module has passed diagnostic tests successfully. On Red when the hardware has failed diagnostics.

OK2 (Software Status). Blinking Green when the module software was downloaded successfully and the module is communicating with the MPX. Blinking Red when the module is in a transitional state. On solid Red if the module failed to download software from the MPX.

SC connectors will be color coded to indicate multimode (Black), long-haul single mode (Yellow), or intermediate-reach single mode (Blue).

2-Port Gigabit Ethernet Switching Module

GSX-K-FM/FS/FH-2W

The GSX-K-FM/FS/FH-2W Gigabit Ethernet backbone switching module contains two fiber SC connectors that support two fully switched 1000Base-LX (long-distance fiber transmissions) or 1000Base-SX (short-distance fiber transmission ports). The GSX-K-FM/FS/FH-2W can be used as a backbone connection in networks where Gigabit Ethernet is used as the backbone media.

The GSX-K-FM/FS/FH-2W can be factory configured with intermediate-reach single mode or multimode fiber ports (see *GSX-K-FM/FS/FH-2W Technical Specifications* on page 3-11 for more information). The intermediate-reach single mode version is referred to as the GSX-K-FS-2W; the long-reach single mode version is referred to as the GSX-K-FH-2W; and the multimode version is referred to as the GSX-K-FM-2W.

The ports are color coded to differentiate the mode: multimode connectors are black, long-haul single mode connectors are yellow, and intermediate-reach single mode connectors are blue. (See *Handling Fiber and Fiber Optic Connectors* on page 3-5 for proper handling of SC connectors and fiber-optic cable.)

The GSX-K-FM/FS/FH-2W takes advantage of new Gigabit Ethernet/Fast Ethernet ASIC technology known as “Kodiak.” This module provides 4 priority levels and 256 queues per Kodiak ASIC.

◆ Note ◆

Kodiak-based modules support up to 4 levels of priority (0-1, 2-3, 4-5, 6-7). This is *not* compatible with the implementation of VLAN priority of Mammoth-based modules. Kodiak based priority VLANs can only be used with other Kodiak based priority VLANs.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

GSX-K-FM/FS/FH-2W Technical Specifications	
Number of ports	2
Connector Type	SC
Standards Supported	802-3z, 1000Base-LX, and 1000Base-SX
Data Rate	1 Gigabit per second (full duplex)
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	8,192
Connections Supported	1000Base-LX or 1000Base-SX connection to backbone or server
Cable Supported	Multimode and single mode
Output Optical Power	-9.5 to -4 dBm (Multimode) -9.5 to -3 dBm (Intermediate-reach single mode) 0 to +5 dBm (Long-reach single mode)
Input Optical Power	-17 to 0 dBm (Multimode) -20 to -3 dBm (Intermediate-reach single mode) -24 to -3 dBm (Long-reach single mode)
Cable Distance	Multimode fiber: \approx 220 m Intermediate-reach single mode fiber: \approx 10 km Long-reach single mode fiber: \approx 70 km
Current Draw	5.25 amps without an HRE-X 6.75 amps with an HRE-X

◆ Special Note ◆

The single mode version of this module has been deemed:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

Warning Label. This label indicates that the module contains an optical transceiver.

This Gigabit Ethernet module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number. Definitions for the LEDs are given below.

RX (Receive). On Green when the corresponding port is receiving data.

TX (Transmit). On Green when the corresponding port is transmitting data.

LINK (Link Status/Disabled). On Green when the corresponding port has a valid physical link and a signal is present. Under normal conditions, this LED should always be on when a cable is connected.

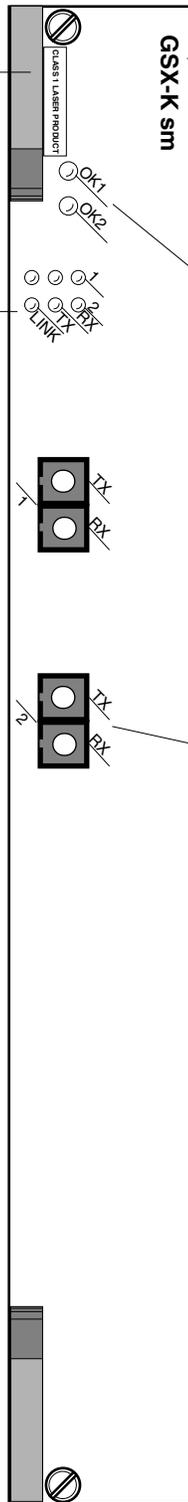
Port LEDs

Module LEDs

Module Label. This label will indicate the GSX-K-FM/FS/FH-2W type. It will read either **GSX-K mm** (multimode cable), **GSX-K sm** (intermediate-reach single mode cable), or **GSX sm K long reach** (long-reach single-mode cable).

Please refer to *2-Port Gigabit Ethernet Switching Module* on page 3-9 for further information on these LEDs.

SC connectors will be color coded to indicate multimode (Black) or intermediate-reach single mode (Blue).



2-Port Advanced Gigabit Ethernet Switching Module

GSX-FM/FS-4W

The GSX-FM/FS-4W Gigabit Ethernet server switching module contains four fiber SC connectors that support four 1000Base-LX (long-distance fiber transmissions) or 1000Base-SX (short-distance fiber transmission ports). The GSX-FM/FS-4W can be factory configured with single (1000Base-LX) mode or multimode (1000Base-SX) fiber ports (see *GSX-FM/FS-4W Technical Specifications* on page 3-14 for more information). The single mode (1000Base-LX) version is referred to as the GSX-FS-4W; the multimode version (1000Base-SX) is referred to as the GSX-FM-4W. The ports are color coded to differentiate the mode: single mode connectors are blue and multimode connectors are black. (See *Handling Fiber and Fiber Optic Connectors* on page 3-5 for proper handling of SC connectors and fiber-optic cable.)

The GSX-FM/FS-4W can be used to connect to Gigabit Ethernet edge devices and servers.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

GSX-FM/FS-4W Technical Specifications	
Number of ports	4
Connector Type	SC
Standards Supported	802-3z, 1000Base-LX, and 1000Base-SX
Data Rate	1 Gigabit per second (full duplex)
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	4,096
Connections Supported	1000Base-LX or 1000Base-SX connection to edge device or server
Cable Supported	1000Base-SX Multimode 1000Base-LX Single mode
Output Optical Power	-9.5 to -4 dBm (Multimode) -9.5 to -3 dBm (Single mode)
Input Optical Power	-17 to 0 dBm (Multimode) -20 to -3 dBm (Single mode)
Cable Distance	1000Base-SX Multimode fiber: approximately 200 m 1000Base-LX Single mode fiber: approximately 10 km
Current Draw	10.0 amps without an HRE-X 11.5 amps with an HRE-X

◆ Special Note ◆

The single mode version of this module has been deemed:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

Warning Label. This label indicates that the module contains an optical transceiver.

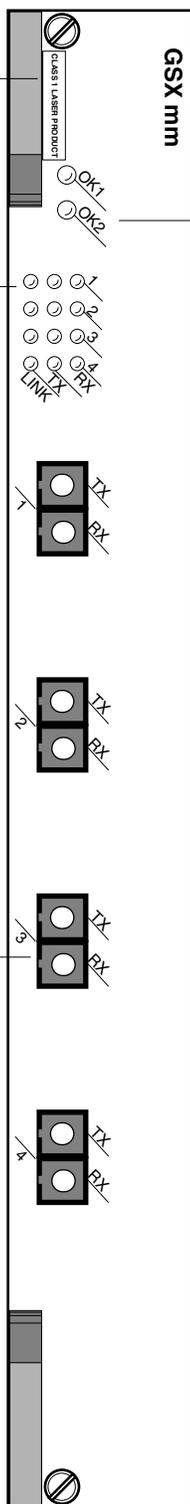
This Gigabit Ethernet module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number. Definitions for the LEDs are given below.

RX (Receive). On Green when the corresponding port is receiving data.

TX (Transmit). On Green when the corresponding port is transmitting data.

LINK (Link Status/Disabled). On Green when the corresponding port has a valid physical link and a signal is present. Under normal conditions, this LED should always be on when a cable is connected.

SC connectors will be color coded to indicate multimode (Black) or single mode (Blue).



Label. This label will indicate the GSX-FM/FS-4W type. It will read either **GSX mm** (multimode cable) or **GSX sm** (single mode cable).

Module LEDs Please refer to *2-Port Gigabit Ethernet Switching Module* on page 3-9 for further information on these LEDs.

4-Port Gigabit Ethernet Switching Module

Auto-Sensing 10/100 Ethernet Modules

Alcatel's Omni Switch/Router 10/100 Ethernet modules can be used to connect networks with a mix of 10 Mbps and 100 Mbps workstations or as a network backbone.

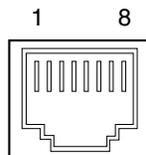
The following Omni Switch/Router 10/100 and Fast Ethernet modules are available:

- ESX-100C-12W Twelve (12) auto-sensing 10/100 Mbps backbone connections using RJ-45 ports.
- ESX-100C-32W Thirty-two (32) auto-sensing 10/100 Mbps desktop connections using RJ-45 ports.
- ESX-K-100C-32W Advanced switching module with thirty-two (32) auto-sensing 10/100 Mbps desktop connections using RJ-45 ports.

These modules are described and illustrated in the following sections.

Ethernet RJ-45 Pinouts

The figure and table below illustrate the pinouts used on RJ-45 ports in Omni Switch/Router 10/100 Ethernet modules.



Ethernet RJ-45 Specifications	
Pin Number	Standard Signal Name
1	RD +
2	RD -
3	TD +
4,	Not Used
5	Not Used
6	TD -
7	Not Used
8	Not Used

ESX-100C-12W

The ESX-100C-12W Omni Switch/Router 10/100 Ethernet backbone switching module contains 12 ports that each support a fully switched 10 or 100 Mbps connection in full- or half-duplex mode. This module provides high-speed backbone connectivity. It also supports backbone features such as 802.1q and OmniChannel. Each port can auto-sense the connection speed and automatically switch at that speed. You configure whether you want to use the auto-sensing functionality through the **10/100cfg** command.

By default, each port is configured to operate in half-duplex, auto-sensing mode. You can configure full-duplex mode on each port through **10/100cfg**. Auto-sensing may be disabled to allow you to manually configure ports through the **10/100cfg** command. An additional software command, **10/100vc**, allows you to view the current line speed and link mode of each port connection. The **10/100cfg** and **10/100vc** commands are described in Chapter 19, “Managing Ethernet Modules.”

The 12 RJ-45 ports may connect to unshielded or unshielded twisted pair (UTP) cable (see *ESX-100C-12W Technical Specifications* on page 3-17 for more information). Each port may connect to a single high-speed device or a hub serving multiple devices. The ESX-100C-12W can be used as a network backbone or in the wiring closet with a mix of 10 Mbps and 100 Mbps workstations.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

ESX-100C-12W Technical Specifications	
Number of ports	12
Connector Type	RJ-45
Standards Supported	IEEE 802.3; IAB RFCs 826, 894
Data Rate	10 or 100 Mbps (full or half duplex)
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	4,096
Connections Supported	10BaseT hub or device 100BaseTx hub or device
Cable Supported	10BaseT Unshielded twisted-pair (UTP) 100BaseTx Unshielded twisted-pair: Category 5, EIA/TIA 568 Shielded twisted-pair Category 5, 100 ohm
Maximum Cable Distance	100 m
Current Draw	5.75 amps without an HRE-X 7.25 amps with an HRE-X

This 10/100 Ethernet module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number. Definitions for the LEDs are given below.

RX (Receive). On Green when the corresponding port is receiving data.

TX (Transmit). On Green when the corresponding port is transmitting data.

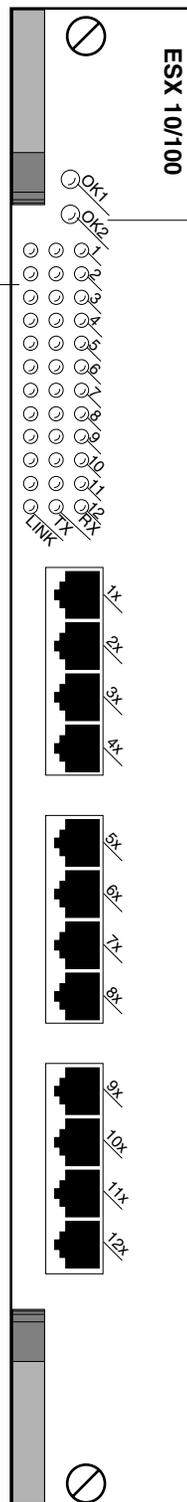
LINK (Link Status/Disabled). On Green when the corresponding port has a valid physical link and a signal is present. Under normal conditions, this LED should always be on when a cable is connected.

Port LEDs

Module LEDs

OK1 (Hardware Status). On Green when the module has passed diagnostic tests successfully. On Amber when the hardware has failed diagnostics or if the corresponding image file for the module is not in flash memory.

OK2 (Software Status). Blinking Green when the module software was downloaded successfully and the module is communicating with the MPX. Blinking Amber when the module is in a transitional state. On solid Amber if the module failed to download software from the MPX.



12-Port Auto-Sensing 10/100 Ethernet Switching Module

ESX-100C-32W

The ESX-100C-32W Omni Switch/Router 10/100 Ethernet switching module contains 32 ports that each support a fully switched 10 or 100 Mbps connection in full- or half-duplex mode. This module offers high density 10/100 connectivity for desktop connections. Each port can auto-sense the connection speed and automatically switch at that speed. You configure whether you want to use the auto-sensing functionality through the **10/100cfg** command.

By default, each port is configured to operate in half-duplex, auto-sensing mode. You can configure full-duplex mode on each port through **10/100cfg**. Auto-sensing may be disabled to allow you to manually configure ports through the **10/100cfg** command. An additional software command, **10/100vc**, allows you to view the current line speed and link mode of each port connection. The **10/100cfg** and **10/100vc** commands are described in Chapter 19, “Managing Ethernet Modules.”

The 32 RJ-45 ports may connect to unshielded or shielded twisted pair (UTP) cable (see *ESX-100C-32W Technical Specifications* on page 3-20 for more information). Each port may connect to a single high-speed device or a hub serving multiple devices. The ESX-100C-32W can be used in the wiring closet with a mix of 100 Mbps Ethernet devices and 10 Mbps Ethernet devices that are transitioning to higher speed connections.

Module ports are divided into four (4) banks of eight (8) ports. Ports are numbered from 1 to 8 within each of the four banks. The four banks are labelled **A**, **B**, **C**, and **D**. This grouping simplifies the display of LEDs, which are organized as a matrix (see *32-Port Auto-Sensing 10/100 Ethernet Switching Module* on page 3-21). Software commands will number these ports 1 through 32, with Port **A1** as 1, Port **B1** as 9, **C1** as 17, **D1** as 25, etc.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

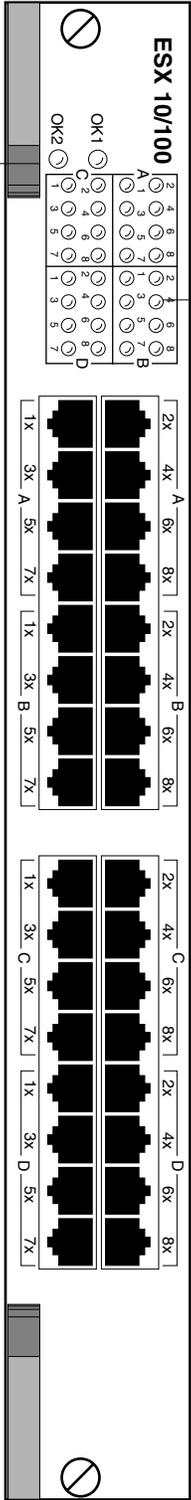
◆ Note ◆

OmniChannel is not supported on the ESX-100C-32W. It is, however, supported on the ESX-100C-12W (see *ESX-100C-12W* on page 3-16) and on the ESX-100FM/FS-12W (see *ESX-100FM/FS-12W* on page 3-25).

ESX-100C-32W Technical Specifications	
Number of ports	32
Connector Type	RJ-45
Standards Supported	IEEE 802.3; IAB RFCs 826, 894
Data Rate	10 or 100 Mbps (full or half duplex)
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024
Connections Supported	10BaseT hub or device 100BaseTx hub or device
Cable Supported	10BaseT Unshielded twisted-pair (UTP) 100BaseTx Unshielded twisted-pair: Category 5, EIA/TIA 568 Shielded twisted-pair Category 5, 100 ohm
Maximum Cable Distance	100 m
Current Draw	11.25 amps without an HRE-X 12.75 amps with an HRE-X

Please refer to *12-Port Auto-Sensing 10/100 Ethernet Switching Module* on page 3-18 for further information on these LEDs.

Module LEDs



Port LEDs

Each LED corresponds to a port on the module. When an LED is on Green continuously, a good cable connection exists. The LED will blink Green when traffic is transmitted or received on the port.

32-Port Auto-Sensing 10/100 Ethernet Switching Module

ESX-K-100C-32W

The ESX-K-100C-32W Omni Switch/Router 10/100 Ethernet switching module contains 32 ports that each support a fully switched 10 or 100 Mbps connection in full- or half-duplex mode. This module offers high density 10/100 connectivity for desktop connections. Each port can auto-sense the connection speed and automatically switch at that speed. You configure whether you want to use the auto-sensing functionality through the **10/100cfg** command.

By default, each port is configured to operate in half-duplex, auto-sensing mode. You can configure full-duplex mode on each port through **10/100cfg**. Auto-sensing may be disabled to allow you to manually configure ports through the **10/100cfg** command. An additional software command, **10/100vc**, allows you to view the current line speed and link mode of each port connection. The **10/100cfg** and **10/100vc** commands are described in Chapter 19, “Managing Ethernet Modules.”

The 32 RJ-45 ports may connect to unshielded or shielded twisted pair (UTP) cable (see *ESX-K-100C-32W Technical Specifications* on page 3-23 for more information). Each port may connect to a single high-speed device or a hub serving multiple devices. The ESX-K-100C-32W can be used in the wiring closet with a mix of 100 Mbps Ethernet devices and 10 Mbps Ethernet devices that are transitioning to higher speed connections.

Module ports are divided into four (4) banks of eight (8) ports. Ports are numbered from 1 to 8 within each of the four banks. The four banks are labelled **A**, **B**, **C**, and **D**. This grouping simplifies the display of LEDs, which are organized as a matrix (see *32-Port Advanced Auto-Sensing 10/100 Ethernet Switching Module* on page 3-24). Software commands will number these ports 1 through 32, with Port **A1** as 1, Port **B1** as 9, **C1** as 17, **D1** as 25, etc.

The ESX-K-100C-32W takes advantage of new Gigabit Ethernet/Fast Ethernet ASIC technology known as “Kodiak.” This module provides 4 priority levels and 256 queues per Kodiak ASIC.

◆ Note ◆

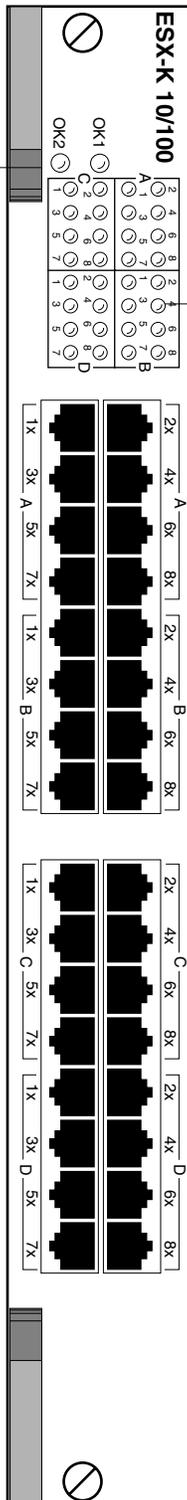
Kodiak-based modules support up to 4 levels of priority (0-1, 2-3, 4-5, 6-7). This is *not* compatible with the implementation of VLAN priority of Mammoth-based modules. Kodiak based priority VLANs can only be used with other Kodiak based priority VLANs.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

ESX-K-100C-32W Technical Specifications	
Number of ports	32
Connector Type	RJ-45
Standards Supported	IEEE 802.3; IAB RFCs 826, 894
Data Rate	10 or 100 Mbps (full or half duplex)
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	ESX-K-100C-32W: 1,024 ESX-K-100C-32W4: 4,096
Connections Supported	10BaseT hub or device 100BaseTx hub or device
Cable Supported	10BaseT Unshielded twisted-pair (UTP) 100BaseTx Unshielded twisted-pair: Category 5, EIA/TIA 568 Shielded twisted-pair Category 5, 100 ohm
Maximum Cable Distance	100 m
Current Draw	10.25 amps without an HRE-X 11.75 amps with an HRE-X

Please refer to *12-Port Auto-Sensing 10/100 Ethernet Switching Module* on page 3-18 for further information on these LEDs.

Module LEDs



Port LEDs

Each LED corresponds to a port on the module. When an LED is on Green continuously, a good cable connection exists. The LED will blink Green when traffic is transmitted or received on the port.

32-Port Advanced Auto-Sensing 10/100 Ethernet Switching Module

Fast (100 Mbps) Ethernet Modules

Alcatel's Omni Switch/Router Fast Ethernet modules can be used to connect networks with 100 Mbps workstations or as a network backbone.

The following Omni Switch/Router Fast Ethernet modules are available:

- ESX-100FM/FS-12W Twelve (12) Fast Ethernet (100 Mbps) backbone connections using MT-RJ ports.
- ESX-K-100FM/FS-16W Advanced switching module with sixteen (16) Fast Ethernet (100 Mbps) backbone connections using MT-RJ ports.

These modules are described and illustrated in the following sections.

ESX-100FM/FS-12W

The ESX-100FM/FS-16W Omni Switch/Router Fast Ethernet switching module has twelve (12) fiber MT-RJ ports that each support a fully-switched 100 Mbps connection in full-duplex mode. This module provides high-speed backbone connectivity. It also supports backbone features such as 802.1q and OmniChannel. Each port uses the full 100 Mbps of bandwidth in each direction (see *ESX-100FM/FS-12W Technical Specifications* on page 3-26). The single mode version is referred to as the ESX-100FS-12W; the multimode version is referred to as the ESX-100FM-12W. Multimode and single mode connectors are differentiated by color: multimode connectors are black and single mode connectors are blue.

◆ Note ◆

If your network currently uses SC connectors, you can order MT-RJ-to-SC cables from Alcatel.

The MT-RJ fiber port supports full-duplex operation. You can configure half-duplex mode on each port through **10/100cfg**. An additional software command, **10/100vc**, allows you to view the current line speed and link mode of each port connection. The **10/100cfg** and **10/100vc** commands are described in Chapter 19, "Managing Ethernet Modules."

The ESX-100FM/FS-12W is best used as a backbone connection in networks where Fast Ethernet is used as the backbone media. Each 100Base-Fx port may also connect to a single high-traffic device, such as a mail or file server.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

ESX-100FM/FS-12W Technical Specifications	
Number of ports	12
Connector Type	MT-RJ
Standards Supported	IEEE 802.3; IAB RFCs 826, 894
Data Rate	100 Mbps (full duplex)
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	4,096
Connections Supported	100Base-Fx connection to backbone or server
Cable Supported	Multimode: 62.5/125 micron multimode fiber Single mode: single mode fiber
Optical output power	Multimode: -19 to -14 dBm Single-mode: -20 to -14 dBm
Optical receiver sensitivity	Multimode: -31 dBm Max. Single-mode: -31 dBm Max.
Cable Distance	Multimode: approximately 2 km Single-mode: approximately 15 km
Current Draw	10.0 amps without an HRE-X 11.5 amps with an HRE-X

Warning Label. This label indicates that the module contains an optical transceiver).

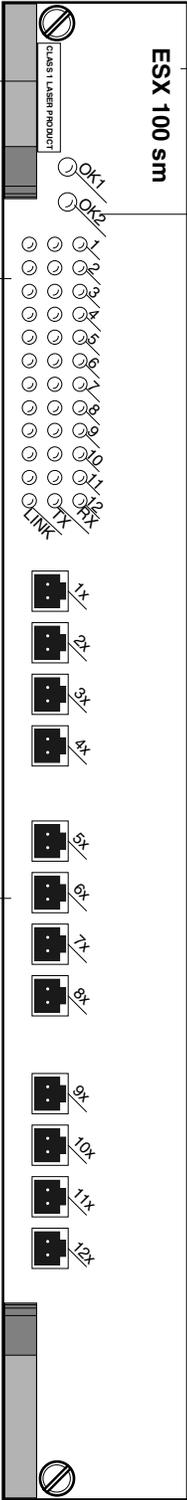
This Fast Ethernet module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number. Definitions for the LEDs are given below.

RX (Receive). On Green when the corresponding port is receiving data.

TX (Transmit). On Green when the corresponding port is transmitting data.

LINK (Link Status/Disabled). On Green when the corresponding port has a valid physical link and a signal is present. Under normal conditions, this LED should always be on when a cable is connected.

MT-RJ connectors will be color coded to indicate multimode (Black) or single mode (Blue).



Module Label. This label will indicate the ESX-100FM/FS-12W type. It will read either **ESX 100 mm** (multimode cable) or **ESX 100 sm** (single mode cable).

Module LEDs Please refer to *12-Port Auto-Sensing 10/100 Ethernet Switching Module* on page 3-18 for further information on these LEDs.

12-Port Fast Ethernet Switching Module

ESX-K-100FM/FS-16W

The ESX-K-100FM/FS-16W Omni Switch/Router Fast Ethernet switching module has sixteen (16) fiber MT-RJ ports that each support a fully-switched 100 Mbps connection in full-duplex mode. This module provides high-speed backbone connectivity. It also supports backbone features such as 802.1q and OmniChannel. Each port uses the full 100 Mbps of bandwidth in each direction (see *ESX-K-100FM/FS-16W Technical Specifications* on page 3-29). The single mode version is referred to as the ESX-K-100FS-16W; the multimode version is referred to as the ESX-K-100FM-16W. Multimode and single mode connectors are differentiated by color: multimode connectors are black and single mode connectors are blue.

◆ Note ◆

If your network currently uses SC connectors, you can order MT-RJ-to-SC cables from Alcatel.

The MT-RJ fiber port supports full-duplex operation. You can configure half-duplex mode on each port through **10/100cfg**. An additional software command, **10/100vc**, allows you to view the current line speed and link mode of each port connection. The **10/100cfg** and **10/100vc** commands are described in Chapter 19, “Managing Ethernet Modules.”

The ESX-K-100FM/FS-16W is best used as a backbone connection in networks where Fast Ethernet is used as the backbone media. Each 100Base-Fx port may also connect to a single high-traffic device, such as a mail or file server.

The ESX-K-100FM/FS-16W takes advantage of new Gigabit Ethernet/Fast Ethernet ASIC technology known as “Kodiak.” This module has provides 4 priority levels and 256 queues per Kodiak ASIC.

◆ Note ◆

Kodiak-based modules support up to 4 levels of priority (0-1, 2-3, 4-5, 6-7). This is *not* compatible with the implementation of VLAN priority of Mammoth-based modules. Kodiak based priority VLANs can only be used with other Kodiak based priority VLANs.

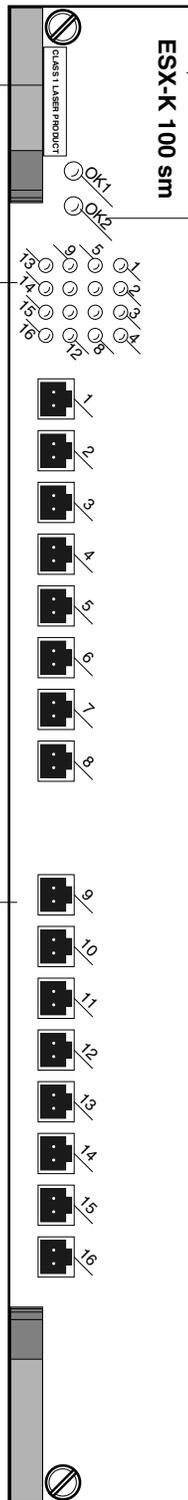
With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

ESX-K-100FM/FS-16W Technical Specifications	
Number of ports	16
Connector Type	MT-RJ
Standards Supported	IEEE 802.3; IAB RFCs 826, 894
Data Rate	100 Mbps (full duplex)
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	8,192
Connections Supported	100Base-Fx connection to backbone or server
Cable Supported	Multimode: 62.5/125 micron multimode fiber Single mode: single mode fiber
Optical output power	Multimode: -19 to -14 dBm Single-mode: -20 to -14 dBm
Optical receiver sensitivity	Multimode: -31 dBm Max. Single-mode: -31 dBm Max.
Cable Distance	Multimode: approximately 2 km Single-mode: approximately 15 km
Current Draw	9.75 amps without an HRE-X 11.25 amps with an HRE-X

Warning Label. This label indicates that the module contains an optical transceiver).

Each LED corresponds to a port on the module. When an LED is on Green continuously, a good cable connection exists. The LED will blink Green when traffic is transmitted or received on the port.

MT-RJ connectors will be color coded to indicate multimode (Black) or single mode (Blue).



Module Label. This label will indicate the ESX-100FM/FS-16W type. It will read either **ESX-K 100 mm** (multimode cable) or **ESX-K 100 sm** (single mode cable).

Module LEDs Please refer to *12-Port Auto-Sensing 10/100 Ethernet Switching Module* on page 3-18 for further information on these LEDs.

16-Port Advanced Fast Ethernet Switching Module

10 Mbps Ethernet Modules

Alcatel's Omni Switch/Router 10 Mbps Ethernet modules can be used to connect networks with 10 Mbps workstations. The following Omni Switch/Router Fast Ethernet modules is available:

- ESX-FM-24W Twelve (12) Fast Ethernet (100 Mbps) backbone connections using VF-45 ports.

This module is described and illustrated in the following sections.

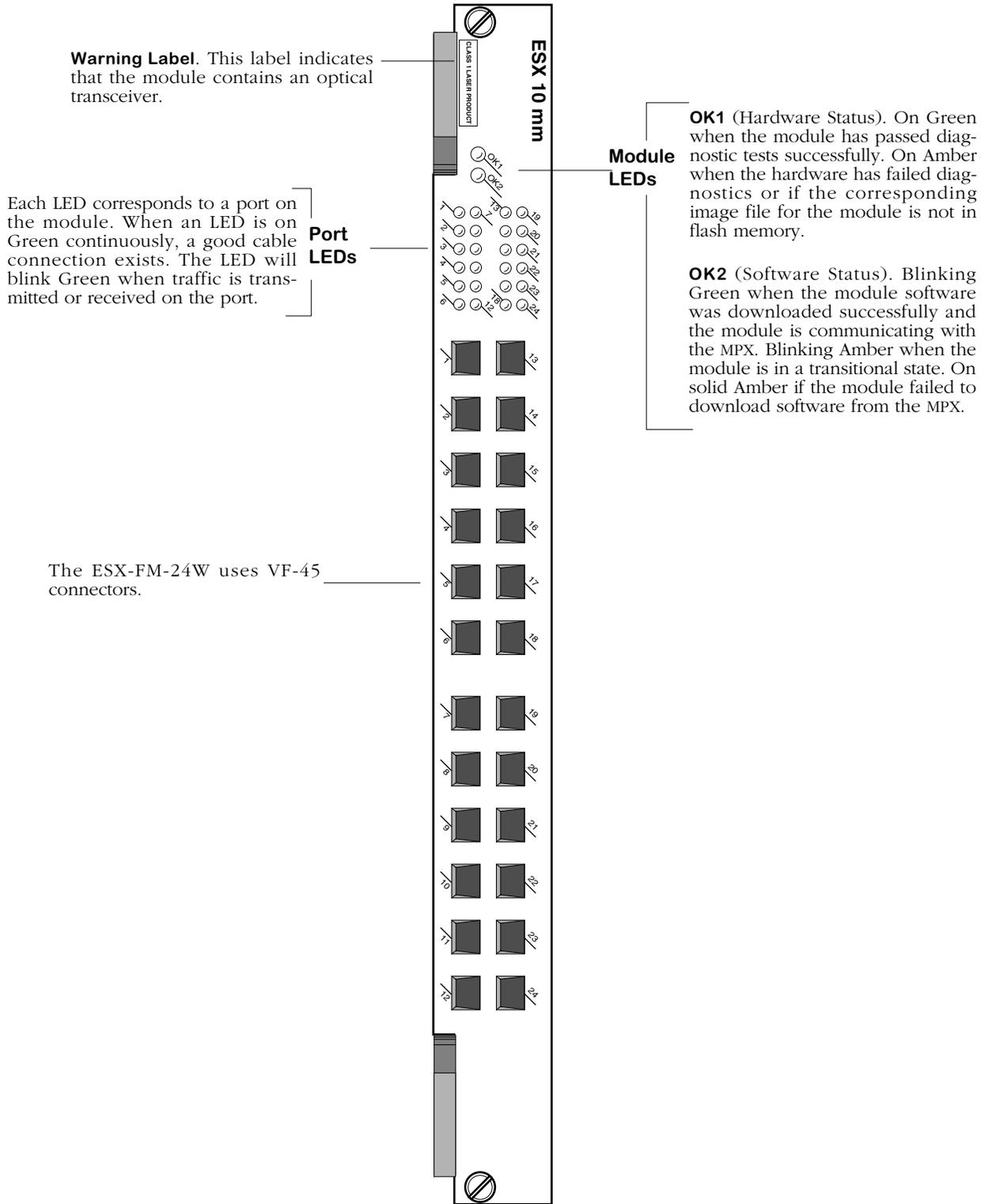
ESX-FM-24W

The ESX-FM-24W switching module contains twenty-four (24) 10BaseFl ports. Each port connection supports one switched Ethernet segment at the full 10 Mbps of bandwidth. The ESX-FM-24W uses VF-45 connectors. Each port supports multimode fiber connections to desk-top devices. See *ESX-FM-24W Technical Specifications* on page 3-32 for more information.

By default, each port is configured to operate in full-duplex mode. You can configure half-duplex mode on each port through **10/100cfg**. An additional software command, **10/100vc**, allows you to view the current link mode of each port connection. The **10/100cfg** and **10/100vc** commands are described in Chapter 19, "Managing Ethernet Modules."

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

ESX-FM-24W Technical Specifications	
Number of ports	24
Connector Type	Fiber VF-45
Standards Supported	IEEE 802.3; IAB RFCs 826, 894
Data Rate	10 Mbps (full duplex)
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024
Connections Supported	10BaseFl connection to desktop
Cable Supported	multimode fiber
Optical output power	-20 to -14 dBm
Optical receiver sensitivity	-33 to -31 dBm
Cable Distance	approximately 2 km
Current Draw	13.0 amps without an HRE-X 14.5 amps with an HRE-X



24-Port 10 Mbps Ethernet Switching Module with VF-45 Connectors

Token Ring Modules

Omni Switch/Router Token Ring modules support Lobe (TSX-C-32W and TSX-CD-16W) and Station (TSX-CD-16W only) configurations. Module ports can connect existing Token Ring Multistation Access Units (MAUs), hubs, and devices. These modules support Transparent Bridging (TB), Source Route Transparent Bridging (SRT), and Source Route Bridging (SRB), IEEE 802.1d, IBM Spanning Tree, port mirroring, RMON, and standard MIBs.

Token Ring ports support a fully switched connection at either 4 or 16 Mbps. In addition, these ports are configurable through software. You can set the ring speed (4 or 16 Mbps), active monitor participation, and frame copied bit variables for all ports. In addition, a variety of error and configuration statistics are available through software commands. See Chapter 21, "Managing Token Ring Modules," for further information on software configuration and monitoring commands.

Omni Switch/Router Token Ring modules also support virtual rings. This feature allows you to group Token Ring ports on an Omni Switch/Router as one logical ring with a common ring number. With virtual rings, you can micro-segment physical Token Rings into smaller, more manageable virtual rings without changing end-station configurations or making any topology changes. Broadcast traffic is also decreased by eliminating source route hops.

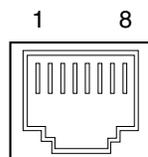
The following Omni Switch/Router Token Ring modules are available:

- TSX-C-32W Thirty-two (32) UTP or STP RJ-45 ports that support desktop connections.
- TSX-CD-16W Sixteen (16) UTP or STP RJ-45 ports that support desktop or MAU connections.

These modules are described and illustrated in the following sections.

Token Ring RJ-45 Pinouts

The figure and table below illustrate the pinouts used on RJ-45 ports in Omni Switch/Router token ring modules.



Token Ring RJ-45 Specifications	
Pin Number	Standard Signal Name
1	Not used
2	Not used
3	TX -
4	RX +
5	RX -
6	TX +
7	Not used
8	Not used

TSX-C-32W

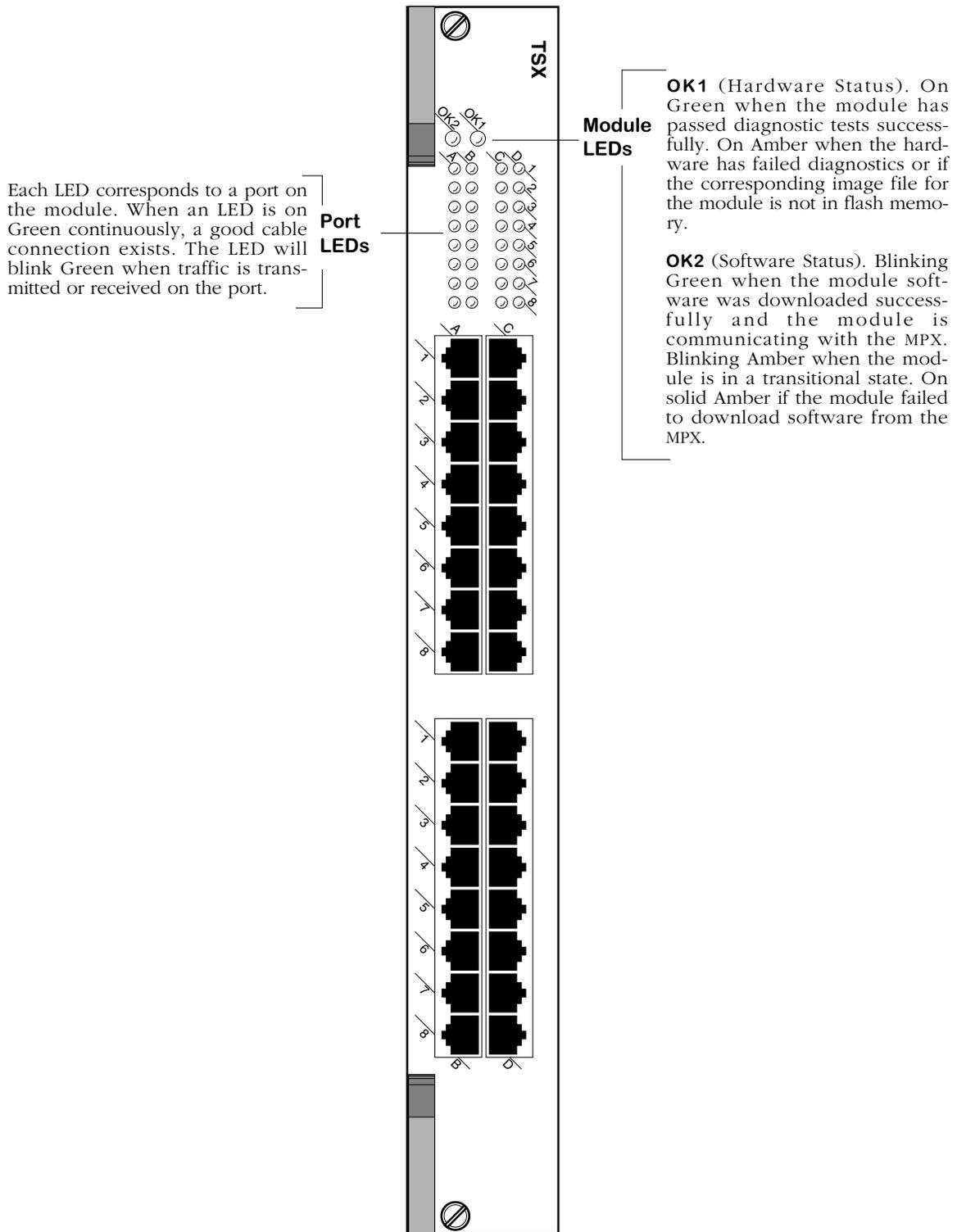
The TSX-C-32W allows you to connect to Token Ring workstations. This module contains thirty-two (32) active ports that may support either unshielded twisted pair (UTP) or shielded twisted pair (STP) connections (see *TSX-C-32W Technical Specifications* on page 3-35 for more information). The ports each support a fully switched connection at either 4 or 16 Mbps in full- or half-duplex mode. The Ring Speed is configurable through the **tpcfg** command. Ports are Lobe only, supporting connections to desktop devices. By default, ports are auto-sensing 4/16 Mbps and full/half duplex mode. If you disable auto sensing with the **tpcfg** command, you can configure an individual port's ring speed (4 or 16 Mbps) and duplex mode (full or half).

If the TSX-C-32W is set to auto-configuration mode (the default), switch software will automatically modify the Ring Speed if there is a discrepancy with the ring to which the port is connected. (The new Ring Speed, however, is not saved in the system configuration file, **mpm.cfg**.)

Module ports are divided into four (4) banks of eight (8) ports. Ports are numbered from 1 to 8 within each of the four banks. The four banks are labelled **A**, **B**, **C**, and **D**. This grouping simplifies the display of LEDs, which are organized as a matrix (see *32-Port Token Ring Switching Module* on page 3-36). Software commands will number these ports 1 through 32, with Port **A1** as 1, Port **B1** as 9, **C1** as 17, **D1** as 25, etc.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

TSX-C-32W Technical Specifications	
Number of ports	32
Connector Type	Shielded RJ-45 (UTP or STP)
Standards Supported	IEEE 8-2.5r
Data Rate	4 or 16 Mbps (full or half-duplex)
Maximum Frame Size	8,144 bytes
MAC Addresses Supported	1,024
Connections Supported	Desktop devices
Cable Supported	Shielded twisted pair (STP) —100 or 150 ohm <ul style="list-style-type: none"> • IBM Type 1 Unshielded twisted pair (UTP) —100 ohm <ul style="list-style-type: none"> • IBM Type 3 • ANSI Category 3, 4, or 5
Maximum Cable Distance	100 m
Current Draw	9.25 amps without an HRE-X 10.75 amps with an HRE-X



32-Port Token Ring Switching Module

TSX-CD-16W

The TSX-CD-16W allows you to configure individual ports as Station or Lobe connections. As a Station port, you can connect existing Token Ring MAUs and hubs to your Omni Switch/Router network. As a Lobe connection, you can connect Omni Switch/Routers to high-traffic Token Ring workstations or servers.

This module contains sixteen (16) active ports that may support either unshielded twisted pair (UTP) or shielded twisted pair (STP) connections (see *TSX-CD-16W Technical Specifications* on page 3-38 for more information). The ports each support a fully switched connection at either 4 or 16 Mbps in full- or half-duplex mode. The Ring Speed is configurable through the **tpcfg** command. By default, ports are auto-sensing 4/16 Mbps, Station/Lobe, and full/half duplex mode. If you disable auto sensing with the **tpcfg** command, you can configure an individual port's ring speed (4 or 16 Mbps), port mode (Station or Lobe) and duplex mode (full or half).

If the TSX-CD-16W is set to auto-configuration mode (the default), switch software will automatically modify the Ring Speed if there is a discrepancy with the ring to which the port is connected. A TSX-CD-16W port detects this difference in Ring Speed as it is inserted into the ring, then it resets itself and comes up in the new Ring Speed. (The new Ring Speed, however, is not saved in the system configuration file, **mpm.cfg**.) Once the port inserts into the ring, automatic Ring Speed detection is disabled (i.e., thereafter the port will not change speed automatically). Both Station and Lobe connections handle automatic speed detection this way.

If a TSX-CD-16W port is set to auto-configuration mode and it is the first device on the ring, the TSX-CD-16W will attempt to auto sense the ring speed every 18 seconds until there is an insertion of another device on the ring. The port does not reset to match the Ring Speed—its speed becomes the Ring Speed. If the port is not the first device, then it will auto-detect the ring speed and match that speed as described in the preceding paragraph.

The TSX-CD-16W module can auto-detect Station/Lobe mode. In addition, you can change an individual port from Lobe to Station or Station to Lobe with the **tpcfg** command. See Chapter 21, "Managing Token Ring Modules," for more information on the **tpcfg** command.

Module ports are divided into two (2) banks of eight (8) ports. Ports are numbered from 1 to 8 within each of the two banks. The two banks are labelled **A** and **B**. This grouping simplifies the display of LEDs, which are organized as a matrix (see *16-Port Token Ring Switching Module* on page 3-39). Software commands will number these ports 1 through 16, with Port **A1** as 1, Port **A2** as 2, **B1** as 9, **B2** as 10, etc.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

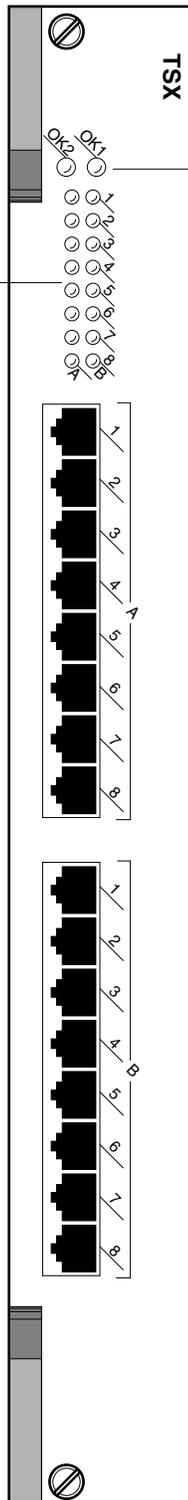
TSX-CD-16W Technical Specifications	
Number of ports	16
Connector Type	Shielded RJ-45 (UTP or STP)
Standards Supported	IEEE 8-2.5r
Data Rate	4 or 16 Mbps (full- or half duplex)
Maximum Frame Size	8,144 bytes
MAC Addresses Supported	4,096
Connections Supported	Desktop devices and MAUs
Cable Supported	Shielded twisted pair (STP) —100 or 150 ohm <ul style="list-style-type: none">• IBM Type 1 Unshielded twisted pair (UTP) —100 ohm <ul style="list-style-type: none">• IBM Type 3• ANSI Category 3, 4, or 5
Maximum Cable Distance	100 m
Current Draw	7.0 amps without an HRE-X 8.5 amps with an HRE-X

Each LED corresponds to a port on the module. When an LED is on Green continuously, a good cable connection exists. The LED will blink Green when traffic is transmitted or received on the port.

Port LEDs

Module LEDs

Please refer to *32-Port Token Ring Switching Module* on page 3-36 for further information on these LEDs.



16-Port Token Ring Switching Module

ATM Uplink Modules

ATM uplink (ASX) switching modules allow you to connect the Omni Switch/Router to ATM servers, backbones, and switches. Omni Switch/Router ATM uplink modules currently support OC-3 (155 Mbps), OC-12 (622 Mbps), DS3, and E3 interfaces and include the following:

- ASX-155FM/FS/FH-1W/2W One or two single mode or multimode fiber OC-3 ports.
- ASX-155RFM/RFS-1W One single mode or multimode fiber OC-3 port pairs (redundant). The port pair contains a primary and backup port.
- ASX-622RFM/RFS-1W One-port redundant fiber single mode or multimode OC-12 switching module. The port pair includes a primary and backup port.
- ASX-M-622RFM/RFS/RFH-1W One-port redundant fiber single mode or multimode fiber OC-12 port.
- ASX-DS3-1W/2W One or two port DS3 switching module.
- ASX-E3-1W/2W One or two port E3 switching module.

The OC-3 modules are suited for connecting the switch to an ATM campus backbone or directly to an ATM server.

Through the use of Point-to-Point Bridging (RFC 1483), you can extend all LAN traffic over the ATM backbone. Several Omni Switch/Routers could be connected over one or more backbones. In such a configuration, you combine the flexibility of the Omni Switch/Router's any-to-any switching with the power and speed of the ATM backbone without the use of an ATM backbone switch.

If you are connecting the Omni Switch/Router directly to an ATM server, then all non-ATM devices in the LAN can communicate with the high-speed ATM server through the Omni Switch/Router.

If your network uses ATM backbone switches, then the Omni Switch/Router ATM modules allow all non-ATM devices in the network to have access to the ATM network through the use of LAN Emulation (LANE) or an Alcatel version of LANE called XLANE, or "VLAN Clusters." XLANE connects Omni Switch/Routers and OmniStack switches together across ATM and legacy LAN networks to gain the benefits of LANE while eliminating interoperability issues. Classical IP (RFC 1577) may also be used to extend LAN traffic over ATM.

ASX ports allow you to configure several traffic parameters, including Peak Cell Rate (PCR), Sustaining Cell Rate (SCR), and Maximum Burst Size (MBS). You can divide ASX ports into discrete "bandwidth groups." Unique PCR, SCR, and MBS values can be assigned to bandwidth groups. This feature, called "traffic shaping," takes place on data that is exiting (i.e., transmitted out) a switch port.

Software controls on the switch allow you to control and monitor activity on ASX modules. On each ATM port, you can configure the connection type (SVC or PVC), Virtual Channel Connections (VCC), segment sizes, and loopback controls. On each VCC, you can configure Quality of Service (QoS), Best Effort, Traffic Descriptor, and Peak Cell Rate variables. In addition, you can configure all ATM bridging and trunking services (Point-to-Point Bridging, LANE, XLANE, Classical IP). See Chapter 33, “Managing ATM Access Modules,” and Chapter 36, “Configuring ATM Services,” for further information on ATM software controls.

◆ Note ◆

Peak cell rates will not be initialized if you replace an ASX module with a slower-speed ASX module in the same slot. (For example, you replace an ASX-155FM-1W with an ASX-DS3-1W.)

ASX-155FM/FS/FH

The ASX-155FM/FS/FH switching module contains one (1) or two (2) fiber (SC) ports that support OC-3 connections. The port connections provide 155 Mbps of bandwidth and connect to either multimode, intermediate-reach single mode, or long-reach single mode cable. The ASX-155FM/FS/FH can be factory configured with single mode or multimode fiber ports (see *ASX-155FM/FS/FH Technical Specifications* on page 3-43 for more information). The intermediate-reach single mode version is referred to as the ASX-155FS; the long-haul (Category 2 laser) single mode version is referred to as the ASX-155FH; and the multimode version is referred to as the ASX-155FM. Connector types are differentiated by color: multimode connectors are black, long-haul single mode connectors are yellow, and intermediate-reach single mode connectors are blue.

The ASX-155FM/FS/FH is ideally suited for connections to an ATM campus fiber backbone. Using point-to-point bridging (RFC 1483), you can extend all devices (ATM and non-ATM) connected to an Omni Switch/Router over the ATM fiber backbone without the use of a high-end ATM switch.

The ASX-155FM/FS/FH switching module is actually a daughtercard that attaches to an Omni Switch/Router High-Speed Module (HSX). The HSX provides the base memory and processing power for these high throughput switching modules.

The HSX contains RISC processors, RAM for holding software image files, ASICs for performing switching, and Content Addressable Memory (CAM) for storing MAC addresses. You plug cable directly into a submodule, but it is the HSX module that connects to the switch backplane.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

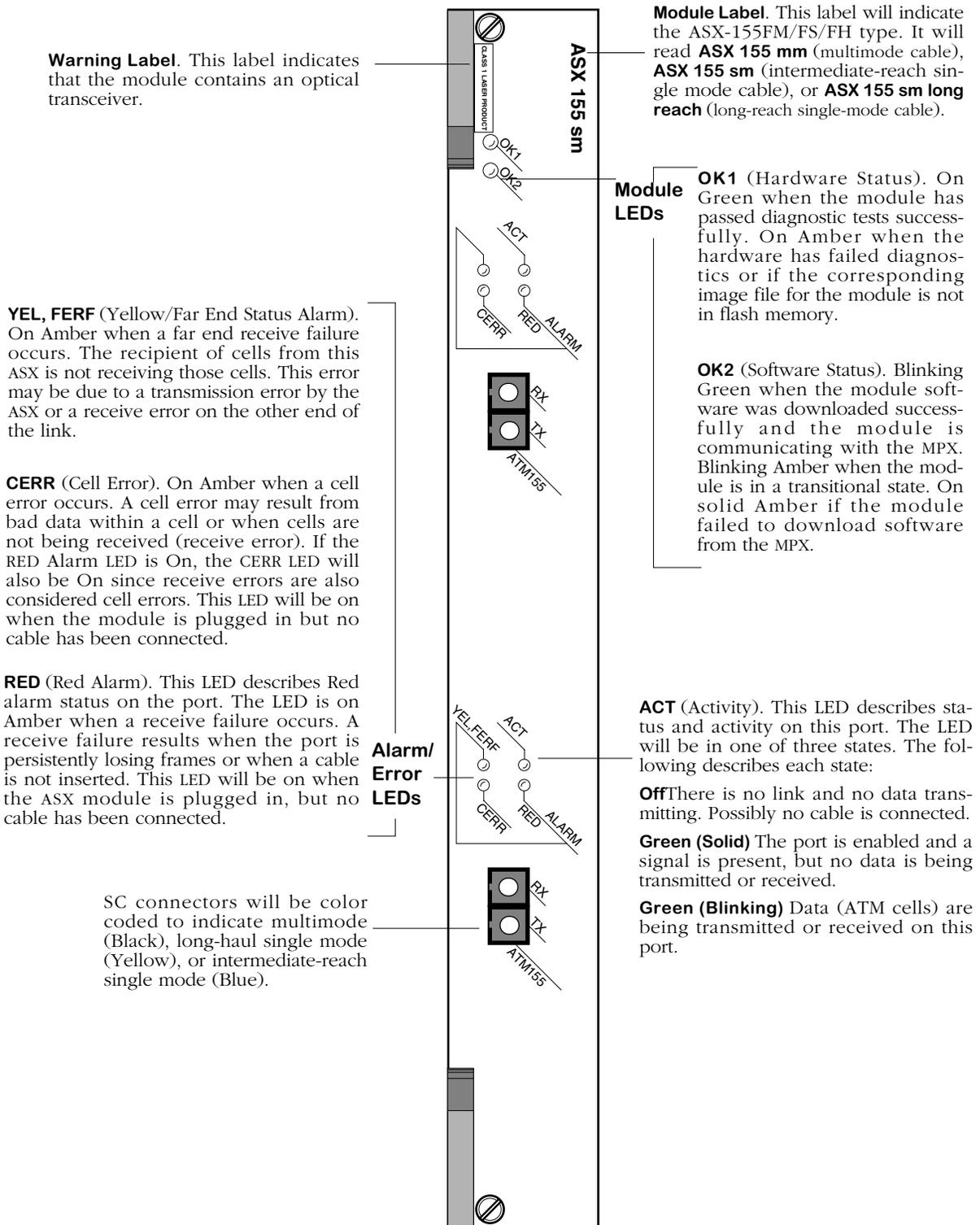
ASX-155FM/FS/FH Technical Specifications	
Number of ports	1 or 2
Connector Type	SC
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/V2.0 MPOA Client
Data Rate	155 Mbps
ATM Adaption Layers	AAL5
MAC Addresses Supported	4,096
Max. No. of VCs Supported	1,024
Connections Supported	OC-3 connections to ATM server, backbone, or switch.
Optical output power	Multimode: -19 to -14 dBm Single mode (intermediate reach): -14 to -8 dBm Single mode (long haul): -5 to 0 dBm
Optical receiver sensitivity	Multimode: -30 to -14 dBm Single mode (intermediate reach): -31 to -8 dBm Single mode (long haul): -34 (max.), -37 (typical)
Power Budget	Multimode: 11 dB Single mode (intermediate reach): 16 dB Single mode (long haul): 29 dBm
Cable Supported	Multimode: 62.5 micron multimode fiber Single mode (intermediate reach and long haul): 9 micron single mode fiber
Cable Distance	Multimode: 4.2 km Single mode (intermediate reach): 24 km Single mode (long haul): 40 km
Current Draw	1-port: 5.25 amps without an HRE-X 1-port: 6.75 amps with an HRE-X 2-port: 6.25 amps without an HRE-X 2-port: 7.75 amps with an HRE-X

◆ **Special Note** ◆

The single mode version of this module is:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.



2-Port 155 Mbps ATM Uplink Switching Module

ASX-155RFM/RFS-1W

The ASX-155RFM/RFS-1W switching module contains one (1) redundant fiber (SC) port pair that supports OC-3 connections. (Only one port in the port pair can be active at one time.) The port connections provide 155 Mbps of bandwidth and connect to either multimode or single mode cable (see *ASX-155RFM/RFS-1W Technical Specifications* on page 3-46 for more information). The ASX-155RFM/RFS-1W can be factory configured with a single mode or multimode fiber port. The single mode version is referred to as the ASX-155RFS-1W; the multimode version is referred to as the ASX-155RFM-1W. Multimode and single mode connectors are differentiated by color: multimode connectors are black and single mode connectors are blue.

The ASX-155RFM/RFS-1W is ideally suited for mission-critical ATM access connections. The redundant port pair ensures that critical backbone and server connections are protected against failures on the primary link.

The ASX-155RFM/RFS-1W switching module is actually a daughtercard that attaches to an Omni Switch/Router High-Speed Module (HSX). The HSX provides the base memory and processing power for these high throughput switching modules.

The HSX contains RISC processors, RAM for holding software image files, ASICs for performing switching, and Content Addressable Memory (CAM) for storing MAC addresses. You plug cable directly into a submodule, but it is the HSX module that connects to the switch backplane.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

ASX-155RFM/RFS-1W Technical Specifications	
Number of ports	1 port pair (the pair consists of 1 primary, 1 backup port)
Connector Type	SC
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/V2.0 MPOA Client
Data Rate	155 Mbps
ATM Adaption Layers	AAL5
MAC Addresses Supported	4,096
Max. No. of VCs Supported	1,024
Connections Supported	OC-3 connections to ATM server, backbone, or switch.
Optical output power	Multimode: -19 to -14 dBm Single mode (intermediate reach): -14 to -8 dBm
Optical receiver sensitivity	Multimode: -30 to -14 dBm Single mode (intermediate reach): -31 to -8 dBm
Power Budget	Multimode: 11 dB Single mode: 16 dB
Cable Supported	Multimode: 62.5 micron multimode fiber Single mode: 9 micron single mode fiber
Cable Distance	Multimode: 4.2 km Single mode: 24 km
Current Draw	5.75 amps without an HRE-X 7.25 amps with an HRE-X

◆ Special Note ◆

The single mode version of this module is:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

Warning Label. This label indicates that the module contains an optical transceiver.

Please refer to *2-Port 155 Mbps ATM Uplink Switching Module* on page 3-44 for further information on these LEDs.

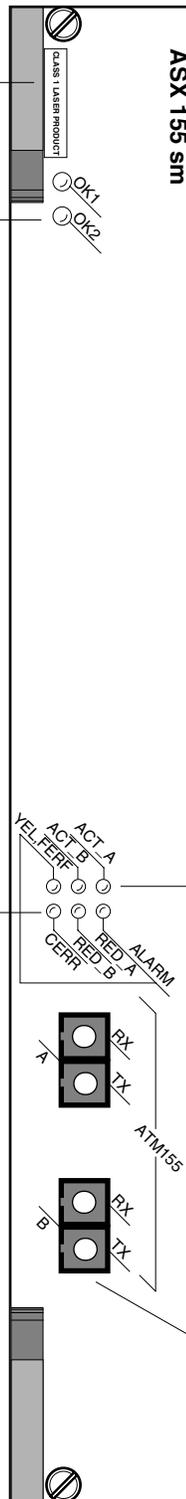
Module Label. This label will indicate the ASX-155RFM/RFS type. It will read either **ASX 155 mm** (multimode cable) or **ASX 155 sm** (single mode cable).

YEL, FERF (Yellow/Far End Status Alarm). On Amber when a far end receive failure occurs. The recipient of cells from this ASX is not receiving those cells. This error may be due to a transmission error by the ASX or a receive error on the other end of the link.

CERR (Cell Error). On Amber when a cell error occurs. A cell error may result from bad data within a cell or when cells are not being received (receive error). If the RED Alarm LED is On, the CERR LED will also be On since receive errors are also considered cell errors. This LED will be on when the module is plugged in but no cable has been connected.

RED_A and RED_B (Red Alarm). These two LEDs describe Red alarm status on Port A (**RED_A**) and Port B (**RED_B**). The LED is on Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the ASX module is plugged in, but no cable has been connected.

Alarm/Error LEDs



ACT_A and ACT_B (Activity). These two LEDs describe status and activity on Port A (**ACT_A**) and Port B (**ACT_B**). Each LED will be in one of three states. The following describes each state:

- Off** There is no link and no data transmitting. Possibly no cable is connected.
- Green (Solid)** The port is enabled and a signal is present, but no data is being transmitted or received.
- Green (Blinking)** Data (ATM cells) are being transmitted or received on this port.

SC connectors will be color coded to indicate multimode (Black) or single mode (Blue).

1-Port (Redundant) 155 Mbps ATM Uplink Switching Module

ASX-622RFS/RFM-1W

The ASX-622RFS/RFM-1W switching module contains one redundant fiber (SC) port pair that supports an OC-12 connection. (Only one port in this pair can be active at one time.) The port connection provides 622 Mbps of bandwidth and connects to either multimode or single mode cable.

The ASX-622RFS/RFM-1W can be factory configured with single mode or multimode fiber ports. The single mode version is referred to as the ASX-622RFS-1W; the multimode version is referred to as the ASX-622RFM-1W. Multimode and single mode connectors are differentiated by color: multimode connectors are black and single mode connectors are blue. See *ASX-622RFM/RFS-1W Technical Specifications* on page 3-49 for more information.

An ASX-622RFS/RFM-1W is ideally suited for mission-critical ATM access connections. The redundant port pair ensures that critical backbone and server connections are protected against failures on the primary link.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

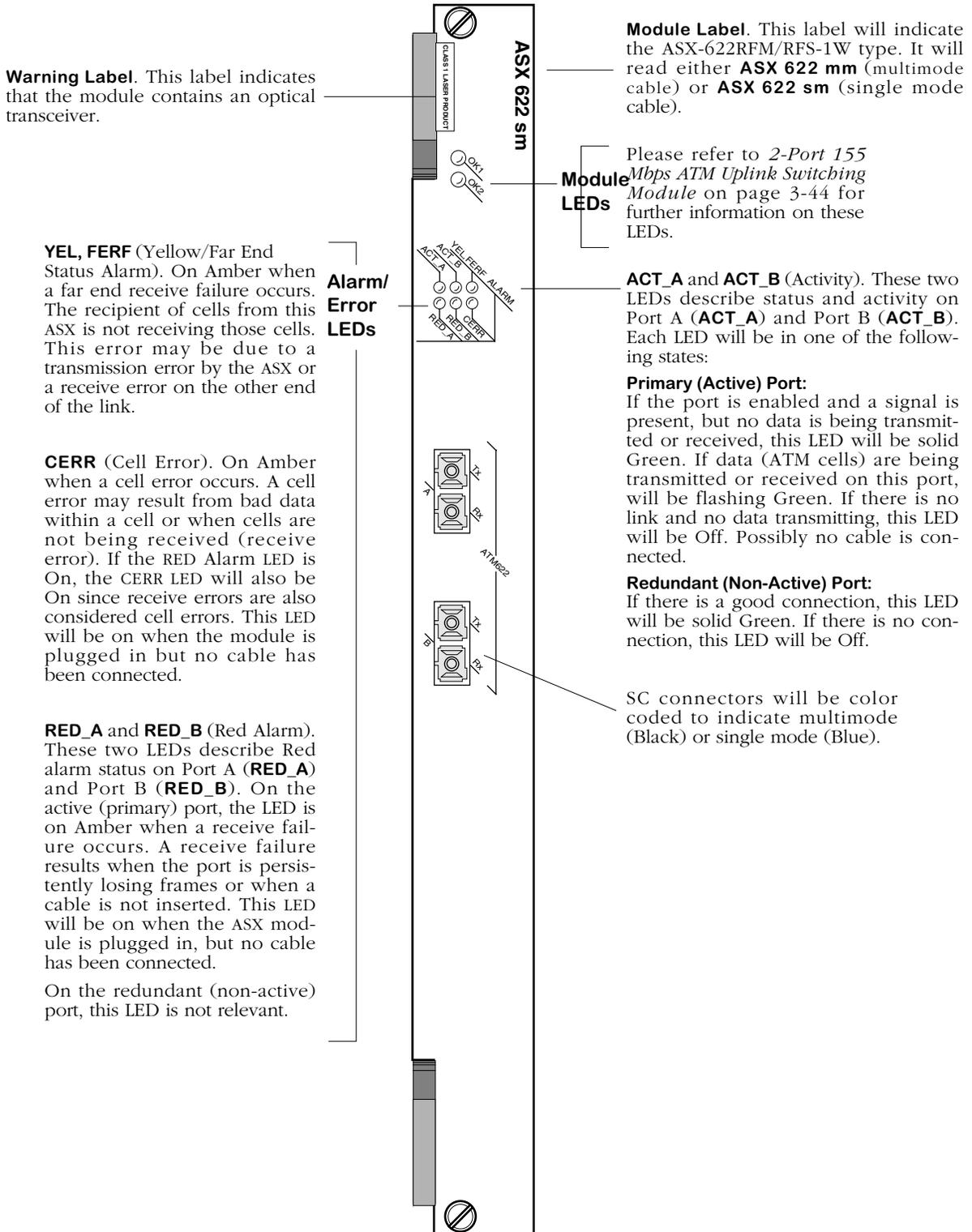
ASX-622RFM/RFS-1W Technical Specifications	
Number of ports	1 primary, 1 backup (functions as 1 port)
Connector Type	SC
Standards Supported	ANSI T1.105-1988 Digital Hierarchy — Optical Interface Rates and Formats Specification T1.624-1993 Broadband ISDN — User Network Interfaces, Rates and Formats T1E1.2/92-020 Broadband ISDN — Customer Installation Interfaces, Physical Media Dependent Specification ATM Forum User-to-Network Interface (UNI) 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/V2.0 MPOA Client
Data Rate	622 Mbps
Maximum Frame Size	8000 bytes
MAC Addresses Supported	4096
Max. No. of VCs Supported	1,024
Connections Supported	OC-12 connections to ATM servers or backbone.
Optical output power	Multimode: -20 to -14 dBm Single mode: -15 to -8 dBm
Optical receiver sensitivity	Multimode: -26 to -14 dBm Single mode: -28 to -8 dBm
Power Budget	Multimode: 6 dB Single mode: 12 dB
Cable Supported	Multimode: 62.5/125 micron multimode fiber Single mode: single mode fiber
Cable Distance	Multimode: 500 m Single mode: 15 km
Current Draw	11.0 without an HRE-X 12.5 with an HRE-X

◆ **Special Note** ◆

The single mode version of this module is:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.



1-Port (Redundant) 622 Mbps ATM Uplink Switching Module

ASX-M-622RFM/RFS/RFH-1W

The ASX-M-622RFM/RFS/RFH-1W uses a SAR ASIC known as “Maker MXT 4400.” This module provides Virtual Channel (VC)-based traffic shaping. The ASX-M-622RFM/RFS/RFH-1W switching module contains one redundant fiber (SC) port pair that supports an OC-12 connection. (Only one port in this pair can be active at one time.) The port connection provides 622 Mbps of bandwidth and connects to either multimode or single mode cable.

The port connection provides 622 Mbps of bandwidth and connect to either multimode or single mode cable. The ASX-M-622RFM/RFS/RFH-1W can be factory configured with intermediate single mode, long-reach single mode, or multimode fiber ports. The intermediate-reach single mode version is referred to as the ASX-M-622RFS-1W; the long-reach single mode version is referred to as the ASX-M-622RFH-1W; the multimode version is referred to as the ASX-M-622RFM-1W.

Multimode and single mode connectors are differentiated by a color code: multimode connectors are black, long-reach single mode connectors are yellow, and intermediate-reach single mode connectors are blue. See *ASX-M-622RFM/RFS/RFH-1W Technical Specifications* on page 3-52 for more information.

The ASX-M-622RFM/RFS/RFH-1W is suited for high-performance backbone connections to an ATM network.

With the optional HRE-X you can increase routing performance up to 12 Mpps in a fully-loaded 9-slot chassis.

◆ Note ◆

Group mobility is *not* supported on the ASX-M-622RFM/RFS/RFH-1W.

ASX-M-622RFM/RFS/RFH-1W Technical Specifications	
Number of ports	1 primary, 1 backup (functions as 1 port)
Connector Type	SC
Standards Supported	ANSI T1.105-1988 Digital Hierarchy — Optical Interface Rates and Formats Specification T1.624-1993 Broadband ISDN — User Network Interfaces, Rates and Formats T1E1.2/92-020 Broadband ISDN — Customer Installation Interfaces, Physical Media Dependent Specification ATM Forum User-to-Network Interface (UNI) 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/V2.0 MPOA Client
Data Rate	622 Mbps
Maximum Frame Size	8000 bytes
MAC Addresses Supported	4096
Max. No. of VCs Supported	1023
Connections Supported	OC-12 connections to ATM servers or backbone.

continued on next page...

ASX-M-622RFM/RFS/RFH-1W Technical Specifications (cont.)	
Optical output power	Multimode: -20 to -14 dBm Single mode (intermediate reach): -15 to -8 dBm Single mode (long reach): -5, to -3 dBm (typical)
Optical receiver sensitivity	Multimode: -26 to -14 dBm Single mode (intermediate reach): -28 to -8 dBm Single mode (long reach): -34 dBm (minimum), -36 dBm (typical)
Power Budget	Multimode: 6 dB Single mode (intermediate reach): 8 dB [check] Single mode (long reach): 10 dB
Cable Supported	Multi-Mode: 62.5 micron multimode fiber Single mode (intermediate reach): intermediate-reach single-mode fiber Single mode (long reach): long-reach single-mode fiber
Cable Distance	Multimode: 500 meters Single mode (intermediate reach): 15 km Single mode (long reach): 40 km
Current Draw	13.5 without an HRE-X 15.0 with an HRE-X

◆ **Special Note** ◆

The single mode version of this module is:

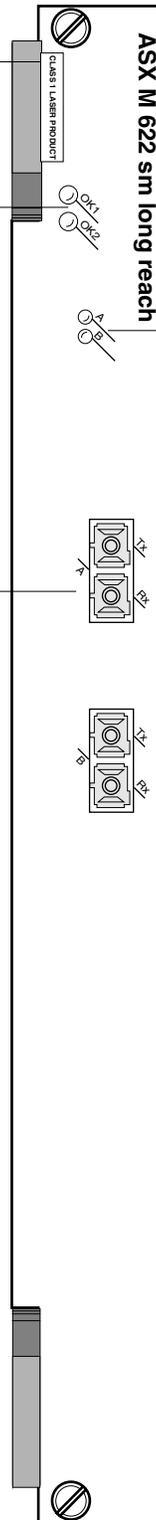
CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

Warning Label. This label indicates that the module contains an optical transceiver.

Please refer to *2-Port 155 Mbps ATM Uplink Switching Module* on page 3-44 for further information on these LEDs.

SC connectors will be color coded to indicate multimode (Black), long-haul single mode (Yellow), or intermediate-reach single mode (Blue).



Module Label. This label will indicate the ASX-M-622RF-1W type. It will read **ASX M 622 mm** (multimode cable), **ASX M 622 sm** (intermediate-reach single mode cable), or **ASX M 622 sm long reach** (long-reach single-mode cable)

The LEDs are labeled **A** or **B**, which corresponds to the port number. When an LED is on Green continuously, a good cable connection exists. The LED will blink Green when traffic is transmitted or received on the port. It will be on Amber when a cell error occurs.

Advanced 1-Port (Redundant) 622 Mbps ATM Uplink Switching Module

ASX-DS3

The ASX-DS3 switching module contains one or two BNC ports that support DS-3 connections. The port connection provides 44.736 Mbps of bandwidth and connects to coaxial (RG-59) cable. ASX-DS3 ports are suited for connections to ATM carrier services offered by North American Telcos. The ASX-DS3 port is a physical DTE (Data Termination Equipment) device that connects to a physical DCE (Data Communication Equipment) device, such as a DSU (Data Service Unit). The one-port version is called the ASX-DS3-1W; the two-port version is called the ASX-DS3-2W. See *ASX-DS3 Technical Specifications* on page 3-56 for more information.

DS-3 is a Digital Signal (DS) interface used to implement wide area, public connectivity for ATM networks. There is a hierarchy of DS services based on channel capacity. DS-0, the lowest bandwidth DS channel, provides 64 Kbps of throughput. Twenty-four (24) DS-0 channels combine to form a DS-1 (1.544 Mbps of throughput). Four DS-1 channels combine to form a DS-2 (6.312 Mbps of throughput). And seven DS-2 channels combine to form a DS-3 (44.736 Mbps of throughput).

By default the ASX-DS3 uses B3ZS line encoding. Using the **dsmod** command, you can configure the module to use C-bit parity or M23 parity and configure it for loopback controls. You should configure the ASX-DS3 module to use the same parity as the ATM service provider.

Two different mapping protocols are used to transmit ATM cells over DS-3: PLCP (Physical Layer Convergence Protocol) and ATM Direct Mapped (ADM) System. The two protocols are not compatible. Many existing DS-3 implementations use PLCP as defined in ANSI T1.624-1993, but many new implementations of DS-3 use ADM. The ASX-DS3 module supports both physical layer protocols.

The ASX-DS3 is actually a submodule, or daughtercard, that attaches to an Omni Switch/Router High-Speed Module (HSX). You plug your cable directly into the ASX-DS3 submodule, but it is the HSX module that connects to the switch backplane.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second.

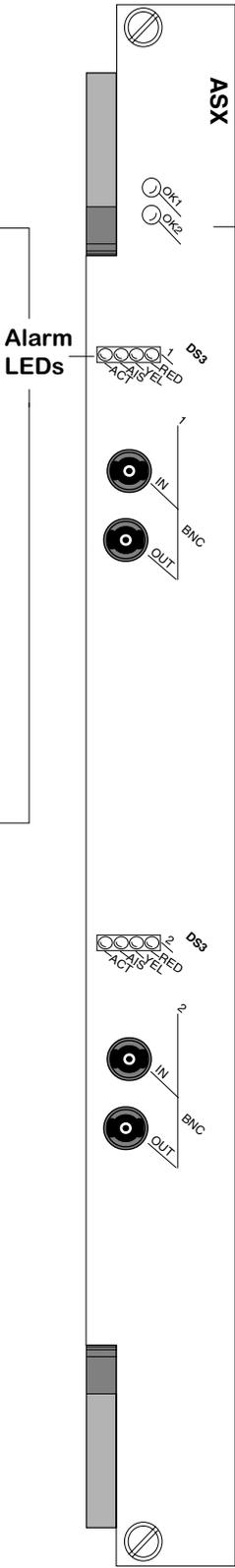
ASX-DS3 Technical Specifications	
Number of ports	1 or 2
Connector Type	BNC
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/V2.0 ANSI T1.624-1993 (PLCP Mapping) MPOA Client
Data Rate	44.736 Mbps
ATM Adaption Layers	AAL5
MAC Addresses Supported	4096
Max. No. of VCs Supported	1,024
Connections Supported	DS-3 connections to ATM carrier service.
Cable Supported	Coaxial RG-59 (75 ohm)
Cable Distance	185 m
Current Draw	ASX-DS3-1W: 5.75 amps without an HRE-X ASX-DS3-1W: 7.25 amps with an HRE-X ASX-DS3-2W: 7.25 without HRE-X ASX-DS3-2W: 8.25 with an HRE-X

RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the ASX module is plugged in, but no cable has been connected.

YEL (Yellow Alarm). On Amber when a far end receive failure occurs. The recipient of cells from this ASX is not receiving those cells. This error may be due to a transmission error by the ASX or a receive error on the other end of the link.

AIS (Alarm Indication Signal). On when a maintenance signal is sent to the ASX by the network. If this LED is on, then there has been a change in the Alarm Indication Signal (AIS).

ACT (Activity). On Green when the port is transmitting or receiving cells.



Module LEDs

Please refer to *2-Port 155 Mbps ATM Uplink Switching Module* on page 3-44 for further information on these LEDs.

ATM DS-3 Uplink Module

ASX-E3

The ASX-E3 switching module contains one or two BNC ports that support E3 connections. Each port connection provides 34.368 Mbps of bandwidth and connects to coaxial (RG-59) cable. ASX-E3 ports are suited for connections to ATM carrier services offered by International Telcos. The ASX-E3 port is a physical DTE (Data Termination Equipment) device that connects to a physical DCE (Data Communication Equipment) device, such as a DSU (Data Service Unit). The one-port version is called the ASX-DS3-1W; the two-port version is called the ASX-DS3-2W. See *ASX-E3 Technical Specifications* on page 3-59 for more information.

E3 is a designation used by Telcos to indicate the capacity of a digital service. E3 actually multiplexes two smaller types of digital service lines (E1 and E2) to reach its channel capacity. E1 is a carrier designation for a digital service with a data rate of 2.048 Mbps. E2 is a carrier designation for a digital services with a data rate of 8.448 Mbps. E3, which interleaves four E2 channels, has a data rate of 34.368.

By default the ASX-E3 uses HDB3 line encoding. Three different mapping protocols are used to transmit ATM cells over an E3 line: Physical Layer Convergence Protocol (PLCP) and two ATM Direct Mapped (ADM) Systems. The PLCP is G.751, and the ADM protocols are G.751 and G.832. The three protocols are not compatible. Many existing E3 implementations use PLCP as defined in ANSI T1.624-1993, but many new implementations of Digital Signaling use ADM. The ASX-E3 module supports all three physical layer protocols. To configure E3 parameters, use the **dsmod** command.

The ASX-E3 is actually a sub-module, or daughtercard, that attaches to an Omni Switch/Router High-Speed Module (HSX). You plug your cable directly into the ASX-E3 sub-module, but it is the HSX module that connects to the switch backplane

With the optional HRE-X you can increase routing performance to 1.5 million packets per second.

ASX-E3 Technical Specifications	
Number of ports	1 or 2
Connector Type	BNC
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/V2.0 ANSI T1.624-1993 (PLCP Mapping) MPOA Client
Data Rate	34.368 Mbps
ATM Adaption Layers	AAL5
MAC Addresses Supported	4096
Max. No. of VCs Supported	1,024
Connections Supported	E3 connections to ATM carrier service.
Cable Supported	Coaxial RG-59 (75 ohm)
Cable Distance	185 m
Current Draw	ASX-E3-1W: 5.75 amps without an HRE-X ASX-E3-1W: 7.25 amps with an HRE-X ASX-E3-2W: 7.25 amps without an HRE-x ASX-E3-2W: 8.75 amps with an HRE-X

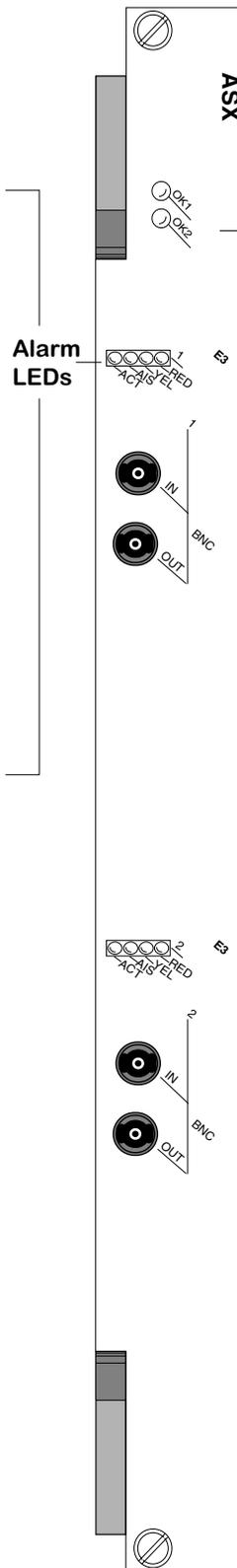
RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the ASX module is plugged in, but no cable has been connected.

YEL (Yellow Alarm). On Amber when a far end receive failure occurs. The recipient of cells from this ASX is not receiving those cells. This error may be due to a transmission error by the ASX or a receive error on the other end of the link.

AIS (Alarm Indication Signal). On when a maintenance signal is sent to the ASX by the network. If this LED is on, then there has been a change in the Alarm Indication Signal (AIS).

ACT (Activity). On Green when the port is transmitting or receiving cells.

Module LEDs Please refer to *2-Port 155 Mbps ATM Uplink Switching Module* on page 3-44 for further information on these LEDs.



ATM E3 Uplink Module

WAN Modules

The Omni Switch/Router currently supports the following Wide Area Network (WAN) modules:

- WSX-S-2W Provides two serial ports that support Frame Relay or PPP.
- WSX-SC Provides four or eight serial ports that support Frame Relay or PPP with data compression.
- WSX-FT1/E1-SC Provides one or two T1/E1 ports and one or two serial ports that support Frame Relay or PPP with data compression.
- WSX-BRI-SC Provides one or two Universal Serial Ports (USPs) ports and one or two ISDN-BRI ports that support Frame Relay or PPP with data compression.
- WSX-M013 Provides 2 or 4 channelized DS3 ports (described in Chapter 56, “Managing Channelized DS3 Modules.”)

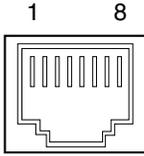
Except for the WSX-M013, all of these modules are described and illustrated in the sections beginning on page 3-66.

A WSX switching module is actually a submodule, or daughtercard, that attaches to an Omni Switch/Router High-Speed Module (HSX). The HSX contains RISC processors, RAM for holding software image files, ASICs for performing switching, and Content Addressable Memory (CAM) for storing MAC addresses. You plug your cable into the WSX submodule, but it is the HSX module that connects to the switch’s backplane.

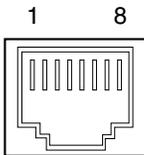
WAN Pinouts

The figures and tables on the following pages illustrate the pinouts used on Omni Switch/Router WAN modules. Please note that the signal commonly known as “remote loop-back” (LL) is not supported on the WAN serial port (see *WAN Serial Port Specifications* on page 3-64). In addition, CTP2, CTP1, and CTP0 are assigned to CS(B), DR(B), and CD(B), respectively, on the serial port. The latter are not used in the cable configurations that require the former.

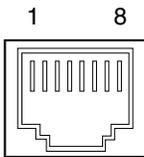
See Appendix B, “Custom Cables,” for information on cables used to connect the serial connector to different interface types.



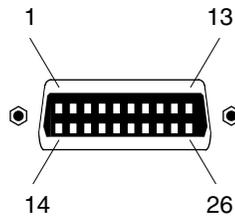
WAN BRI Port Specifications (S/T Interface)	
Pin Number	Standard Signal Name
1	Not Used
2	Not Used
3	Rcv + from TE
4,	Rcv - from TE
5	Xmt + from TE
6	Xmt - from TE
7	Not Used
8	Not Used



WAN BRI Port Specifications (U Interface)	
Pin Number	Standard Signal Name
1	Not Used
2	Not Used
3	Xmt to /Rcv from Network
4,	Xmt to /Rcv from Network
5	Not Used
6	Not Used
7	Not Used
8	Not Used



WAN T1/E1 Port Specifications	
Pin Number	Standard Signal Name
1	Rx_Ring
2	Rx_Tip
3	Chassis GND
4,	Tx_Ring
5	Tx_Tip
6	Chassis GND
7	Chassis GND (A jumper is provided for connecting Pins 7 and 8 to the chassis ground, if required.)
8	Chassis GND (A jumper is provided for connecting Pins 7 and 8 to the chassis ground, if required.)



WAN Serial Port Numbering

WAN Serial Port Specifications							
Generic Signal Name	Source	Alcatel SPI		EIA-530		RS-449	
		Mnemonic	Pin	Mnemonic	Pin	Mnemonic	Pin
Shield	--	Shield	1	--	1	--	1
Signal Ground	--	AB	7	AB	7	SG	19
Transmitted Data	DTE	TD(A)	2	BA(A)	2	SD(A)	4
		TD(B)	14	BA(B)	14	SD(B)	22
Received Data	DCE	RD(A)	3	BB(A)	3	RD(A)	6
		RD(B)	16	BB(B)	16	RD(B)	24
Transmit Clock	DCE	TC(A)	15	DB(A)	15	ST(A)	5
		TC(B)	12	DB(B)	12	ST(B)	23
Receive Clock	DCE	TC(A)	17	DD(A)	17	RT(A)	8
		TC(B)	9	DD(B)	9	RT(B)	26
Ext. Transmit Clock	DTE	XC(A)	24	DA(A)	24	TT(A)	17
		XC(B)	11	DA(B)	11	TT(B)	35
Request To Send	DTE	RS(A)	4	CA(A)	4	RS(A)	7
		RS(B)	19	CA(B)	19	RS(B)	25
Clear To Send	DCE	CS(A)	5	CB(A)	5	CS(A)	9
		CS(B)	13	CB(B)	13	CS(B)	27
Data Set Ready	DCE	DR(A)	6	CC(A)	6	DM(A)	11
		DR(B)	22	CC(B)	22	DM(B)	29
Data Terminal Ready	DTE	TR(A)	20	CD(A)	20	TR(A)	12
		TR(B)	23	CD(B)	23	TR(B)	30
Data Carrier Detect	DCE	CD(A)	8	CF(A)	8	RR(A)	13
		CD(B)	10	CF(B)	10	RR(B)	31
Local Loopback	DTE	LL	18	LL	18	LL	10
Remote Loopback	DTE	RL	21	RL	21	RL	14
Ring Indicator	DCE	RI/TM	25	--	--	--	--
Test Mode	DCE	RI/TM	25	TM	25	TM	18
Cable Type 4	--	CTP4	18		n/c		n/c
Cable Type 3	--	CTP3	26		n/c		n/c
Cable Type 2	--	CTP2	13				
Cable Type 1	--	CTP1	22				
Cable Type 0	--	CTP0	10				

continued on next page...

WAN Serial Port Specifications (cont.)							
Generic Signal Name	Source	X.21/X.26		V.35		RS232	
		Mnemonic	Pin	Mnemonic	Pin	Mnemonic	Pin
Shield	--	--	1	--	A	--	1
Signal Ground	--	G	8	102	B	AB	7
Transmitted Data	DTE	T(A)	2	103(A)	P	BA	2
		T(B)	9	103(B)	S		
Received Data	DCE	R(A)	4	104(A)	R	BB	3
		R(B)	11	104(B)	T		
Transmit Clock	DCE	--	--	114(A)	Y	DB	15
				114(B)	AA		
Receive Clock	DCE	S(A)	6	115(A)	V	DD	17
		S(B)	13	115(B)	X		
Ext. Transmit Clock	DTE	B(A)	7	113(A)	U	DA	24
		B(B)	14	113	W		
Request To Send	DTE	C(A)	3	105	C	CA	4
		C(B)	10				
Clear To Send	DCE	--	--	106	D	CB	5
Data Set Ready	DCE	--	--	107	E	CC	6
Data Terminal Ready	DTE	--	--	108	H	CD	20
Data Carrier Detect	DCE	I(A)	5	109	F	CF	8
		I(B)	12				
Local Loopback	DTE	--	--	141	L	LL	18
Remote Loopback	DTE	--	--	140	N	RL	21
Ring Indicator	DCE	--	--	125	J	CE	22
Test Mode	DCE	--	--	142	NN	TM	25
Cable Type 4	--		n/c		n/c		
Cable Type 3	--		n/c		n/c		
Cable Type 2	--						
Cable Type 1	--						
Cable Type 0	--						

WSX-S-2W

The WSX-S-2W supports two (2) serial ports, which can provide access rates from 9.6 Kbps to 2 Mbps. The WSX-S-2W also supports three types of clocking (internal, external, and split). See *WSX-S-2W Technical Specifications* on page 3-66 for more information.

◆ Note ◆

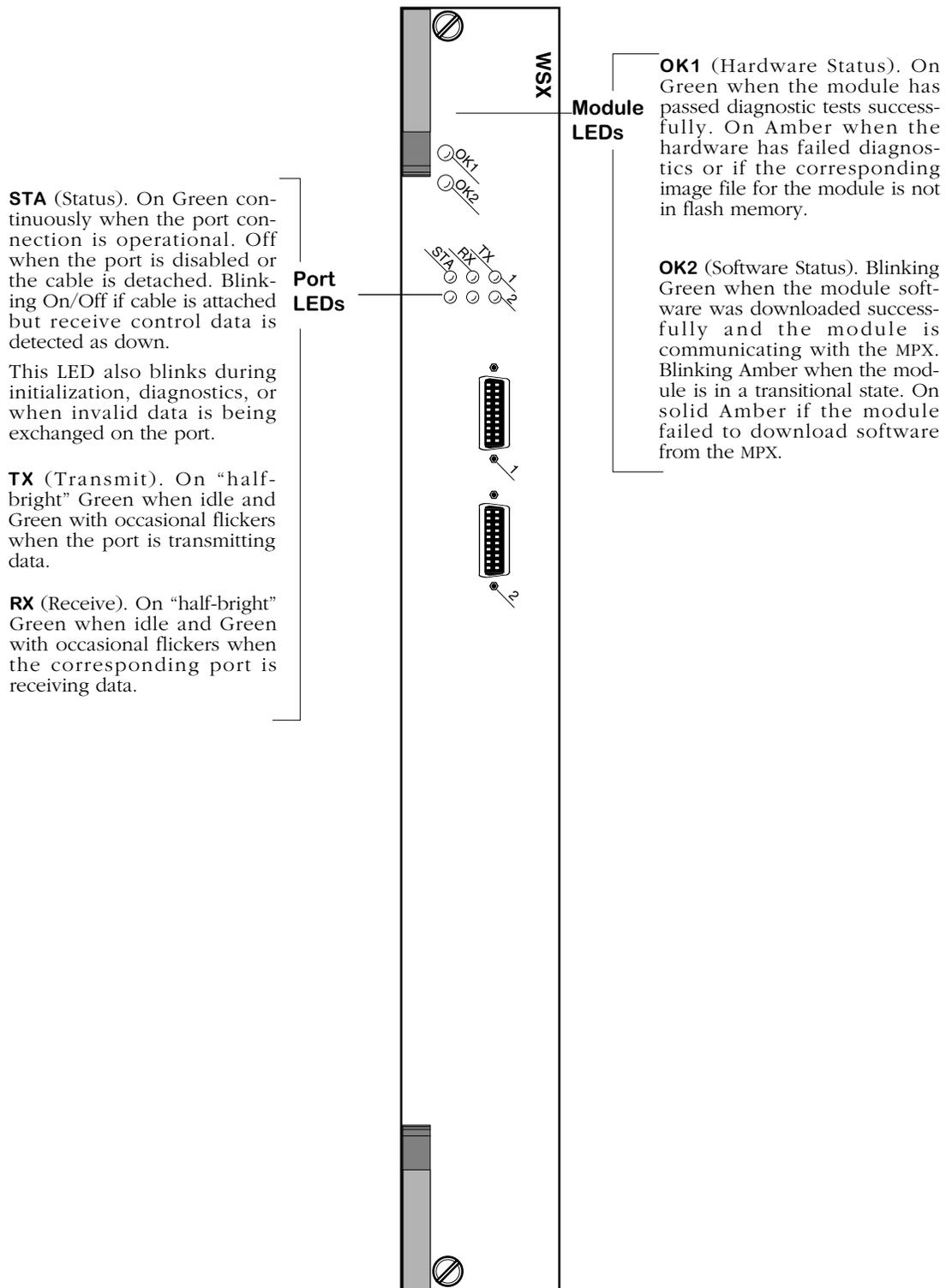
The WSX-S-2W does not support hardware compression.

The WSX-S-2W can sense and auto-configure for any of five serial cable types (RS-232, V.35, X.21, RS-530, and RS-449). A WSX-S-2W port is normally considered a physical DTE device. It can be turned into a physical DCE device—for speed or clocking purposes— by plugging in a DCE cable. The WSX-S-2W senses whether a DCE or DTE cable is connected.

Software in the switch allows you to configure parameters for the Frame Relay or Point-to-Point Protocol (PPP). Software commands allow you to view the status of the WAN connection at the WSX-S-2W board, port, or virtual circuit level. Extensive statistics are provided at each level. Software commands for Frame Relay are described in Chapter 49, “Managing Frame Relay”; commands for PPP are described in Chapter 50, “Point to Point Protocol.”

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

WSX-S-2W Technical Specifications	
Number of ports	2
Connector Type	High-density 26-pin shielded serial
Protocols Supported	Frame Relay and Point-to-Point (PPP)
Data Rates Supported	9.6, 19.2, 56, 64, 128, 256, 512, 768, 1024, 1536, 2048 Kbps
Clocking	Internal, External, or Split
Virtual Circuits Supported	Permanent Virtual Circuits (PVCs)
MAC Addresses Supported	4,096
Connections Supported	Physical Data Terminal Equipment (DTE) or Data Communication Equipment (DCE)
Cable Supported	DTE or DCE in the following types: R2-232, V.35, X.21, RS-530, RS-449
Power Consumption	5.25 amps (without an HRE-X) 6.75 amps (with an HRE-X)



2-Port WAN Frame Relay Switching Module

WSX-SC

The WSX-SC supports 4 or 8 serial ports, each of which can provide access rates from 9.6 Kbps to 2 Mbps. The 4-port version is referred to as the WSX-SC-4W, and the 8-port version is referred to as the WSX-SC-8W. The WSX-SC supports STAC hardware compression and three types of clocking (internal, external, and split). See *WSX-SC Technical Specifications* on page 3-69 for more information.

The WSX-SC can sense and auto-configure for any of five serial cable types (RS-232, V.35, X.21, RS-530, and RS-449). A WSX-SC port is normally considered a physical DTE device. It can be turned into a physical DCE device—for speed or clocking purposes—by plugging in a DCE cable. The WSX-SC board senses whether a DCE or DTE cable is connected.

Software in the switch allows you to configure parameters for the Frame Relay or Point-to-Point Protocol (PPP). Software commands allow you to view the status of the WAN connection at the WSX-SC board, port, or virtual circuit level. Extensive statistics are provided at each level. Software commands for Frame Relay are described in Chapter 49, “Managing Frame Relay”; commands for PPP are described in Chapter 50, “Point to Point Protocol.”

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

WSX-SC Technical Specifications	
Number of ports	4 or 8
Connector Type	High-density 26-pin shielded serial
Protocols Supported	Frame Relay and Point-to-Point (PPP)
Data Rates Supported	9.6, 19.2, 56, 64, 128, 256, 512, 768, 1024, 1536, 2048 Kbps
Compression	Hardware-based using STAC 9705
Clocking	Internal, External, or Split
Virtual Circuits Supported	Permanent Virtual Circuits (PVCs)
MAC Addresses Supported	4,096
Connections Supported	Physical Data Terminal Equipment (DTE) or Data Communication Equipment (DCE)
Cable Supported	DTE or DCE in the following types: R2-232, V.35, X.21, RS-530, RS-449
Power Consumption	WSX-SC-4W without an HRE-X: 6.25 amps WSX-SC-4W with an HRE-X: 7.75 amps WSX-SC-8W without an HRE-X: 8.25 amps WSX-SC-8W with an HRE-X: 9.75 amps

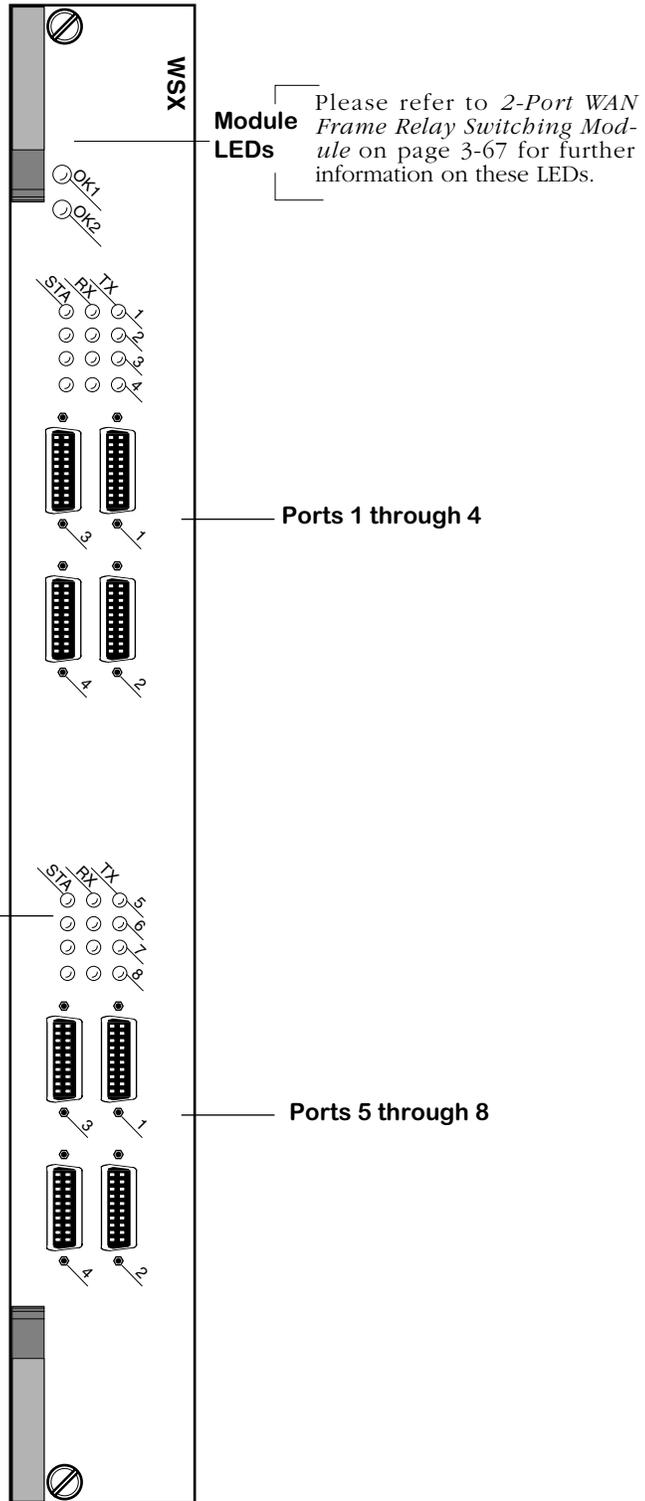
The module includes one row of LEDs for each port. The LEDs for a given port are located in the row labeled with the port number. If the WSX module includes a total of eight ports, then the module contains two sets of four rows of LEDs. The second set of LEDs are located above the second set of ports.

STA (Status). On Green continuously when the port connection is operational. Off when the port is disabled or the cable is detached. Blinking On/Off if cable is attached but receive control data is detected as down.

This LED also blinks during initialization, diagnostics, or when invalid data is being exchanged on the port.

TX (Transmit). On “half-bright” Green when idle and Green with occasional flickers when the port is transmitting data.

RX (Receive). On “half-bright” Green when idle and Green with occasional flickers when the corresponding port is receiving data.



8-Port WAN Frame Relay Switching Module

WSX-FT1/E1-SC

The WSX-FT1/E1-SC module contains one or two T1 or E1 ports and one or two serial ports. T1 and E1 ports use RJ-48C connectors. The T1 version of this module is referred to as the WSX-FT1-SC; the E1 version is referred to as the WSX-FE1-SC. You can configure these ports to run either Frame Relay or the Point-to-Point Protocol (PPP). See *WSX-FT1/E1-SC Technical Specifications* on page 3-72 for more information.

This module includes an integrated CSU/DSU to enable direct connection to a T1/E1 device, such as a PBX, or a T1/E1 line to a service provider.

You can configure physical port parameters through software commands. Configuration options include frame format, facility datalink, and line coding. In addition, the switch can store up to 24 hours of local and remote statistics. See Chapter 53, “Managing T1 and E1 Ports,” for more information on software-configurable parameters.

The WSX-FT1/E1-SC also supports STAC hardware compression.

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

WSX-FT1/E1-SC Technical Specifications	
Number of ports	1 or 2 T1 or E1 ports 1 or 2 Universal Serial ports
Connector Types	T1/E1: RJ-48C Serial: High-density, 26-pin shielded
Standards Supported	RFCs 1406, 1213, 1659
Frame Formats	T1: Superframe, Extended Superframe, Unframed E1: E1, E1-CRC, E1-MF, E1-CRC-MF, Unframed
Line Coding	T1: B8ZS or AMI E1: HDB3 or AMI
Data Rates Supported	T1: 1.544 Mbps E1: 2.048 Mbps Serial: 56, 64, 128, 256, 384, 512, 768, 1024, 1536, 1544, 2048 Kbps
Compression	Hardware-based using STAC 9705
Facility Datalink Protocol	ANSI T1.403 and AT&T 54016
MAC Addresses Supported	4,096
Connections Supported	Physical Data Terminal Equipment (DTE) or Data Communication Equipment (DCE)
Cable Supported	Serial Ports DTE or DCE of the following types: R2-232, V.35, X.21, RS-530, RS-449
Cable Distance	T1/E1 (short haul): 200 meters T1/E1 (long haul): 1829 meters
Power Consumption	WSX-FT1/E1-SC-1W without an HRE-X: 5.75 amps WSX-FT1/E1-SC-1W with an HRE-X: 7.25 amps WSX-FT1/E1-SC-2W without an HRE-X: 7.25 amps WSX-FT1/E1-SC-2W with an HRE-X: 8.75 amps

This module includes one set of LEDs for each port. The LEDs for a given port are located above the port. If the WSX module includes four ports, then the module contains two sets of LEDs. The second set of LEDs are located above the third and fourth ports.

STA (Status). On Green continuously when the port connection is operational. Off when the port is disabled or the cable is detached. Blinking On/Off if cable is attached but receive control data is detected as down.

This LED also blinks during initialization, diagnostics, or when invalid data is being exchanged on the port.

TX (Transmit). On “half-bright” Green when idle and Green with occasional flickers when the port is transmitting data.

RX (Receive). On “half-bright” Green when idle and Green with occasional flickers when the corresponding port is receiving data.

Port 3: T1 or E1

Port 4: Serial



Module LEDs Please refer to *2-Port WAN Frame Relay Switching Module* on page 3-67 for further information on these LEDs.

Port 1: T1 or E1

Port 2: Serial

T1/E1 Port LEDs

ALM (Alarm). On Green when the port is enabled and a signal is present. On Yellow when an error has occurred on the port.

ACT (Activity). On Green when the T1 or E1 port is transmitting or receiving data.

STA (Status). On Green continuously when the port connection is operational. Off when the port is disabled or the cable is detached.

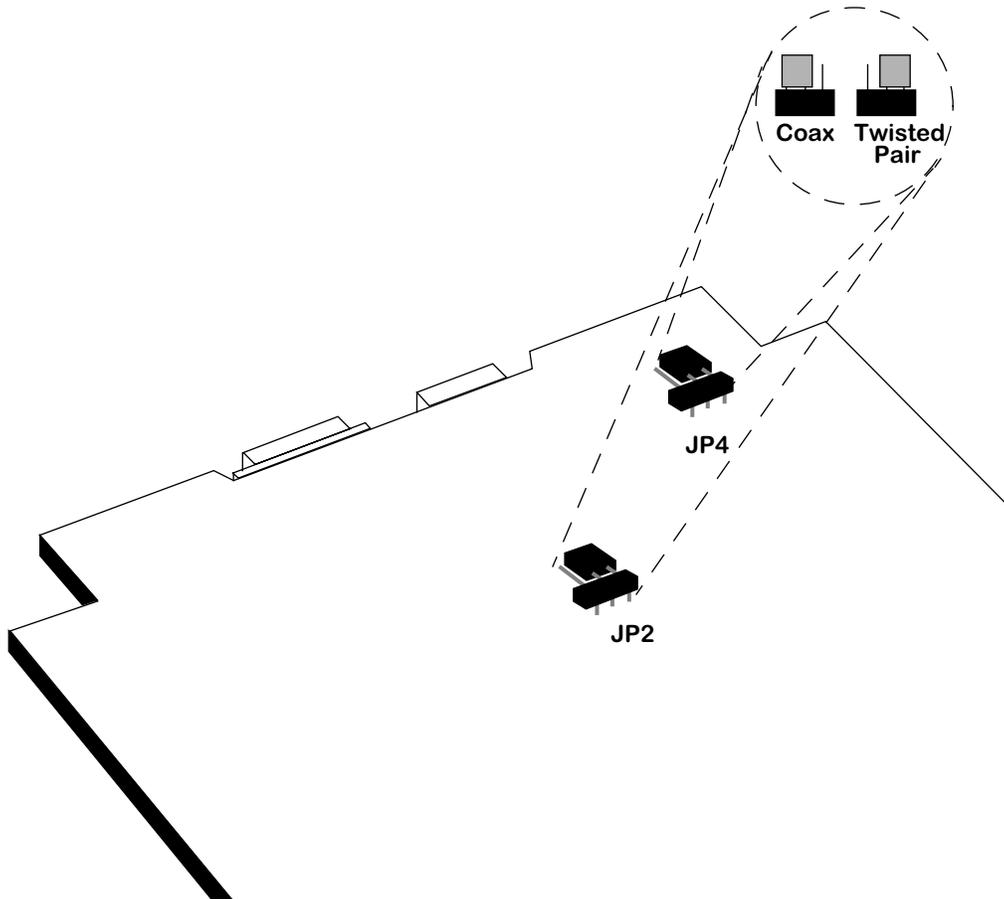
WAN 2-Port Serial and 2-Port Fractional T1/E1 Switching Module

WSX-FE1-SC Cabling/Jumper Settings

The WSX-FE1-SC supports both twisted pair (120 Ohm) and coaxial (75 Ohm) cable types. The default is 120 Ohm. You must set a pair of jumpers (JP2 and JP4) on the back of the board to correspond to the type of cable you are using. For more detailed information on the types of cables to use with this module, see Appendix B, "Custom Cables." The illustration below shows the correct jumper positions.

◆ **Note** ◆

JP3 is reserved. Do not set a jumper across JP3.



Cable Termination Jumpers for WSX-FE1-SC

WSX-BRI-SC

The ISDN Basic Rate Interface WAN Switching Module (WSX-BRI-SC) supports either one (1) serial port and one (1) BRI port or two (2) serial ports and two (2) BRI ports. The version with 1 serial port and 1 BRI port is referred to as the WSX-BRI-SC-1W; the version with 2 serial ports and 2 BRI ports is referred to as the WSX-BRI-SC-2W. See *WSX-BRI-SC Technical Specifications* on page 3-76 for more information.

The serial port on a WSX-BRI-SC module is essentially the same as the serial ports found on the WSX-SC module. A WSX-BRI-SC serial port can detect, and configure itself, for any of five serial cable types (RS-232, V.35, X.21, RS-530, and RS-449). A WSX-BRI-SC serial port is normally considered a physical DTE device, but it can be turned into a physical DCE device—for speed or clocking purposes—by simply plugging in a DCE cable. The WSX-BRI-SC internally senses whether a DCE or DTE cable is connected and configures itself appropriately.

The BRI port on the WSX-BRI-SC board can be configured as either a “U” or an “S/T” type of interface (the board is shipped set to “U”). Either type of interface supports two “B” channels operating at 56/64 Kbps and one “D” channel operating at 16 Kbps.

Software running in the switch allows you to configure the operation of the Point-to-Point Protocol (PPP) over the serial port or the BRI port. The serial port can also support the Frame Relay protocol. The software commands used to configure PPP are described in Chapter 50, “Point-to-Point Protocol.” The software commands used to configure Frame Relay are described in Chapter 49, “Managing Frame Relay.” The software commands used to configure the WAN “links” that support PPP connections are described in Chapter 51, “WAN Links.” Finally, the software commands used to manage the ISDN ports are described in Chapter 52, “Managing ISDN Ports.”

With the optional HRE-X you can increase routing performance to 1.5 million packets per second per module and up to 12 Mpps in a fully-loaded 9-slot chassis.

WSX-BRI-SC Technical Specifications	
Number of ports	1 or 2 pairs of a serial port and an ISDN Basic Rate Interface (BRI) port
Serial Connector Type	High-density 26-pin shielded serial
BRI Connector Type	RJ-45
Protocols Supported	Point-to-Point Protocol (PPP); Frame Relay (supported on the serial port only)
Data Rates Supported	2 "B" Channels at 56/64 Kbps 1 "D" Channel at 16 Kbps
Compression	Hardware-based using STAC 9705
MAC Addresses Supported	4,096
Serial Port Connections Supported	Physical Data Terminal Equipment (DTE) or Data Communication Equipment (DCE)
Serial Cables Supported	DTE or DCE in the following types: R2-232, V.35, X.21, RS-530, RS-449
BRI Port Connections Supported	"U" interface or "S/T" interface (jumper-selectable; "U" is shipping default)
Maximum Cable Distance	BRI: 100 m
Switch Types Supported	National ISDN-1, AT&T 5ESS, Northern Telecom DMS100, ETSI Euro-ISDN Net3
ISDN Standards Supported	Q.921, Q.931, I.430, T1.601
Power Consumption	WSX-BRI-SC-1W without an HRE-X: 4.75 amps WSX-BRI-SC-1W with an HRE-X: 6.25 amps WSX-BRI-SC-2W without an HRE-X: 5.25 amps WSX-BRI-SC-2W with an HRE-X: 6.75 amps

The WSX-BRI module includes one set of LEDs for each port. The LEDs for a given port are located in the set labeled with the port number. If the HSX module contains two WSX-BRI daughter cards, the second set of ports (one Serial and one BRI) are numbered as Ports 3 and 4 respectively, and include their own separate set of LEDs that function exactly like those related to Ports 1 and 2.

STA (Status). On Green continuously when the port connection is operational. Off when the port is disabled or the cable is detached. Blinking On/Off if cable is attached but receive control data is detected as down.

This LED also blinks during initialization, diagnostics, or when invalid data is being exchanged on the port.

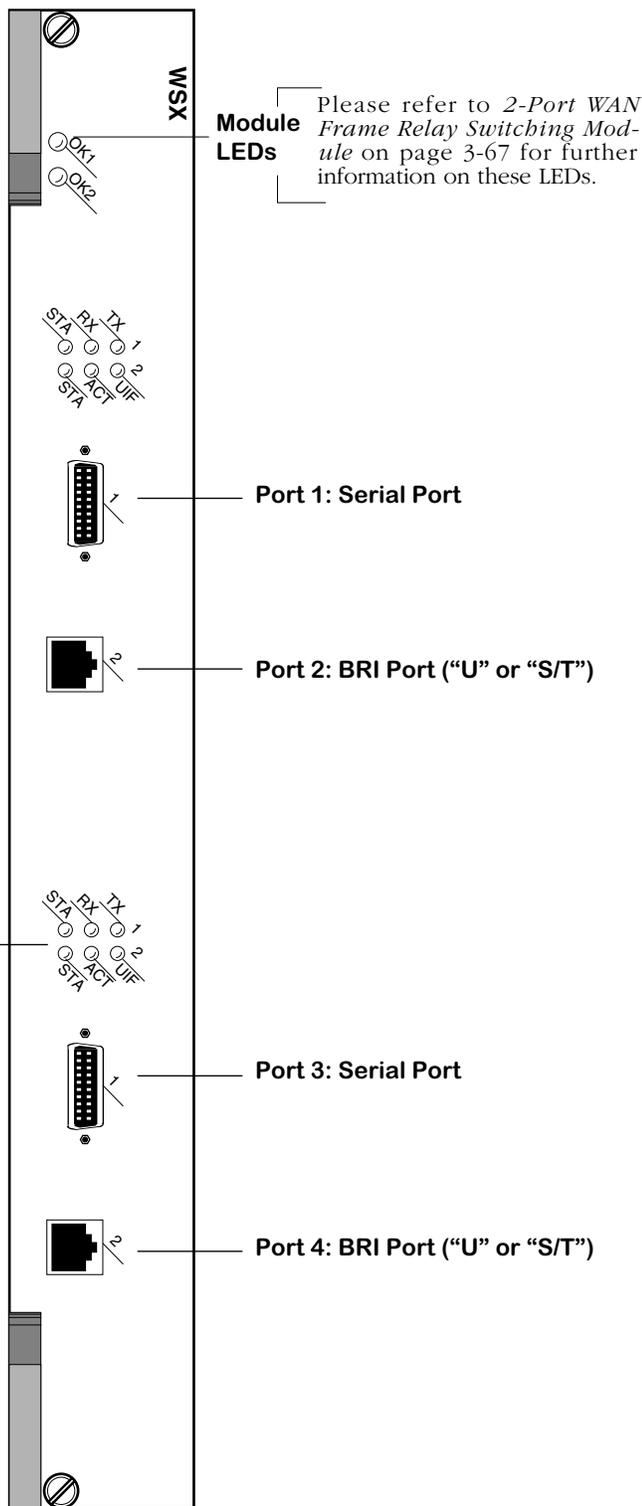
TX (Transmit). On “half-bright” Green when idle and Green with occasional flickers when the port is transmitting data.

RX (Receive). On “half-bright” Green when idle and Green with occasional flickers when the corresponding port is receiving data.

ACT (Activity). On Green when the ISDN-BRI port is sending or receiving data.

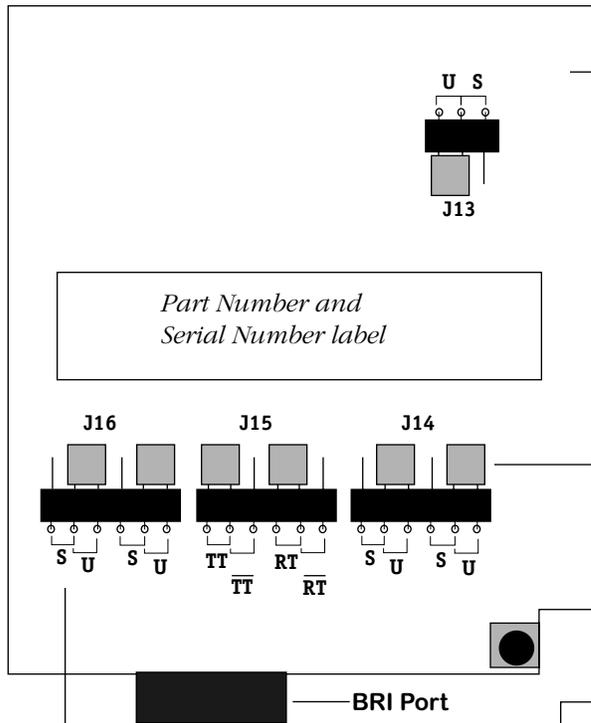
UIF (“U” Interface). On Green when the ISDN-BRI port is configured as a “U” type of interface. Off when the port is configured as an “S/T” type of interface.

STA (Port 2/4 Status). On Green continuously when the port connection is operational. Off when the BRI port is disabled or the cable is detached. This LED blinks during initialization.



WAN 2-Port Serial and 2-Port BRI-ISDN Switching Module

**Jumper Configuration for the "U" Interface
(this is how the board is shipped)**

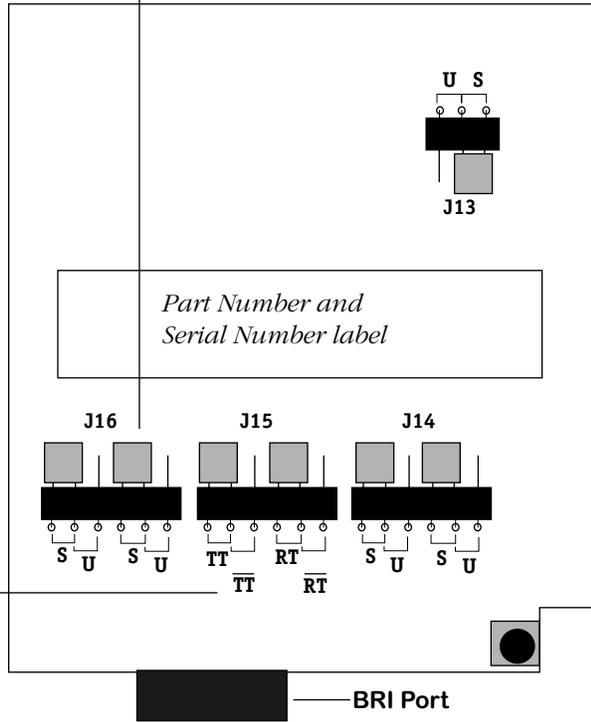


This is a simplified view of the bottom lower-right quadrant of the WSX-BRI submodule. Immediately above the BRI port are three jumper blocks labelled J14, J15, and J16. About two inches above and to the right is another jumper labeled J13. J13, J14, and J16 are used to switch between the "U" and "S/T" interfaces. J15 is used to set transmit and receive termination for the "S/T" interface.

The gray boxes are the jumper blocks

The small labels next to the jumper pins at J13, J14, and J16 indicate which pins must be bridged to set the BRI port to either the "U" or the "S/T" interface.

Small labels under the pins at J15 indicate which pins must be bridged to set Transmit Termination (tt) and Receive Termination (rt) to the "on" or "off" position (the two sets of letters with a line over them indicate the "off" settings).



**Jumper Configuration for the "S/T" Interface
(transmit/receive termination are set to "on")**

4 The OmniSwitch Chassis

The OmniSwitch[®] is an advanced networking product that serves as a platform for a broad range of network interfaces. It supports Ethernet, Fast Ethernet (100 Mbps), Token Ring, ATM, and WAN interfaces on a variety of copper and fiber optic cables. It automatically translates between any of these MAC-layer and media types.

The OmniSwitch includes support for IP and IPX Routing, AutoTracker policy-based Virtual LANs (VLANs), ATM LAN Emulation, Group multiplexing over LANs and WANs, any-to-any switching, port mirroring, RMON, and SNMP trap support.

The OmniSwitch architecture is based on a store-and-forward technology. This technology allows the OmniSwitch to filter out run packets, packets that exceed the maximum length allowed, CRC-flawed packets, misaligned packets, and other packets with errors. The switching process combines hardware-based switching with software-based management, resulting in a design where hardware can quickly perform rote switching tasks while allowing software to individually examine frames.

OmniSwitch Components

The OmniSwitch is composed of the following:

- Chassis and backplane
- Power supplies: one or two.
- Management Processor Modules (MPMs): one or two.
- Switching Modules (two to eight) that support the various network interface types.

The OmniSwitch chassis, and backplane are described in this chapter. The MPM Module provides some of the core routing, VLAN MAC learning, SNMP, and file management functions for the entire OmniSwitch. Only one MPM is required per OmniSwitch, but you can add another for redundancy. The MPM is described in detail in Chapter 6, “The Management Processor Module (MPM).” OmniSwitch power supplies are described in Chapter 5, “OmniSwitch Power Supplies.”

The OmniSwitch deploys a distributed architecture in which many of the processing functions are handled by individual Switching Modules. Each Switching Module adds additional memory and processing power to the entire OmniSwitch. Switching modules perform software filtering, translations between dissimilar network interfaces, and hardware-based switching. Each Switching Module supports multiple MAC addresses per port such that both individual devices and networks can be connected to a single switch port. All Switching Modules are described in detail in Chapter 7, “OmniSwitch Switching Modules.”

OmniSwitch Frame and Management Buses

The OmniSwitch frame bus operates at 640 or 960 Mbps depending on the MPM used and the switching modules' revision levels. The MPM-1G and MPM-III supports a frame bus capacity of 960 Mbps while the original MPM and the MPM-II support 640 Mbps. The Frame Bus supports high-performance switching while maintaining separation between up to 96 Groups, or broadcast domains, in any one switch or up to 65K Groups in an entire network. Switching traffic on and off the frame bus is hardware-controlled; an entire block of data is shifted on each transfer. Pipelining keeps data moving through the OmniSwitch with very low latency. Management of switching modules is provided via a separate management bus which operates at 120 Mbps.

ATM Cell Switching Matrix

An enhanced version of the OmniSwitch backplane provides an ATM cell matrix in addition to the frame and management bus. This ATM cell matrix operates at up to 13.2 Gbps. The ATM cell switching fabric is fully distributed with no central switch component and therefore no single point of failure. The cell switching functionality operates in the Omni-3wx, Omni-5x, Omni-5wx, Omni-9x, and Omni-9wx chassis types. OmniSwitch cell switching is described in more detail in Chapter 40, “Cell Switching Modules (CSMs).”

OmniSwitch Chassis Types

There are eleven (11) different versions of the OmniSwitch chassis—one chassis type has three module slots, four chassis types have five module slots, and six chassis have nine module slots. The table on the following page summarizes the features of each of the eleven chassis types. Each chassis type is described in more detail on the pages that follow.

◆ Note ◆

In the current release, a maximum of seven (7) 32-port switching modules (e.g., ESM-100C-32W) is supported in 9-slot OmniSwitch chassis.

Chassis Name	Module Slots	MPMs Supported	Cell Switching Supported?	Power Supply Type
Omni-3wx	3 wide	MPM-1GW, MPM-C, MPM-III	Yes	Built-in (150W) Can Use BPS (250W)
Omni-5wx	5 wide	MPM-1GW, MPM-C, MPM-III	Yes	PS5-250 (250W) PS5-DC250 (-48VDC,250W)
Omni-9wx	9 wide	MPM-1GW, MPM-C, MPM-III	Yes	PS9-500 (500W) PS9-DC500 (-48VDC,500W)
Omni-9wx-PLUS	9 wide	MPM-1GW, MPM-C, MPM-III	Yes	PS9-650 (650W)
Omni-9wxp	9 wide	MPM-1GW, MPM-C, MPM-III	Yes	PS9-725 (750W)
Omni-5	5	MPM, MPM-II, MPM-1G	No	PS5 (150W) PS5-DC48 (-48VDC,150W)
Omni-9	9	MPM, MPM-II, MPM-1G	No	PS9 (350W)
Omni-5e	5	MPM, MPM-II, MPM-1G	No	PS5-250 (250W) PS5-DC250 (-48VDC,250W)
Omni-9e	9	MPM, MPM-II MPM-1G	No	PS9-500 (500W) PS9-350 (350W) PS9-DC500 (-48VDC,500W)
Omni-5x	5	MPM-II, MPM-1G	Yes	PS5-250 (250W) PS5-DC250 (-48VDC,250W)
Omni-9x	9	MPM-II, MPM-1G	Yes	PS9-500 (500W) PS9-DC500 (-48VDC,500W)

OmniSwitch Failure-Resistant Features

The OmniSwitch has several features that provide redundancy and reliability. The switch backplane actually contains no active components. Every module contains its own processors and redundancy can be added to all critical components.

- Redundant Management Processor Module (MPM). When two MPMs are installed, one serves as the primary MPM and the other serves as the secondary. In the event of a failure of the primary MPM, the secondary automatically takes over the management role for the OmniSwitch.
- Redundant power supplies. The OmniSwitch's power supplies can support a fully configured unit. See Chapter 5, "OmniSwitch Power Supplies," for more information.
- Hot-replaceable modules. All modules, including redundant MPMs, can be removed and re-inserted while the unit is operational.
- Temperature alarm. Special hardware in the switch detects over-temperature conditions and immediately notifies the network manager.
- Flash memory. All operating software and configuration information are stored in non-volatile flash memory. You can download new software revisions while the OmniSwitch is operational. No mechanical disk drive is used for storage.
- Extensive LED indicators. Each OmniSwitch module contains an extensive array of LED indicators that allow you to get a quick glance at the board's health, port states, port activity, collisions, beacons, and many other status indicators.

Omni-3wx

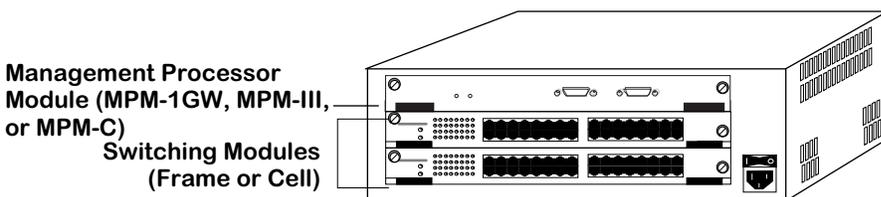
The Omni-3wx chassis supports new high-density wide switching modules in addition to thin versions. It contains three slots for MPM, FCSM, and switching modules. Slots are numbered from 1 to 3 starting with the topmost slot. A built-in power supply is located on the right side of the chassis, and a fan cooling system is located on the left side of the chassis.

The entire chassis can be rack-mounted. You can view all cabling, power supplies, module interfaces, and LEDs at the front of the chassis.

Wide modules are standard for high-density Ethernet and ATM modules. Wide versions of previously thin modules are available for all switching modules. If thin versions of the modules are installed, a spacer panel must be used to fill the extra space between modules.

The MPM-1GW, MPM-C, or MPM-III is used in the Omni-3wx chassis. The MPM-1GW/C/III must be installed in either Slot 1 or 2. If the MPM-1GW/C/III is installed in Slot 2, you can install a switching module in Slot 1. If it is installed in Slot 1, a Switching Module can be installed in Slot 2.

The Omni-3wx backplane supports the ATM cell switching matrix, the 640/960 Mbps frame-switching bus, and the 120 Mbps management bus. The chassis may be configured as a pure LAN switch (only frame switching modules) or as a pure ATM switch (only cell switching modules).



The Omni-3wx

Power Supply

The Omni-3wx uses a built-in AC or DC power supply that has a capacity of 25 Amps at 5 volts and 2 amps at 12 volts for 150 Watts of output power. (The DC version of the Omni-3wx is known as the Omni-3wx-48V.) The Omni-3wx may also be connected to a Backup Power Supply (BPS) to provide power redundancy. A power connector is provided on the back of the Omni-3wx that connects to a BPS. See Chapter 5, "OmniSwitch Power Supplies," for more information on the Omni-3wx power supply and the BPS.

Omni-3wx Technical Specifications	
Total Module Slots	3
Total Slots for Switching Modules	2
Physical Dimensions	5.25" (13.34 cm) high, 17.13" (43.51 cm) wide, 13.00" (33.02 cm) deep
Weight	18 lb. (8.18 kg), fully populated with modules and power supplies.
Switching Backplane	ATM Cell Bus Up to 5.2 Gbps 640 or 960 Mbps Frame Bus (dependent on MPM type) 120 Mbps Control Bus
Temperature Operating Range	0 to 40 degrees Celsius 32 to 104 degrees Fahrenheit
Humidity	
Altitude	Sea level to 10,000 feet (3 km)
Agency Listings	UL 1950 CSA-C22.2 EN60950 FCC Part 15, Subpart B (Class A) EN55022, 1987/EN50081 FCC Class B C.I.S.P.R. 22: 1985 EN50082-1, 1992 IEC 801-2, 1991 IEC 801-3, 1984 IEC 801-4, 1988 VCCI V-3/94.04 (Class 1)

Omni-5wx

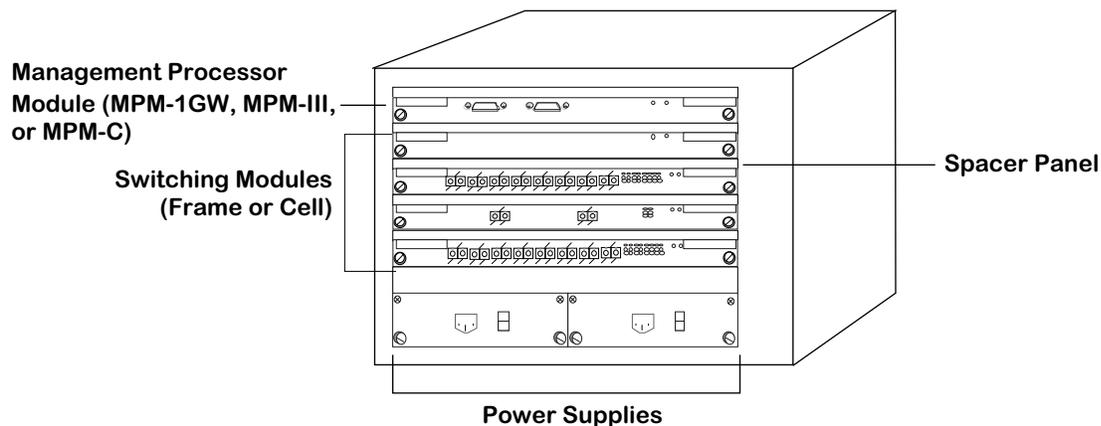
The Omni-5wx chassis supports the new high-density wide switching modules in addition to thin versions of switching modules. It contains five slots for MPM, FCSM, and switching modules. Slots are numbered from 1 to 5 starting with the topmost slot. Slots for two power supplies are located at the bottom of the chassis.

The entire chassis can wall-mounted or rack-mounted. You can view all cabling, power supplies, module interfaces, and LEDs at the front of the chassis.

Wide modules are standard for high-density Ethernet and ATM modules. Wide versions of previously thin modules will be available for all switching modules. If thin versions of the modules are installed, a spacer panel must be used to fill the extra space between modules.

The Omni-5wx uses the MPM-1GW, MPM-C, or MPM-III. The MPM-1GW/C/III must be installed in either Slot 1 or 2. If the MPM-1GW/C/III is installed in Slot 2, you can install a switching module in Slot 1. If it is installed in Slot 1, a Switching Module can be installed in Slot 2. When dual-redundant MPM-1GW/C/IIIs are installed, one of them must be installed in Slot 1 and the other in Slot 2.

The Omni-5wx backplane is functionally the same as the Omni-5x backplane, but it has been modified to fit the larger chassis unit. It supports the ATM cell switching matrix, the 640/960 Mbps frame-switching bus, and the 120 Mbps management bus. The chassis may be configured as a pure LAN switch (only frame switching modules), a pure ATM switch (only cell switching modules), or as a hybrid LAN/ATM switch (mixture of frame and cell switching modules).



The Omni-5wx

Power Supplies

The Omni-5wx provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to the operation. See Chapter 5, "OmniSwitch Power Supplies," for more information on the Omni-5wx power supplies.

Omni-5wx Technical Specifications	
Total Module Slots	5
Total Slots for Switching Modules	4
Physical Dimensions	12.25" (31.12 cm) high, 17.14" (43.54 cm) wide, 13" (33.02 cm) deep
Weight	53 lb. (24.09 kg), fully populated with modules and power supplies.
Switching Backplane	Cell Switching Matrix 640/960 Mbps Frame Bus 120 Mbps Control Bus
Temperature Operating Range	0 to 45 degrees Celsius 32 to 113 degrees Fahrenheit
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Altitude	Sea level to 10,000 feet (3 km)
Agency Listings	UL 1950 CSA-C22.2 EN60950 FCC Part 15, Subpart B (Class A) EN55022, 1987/EN50081 FCC Class B C.I.S.P.R. 22: 1985 EN50082-1, 1992 IEC 801-2, 1991 IEC 801-3, 1984 IEC 801-4, 1988 VCCI V-3/94.04 (Class 1)

Omni-9wx

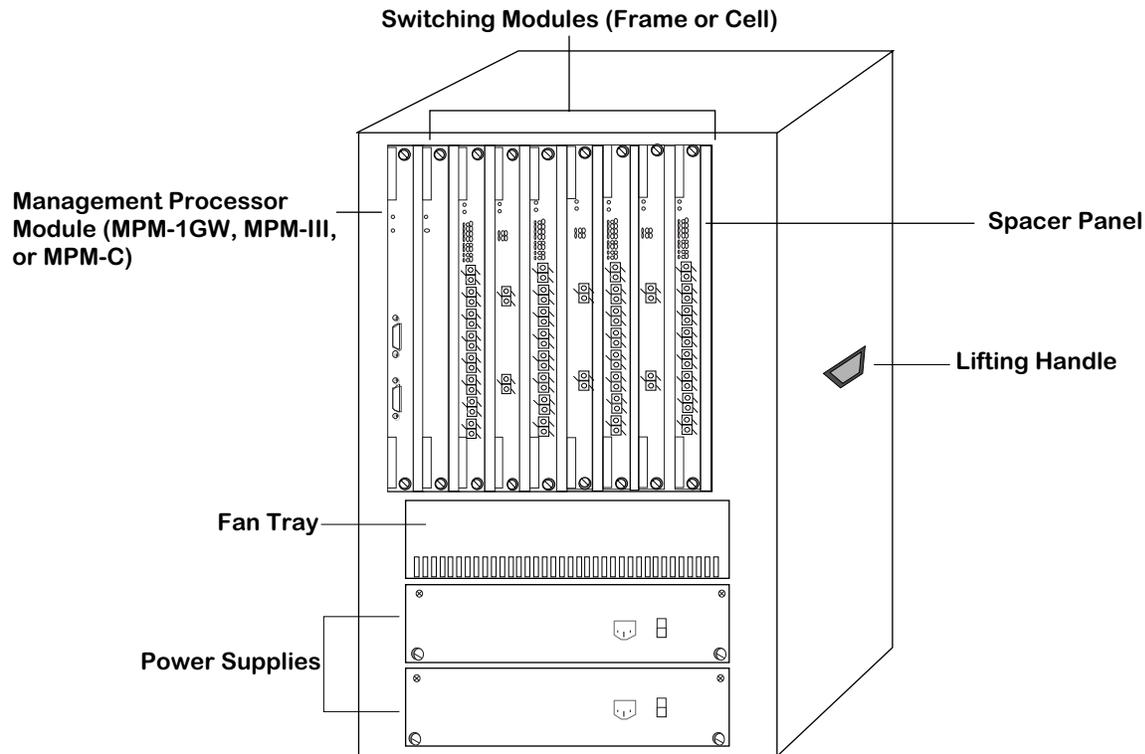
The Omni-9wx chassis supports the new high-density wide switching modules in addition to thin versions of switching modules. It contains nine slots for MPM, FCSM, and switching modules. Slots are numbered from 1 to 9 starting with the leftmost slot. Slots for two power supplies are located at the bottom of the chassis. A separate, removable fan tray containing four fans is located above the power supply module bays.

A fully loaded Omni-9wx weighs nearly 100 lbs. Therefore, it is recommended that if you are rack-mounting the chassis that you use a rack mount shelf instead of just brackets. Using a shelf will ensure that the weight of the chassis can be supported. In addition, the Omni-9wx contains side handles to make lifting and installation easier.

Wide modules are standard for high-density Ethernet and ATM modules. Wide versions of previously thin modules are available for all switching modules. If thin versions of the modules are installed, a spacer panel must be used to fill the extra space between modules.

The Omni-9wx chassis uses the MPM 1GW, MPM-C, or MPM-III. The MPM must be installed in either Slot 1 or 2. If the MPM is installed in Slot 2, you can install a Switching Module in Slot 1. If it is installed in Slot 1, a Switching Module can be installed in Slot 2. When dual-redundant MPMs are installed, one of them must be installed in Slot 1 and the other in Slot 2.

The Omni-9wx backplane is functionally the same as the Omni-9x backplane, but it has been modified to fit the larger chassis unit. It supports the 13.2 Gbps ATM cell switching matrix, the 640/960 Mbps frame-switching bus, and the 120 Mbps management bus. The chassis may be configured as a pure LAN switch (only frame switching modules), a pure ATM switch (only cell switching modules), or as a hybrid LAN/ATM switch (mixture of frame and cell switching modules).



The Omni-9wx

Power Supplies

The Omni-9wx provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to the operation. See Chapter 5, “OmniSwitch Power Supplies,” for more information on the Omni-9wx power supplies.

Two “high current” versions of the Omni-9wx chassis are available. One is called the Omni-9wx-PLUS. This chassis uses the Omni-PS9-650P power supply, which provides 650 Watts of power at 5 Volts. Another is called the Omni-9wxp. This chassis uses the PS9-725 power supply, which provides 750 watts of power at 5 Volts.

Omni-9wx, Omni-9wx-PLUS, and Omni-9wxp Technical Specifications	
Total Module Slots	9
Total Slots for Switching Modules	8
Physical Dimensions	24.50”(62.23 cm) high, 16.60” (42.16 cm) wide, 13.25” (36.66 cm) deep
Weight	96 lb. (43.55 kg), fully populated with modules and power supplies.
Switching Backplane	13.2 Gbps Cell Bus 640/960 Mbps Frame Bus 120 Mbps Control Bus.
Temperature Operating Range	0 to 45 degrees Celsius 32 to 113 degrees Fahrenheit
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Altitude	Sea level to 10,000 feet (3 km)
Agency Listings	UL 1950; CSA-C22.2; EN60950; EN55022, 1987/EN50081; C.I.S.P.R. 22: 1985; EN50082-1, 1992; IEC 801-2, 1991; IEC 801-3, 1984; IEC 801-4, 1988; VCCI V-3/94.04 (Class 1); FCC Part 15, Subpart B (Class A); FCC Class B

Discontinued Chassis

The chassis described in the following sections, while still supported, are no longer manufactured by Alcatel. These chassis have been replaced by the newer versions, which are described in the preceding sections.

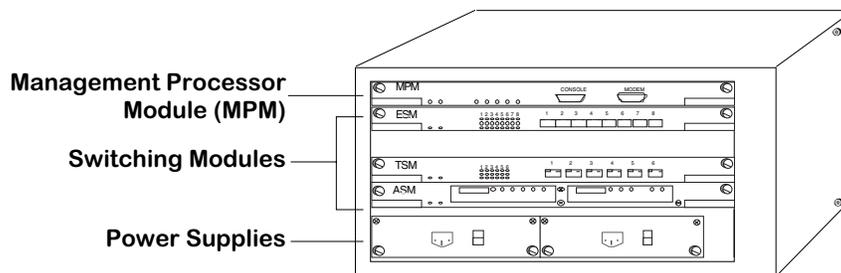
Omni-5

The Omni-5 contains five slots for MPM and Switching Modules. The slots are numbered 1 to 5 starting from the topmost slot. The MPM module must be installed in either Slot 1 or 2. If the MPM is installed in Slot 2, you can install a Switching Module in Slot 1. If it is installed in Slot 1, a Switching Module can be installed in Slot 2. When dual-redundant MPMs are installed, one MPM must be installed in Slot 1 and the other in Slot 2. Slots for two power supplies are located at the bottom of the chassis enclosure.

The enclosure is a front-access chassis which can be wall-mounted or rack-mounted. You can view all cabling, power supplies, module interfaces, indicators, and displays at the front of the enclosure. Cable organizers are available as are blanking panels for unpopulated slots.

◆ Note ◆

The Omni-5 chassis is supported, but it has been discontinued. This chassis has been replaced by an enhanced version called the Omni-5wx. The Omni-5wx is described in *Omni-5wx* on page 4-7.



The Omni-5

Power Supplies

The Omni-5 provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to the operation. See Chapter 5, “OmniSwitch Power Supplies,” for more information on the Omni-5 power supplies.

Omni-5 Technical Specifications	
Total Module Slots	5
Total Slots for Switching Modules	4
Physical Dimensions	8.75" (22.23 cm) high, 17" (43.18 cm) wide, 13" (33.02 cm) deep
Weight	30 lb. (13.64 kg), fully populated with modules and power supplies.
Switching Backplane	640 Mbps Frame Bus; 120 Mbps Control Bus.
Temperature Operating Range	0 to 45 degrees Celsius 32 to 113 degrees Fahrenheit
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Altitude	Sea level to 10,000 feet (3 km)
Agency Listings	UL 1950 CSA-C22.2 EN60950 FCC Part 15, Subpart B–Class A EN55022, 1987/EN50081 C.I.S.P.R. 22: 1985 EN50082-1, 1992 IEC 801-2, 1991 IEC 801-3, 1984 IEC 801-4, 1988 VCCI V-3/94.04–Class 1

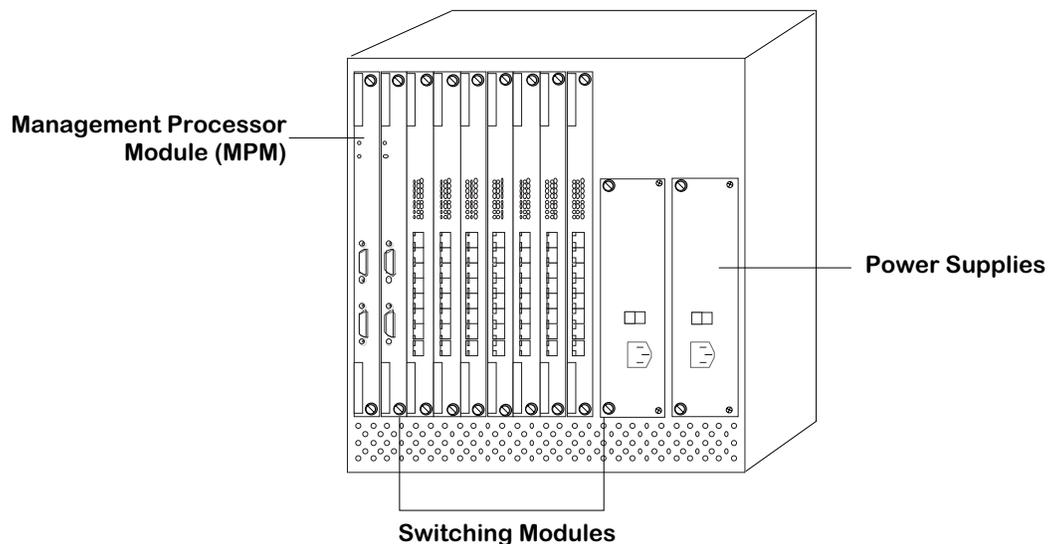
Omni-9

The Omni-9 contains nine slots for MPM and Switching Modules. The slots are numbered 1 to 9 starting from the leftmost slot. The MPM module must be installed in either Slot 1 or 2. If the MPM is installed in Slot 2, you can install a Switching Module in Slot 1. If it is installed in Slot 1, a Switching Module can be installed in Slot 2. When dual-redundant MPMs are installed, one MPM must be installed in Slot 1 and the other in Slot 2. Slots for two power supplies are located on the right side of the chassis enclosure.

The enclosure is a front-access chassis which can be wall-mounted or rack-mounted. You can view all cabling, power supplies, module interfaces, indicators, and displays at the front of the enclosure. Cable organizers are available as are blanking panels for unpopulated slots.

◆ Note ◆

The Omni-9 chassis is supported, but it has been discontinued. This chassis has been replaced by an enhanced version called the Omni-9wx. The Omni-9wx is described in *Omni-9wx* on page 4-9.



The Omni-9

Power Supplies

The Omni-9 provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to the operation. See Chapter 5, “OmniSwitch Power Supplies,” for more information on the Omni-9 power supplies.

Omni-9 Technical Specifications	
Total Module Slots	9
Total Slots for Switching Modules	8
Physical Dimensions	17.0" (43.18 cm) high, 17" (43.18 cm) wide, 15.5" (39.37 cm) deep
Weight	55 lb., fully populated with modules and power supplies.
Switching Backplane	640 Mbps Frame Bus; 120 Mbps Control Bus.
Temperature Operating Range	0 to 45 degrees Celsius 32 to 113 degrees Fahrenheit
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Altitude	Sea level to 10,000 feet (3 km)
Agency Listings	UL 1950 CSA-C22.2 EN60950 FCC Part 15, Subpart B-Class A EN55022, 1987/EN50081 C.I.S.P.R. 22: 1985 EN50082-1, 1992 IEC 801-2, 1991 IEC 801-3, 1984 IEC 801-4, 1988 VCCI V-3/94.04-Class 1

Omni-5e

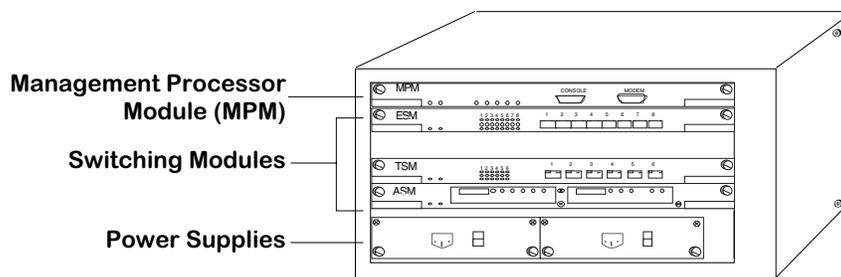
The Omni-5e is an enhanced version of the Omni-5 chassis. The Omni-5e chassis is designed to improve cooling and emissions compliance while continuing to support all existing frame switching modules. The Omni-5e provides the same functionality as the Omni-5 chassis while incorporating a new fan structure for improved cooling and a more powerful (250-watt versus 150-watt) power supply. This improved power supply allows the Omni-5e chassis to support any mix of switching modules with a single power supply.

The Omni-5e contains five slots for MPM and Switching Modules. The slots are numbered 1 to 5 starting from the topmost slot. The MPM module must be installed in either Slot 1 or 2. If the MPM is installed in Slot 2, you can install a Switching Module in Slot 1. If it is installed in Slot 1, a Switching Module can be installed in Slot 2. When dual-redundant MPMs are installed, one MPM must be installed in Slot 1 and the other in Slot 2. Slots for two power supplies are located at the bottom of the chassis enclosure.

The enclosure is a front-access chassis which can be wall-mounted or rack-mounted. You can view all cabling, power supplies, module interfaces, indicators, and displays at the front of the enclosure. Cable organizers are available as are blanking panels for unpopulated slots.

◆ Note ◆

The Omni-5e chassis is supported, but it has been discontinued. This chassis has been replaced by an enhanced version called the Omni-5wx. The Omni-5wx is described in *Omni-5wx* on page 4-7.



The Omni-5e

Power Supplies

The Omni-5e provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to the operation. See Chapter 5, “OmniSwitch Power Supplies,” for more information on the Omni-5e power supplies.

Omni-5e Technical Specifications	
Total Module Slots	5
Total Slots for Switching Modules	4
Physical Dimensions	8.75" (22.23 cm) high, 17" (43.18 cm) wide, 13" (33.02 cm) deep
Weight	30 lb., fully populated with modules and power supplies.
Switching Backplane	640/960 Mbps Frame Bus; 120 Mbps Control Bus.
Temperature Operating Range	0 to 45 degrees Celsius 32 to 113 degrees Fahrenheit
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Altitude	Sea level to 10,000 feet (3 km)
Agency Listings	UL 1950 CSA-C22.2 EN60950 FCC Part 15, Subpart B–Class A EN55022, 1987/EN50081 FCC Class B C.I.S.P.R. 22: 1985 EN50082-1, 1992 IEC 801-2, 1991 IEC 801-3, 1984 IEC 801-4, 1988 VCCI V-3/94.04–Class 1

Omni-9e

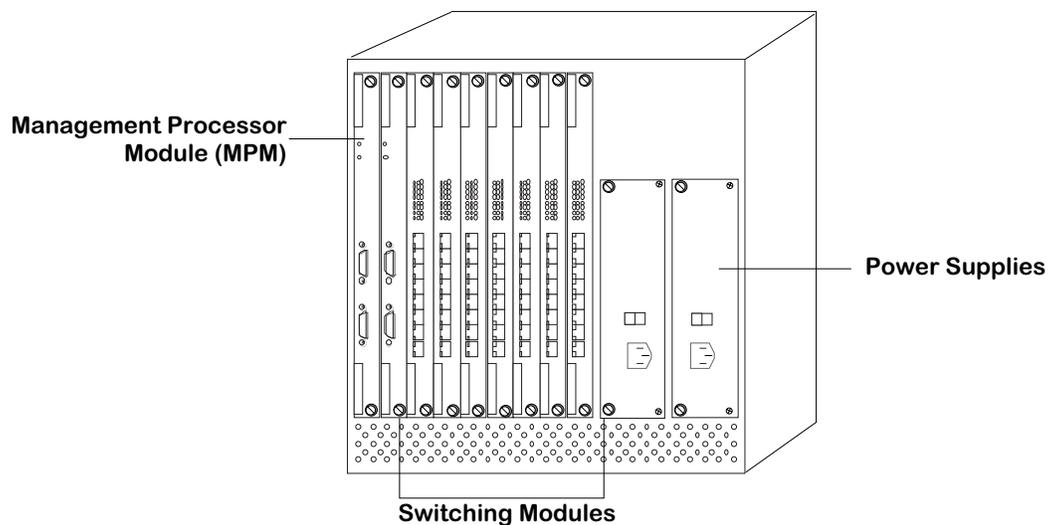
The Omni-9e is an enhanced version of the Omni-9 chassis. The Omni-9e chassis is designed to improve cooling and emissions compliance while continuing to support all existing frame switching modules. The Omni-9e provides the same functionality as the Omni-9 chassis while incorporating a new fan structure for improved cooling and a more powerful power supply. These improvements allow the Omni-9e chassis to support any mix of switching modules with a single power supply.

The Omni-9e contains nine slots for MPM and Switching Modules. The slots are numbered 1 to 9 starting from the leftmost slot. The MPM module must be installed in either Slot 1 or 2. If the MPM is installed in Slot 2, you can install a Switching Module in Slot 1. If it is installed in Slot 1, a Switching Module can be installed in Slot 2. When dual-redundant MPMs are installed, one MPM must be installed in Slot 1 and the other in Slot 2. Slots for two power supplies are located on the right side of the chassis enclosure.

The enclosure is a front-access chassis which can be wall-mounted or rack-mounted. You can view all cabling, power supplies, module interfaces, indicators, and displays at the front of the enclosure. Cable organizers are available as are blanking panels for unpopulated slots.

◆ Note ◆

The Omni-9e chassis is supported, but it has been discontinued. This chassis has been replaced by an enhanced version called the Omni-9wx. The Omni-9wx is described in *Omni-9wx* on page 4-9.



The Omni-9e

Power Supplies

The Omni-9e provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to the operation. See Chapter 5, “OmniSwitch Power Supplies,” for more information on the Omni-9e power supplies.

Omni-9e Technical Specifications	
Total Module Slots	9
Total Slots for Switching Modules	8
Physical Dimensions	17.0" (43.18 cm) high, 17.0" (43.18 cm) wide, 15.5" (39.37 cm) deep
Weight	55 lb. (25 kg), fully populated with modules and power supplies.
Switching Backplane	640/960 Mbps Frame Bus; 120 Mbps Control Bus.
Temperature Operating Range	0 to 45 degrees Celsius 32 to 113 degrees Fahrenheit
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Altitude	Sea level to 10,000 feet (3 km)
Agency Listings	UL 1950 CSA-C22.2 EN60950 FCC Part 15, Subpart B–Class A EN55022, 1987/EN50081 FCC Class B C.I.S.P.R. 22: 1985 EN50082-1, 1992 IEC 801-2, 1991 IEC 801-3, 1984 IEC 801-4, 1988 VCCI V-3/94.04–Class 1

Omni-5x

The Omni-5x is physically the same as an Omni-5e. Module slots and power supplies are located in the same places and the same power supplies are used in both chassis. The primary difference between the two chassis is that the Omni-5x supports the ATM cell switching matrix in addition to the 640/960 Mbps frame-switching bus and the 120 Mbps management bus.

The Omni-5x chassis requires the use of an MPM-II or MPM-1G module.

Frame and cell switching are integrated in the Omni-5x. All existing frame switching modules are supported in the Omni-5x. In fact, pure frame switching applications can be handled without converting frames to cells and back from cells to frames. The chassis may be configured as a pure LAN switch (only frame switching modules), a pure ATM switch (only cell switching modules), or as a hybrid LAN/ATM switch (mix of frame and cell switching modules).

The Omni-5x provides native ATM switching, both for backbone and workstation access. The ATM switching backplane allows the Omni-5x to support Cell Switching Modules (CSMs). CSMs support ATM25, ATM OC-3c/STM-1, and OC-12c/STM-4c interfaces. CSMs are described more thoroughly in Chapter 40, "Cell Switching Modules (CSMs)."

The ATM cell switching fabric is fully distributed with the aggregate 6.8 Gbps distributed across all Cell Switching Modules. There is no central switch component and therefore no single point of failure. In addition, the cell backplane employs an advanced dynamic input buffered/output controlled queuing scheme which provides non-blocking performance and scales buffer requirements as the system grows.

◆ Note ◆

The Omni-5x chassis is supported, but it has been discontinued. This chassis has been replaced by an enhanced version called the Omni-5wx. The Omni-5wx is described in *Omni-5wx* on page 4-7.

Power Supplies

The Omni-5x provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to operation. See Chapter 5, "OmniSwitch Power Supplies," for more information on the Omni-5x power supplies.

Omni-5x Technical Specifications	
Total Module Slots	5
Total Slots for Switching Modules	4
Physical Dimensions	8.75" (22.23 cm) high, 17" (43.18 cm) wide, 13" (33.02 cm) deep
Weight	30 lb. (13.64 kg), fully populated with modules and power supplies.
Switching Backplane	Cell Switching Matrix 640 or 960 Mbps Frame Bus (dependent on MPM type) 120 Mbps Control Bus
Temperature Operating Range	0 to 45 degrees Celsius 32 to 113 degrees Fahrenheit
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Altitude	Sea level to 10,000 feet (3 km)
Agency Listings	UL 1950 CSA-C22.2 EN60950 FCC Part 15, Subpart B (Class A) EN55022, 1987/EN50081 FCC Class B C.I.S.P.R. 22: 1985 EN50082-1, 1992 IEC 801-2, 1991 IEC 801-3, 1984 IEC 801-4, 1988 VCCI V-3/94.04 (Class 1).

Omni-9x

The Omni-9x is physically the same as an Omni-9e. Module slots and power supplies are located in the same places and the same power supplies are used in both chassis. The primary difference between the two chassis is that the Omni-9x supports a 13.2 Gbps cell switching matrix in addition to the 640/960 Mbps frame-switching bus and the 120 Mbps management bus. The Omni-9x backplane requires the use of an MPM-II or MPM-1G module.

Frame and cell switching are integrated in the Omni-9x. All existing frame switching modules are supported in the Omni-9x. In fact, pure frame switching applications are handled without converting frames to cells and cells to frames. The chassis may be configured as a pure LAN switch (only frame switching modules), a pure ATM switch (only cell switching modules), or as a hybrid LAN/ATM switch (mixture of frame and cell switching modules).

The Omni-9x provides native ATM switching, both for backbone and workstation access. The ATM switching backplane allows the Omni-9x to support Cell Switching Modules (CSMs). CSMs support ATM25, ATM OC-3c/STM-1, and OC-12c/STM-4c interfaces. CSMs are described more thoroughly in Chapter 40, "Cell Switching Modules (CSMs)."

The ATM cell switching fabric is fully distributed with the aggregate 13.2 Gbps distributed across all Cell Switching Modules. There is no central switch component and therefore no single point of failure. In addition, the cell backplane employs an advanced dynamic input buffered/output controlled queuing scheme which provides non-blocking performance and scales buffer requirements as the system grows.

◆ Note ◆

The Omni-9x chassis is supported, but it has been discontinued. This chassis has been replaced by an enhanced version called the Omni-9wx. The Omni-9wx is described in *Omni-9wx* on page 4-9.

Power Supplies

The Omni-9x provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to operation. See Chapter 5, "OmniSwitch Power Supplies," for more information on the Omni-9x power supplies.

Omni-9x Technical Specifications	
Total Module Slots	9
Total Slots for Switching Modules	8
Physical Dimensions	17.0" (43.18 cm) high, 17.0" (43.18 cm) wide, 15.5" (39.37 cm) deep
Weight	55 lb. (25 kg), fully populated with modules and power supplies.
Switching Backplane	13.2 Gbps Cell Bus 640 or 960 Mbps Frame Bus (dependent on MPM type) 120 Mbps Control Bus.
Temperature Operating Range	0 to 45 degrees Celsius 32 to 113 degrees Fahrenheit
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Altitude	Sea level to 10,000 feet (3 km)
Agency Listings	UL 1950 CSA-C22.2 EN60950 FCC Part 15, Subpart B (Class A) EN55022, 1987/EN50081 FCC Class B C.I.S.P.R. 22: 1985 EN50082-1, 1992 IEC 801-2, 1991 IEC 801-3, 1984 IEC 801-4, 1988 VCCI V-3/94.04 (Class 1).

5 OmniSwitch Power Supplies

AC and DC power supplies are available for all OmniSwitch chassis. Except for the Omni-3wx, you can install and remove these supplies. Descriptions of the power supplies begin on page 5-3. See Chapter 4, “The OmniSwitch Chassis,” for more information on OmniSwitch chassis.

Redundant Power Supplies

OmniSwitch power supplies can support a fully configured unit. When operating with two power supplies, load sharing is automatic. In the event of failure on one of the supplies, the redundant power supply is capable of powering the OmniSwitch without any loss of data. If power to one supply fails, the switch will automatically notify the network manager and keep running with no loss of data.

Hot-Swappable Power Supplies

Power supplies can be removed and inserted while the unit is operational. You can add or replace a power supply at any time.

Dual AC Inputs

Each AC power supply has its own power cord. If dual power supplies are installed a loss of power due to a circuit breaker on one power supply will not affect the other power supply.

Replacing Power Supplies (9-Slot Chassis)

If a power supply ever needs to be replaced in an OmniSwitch or Omni Switch/Router 9-slot Chassis (e.g., Omni-9x, Omni-9e(t), Omni-9wx, Omni-9wx-PLUS, Omni-9wxp, OmniS/R-9 or OmniS/R-9p), it is strongly recommended that power supplies not be mixed, except under the conditions and exceptions shown in the following table.

◆ **Note** ◆

In all cases, swapping operations must be made with the power switch of the replacement power supply turned OFF. Failure to turn the power switch off during the swapping operation may cause the data switch to reset and restart.

Replacing Power Supplies (9-Slot Chassis)

If One of Two Power Supplies Fails	Revision	Replace	With
500-watt	Any	Both Power Supplies	Two 650-watt (Revision M1+) or two 725-watt Power Supplies
650-watt	Pre-M1	Both Power Supplies	Two 650-watt (Revision M1+) or two 725-watt Power Supplies
650-watt	M1 or later	Failed Power Supply	One 650-watt (Revision M1+) or one 725-watt Power Supply
725-watt	Any	Failed Power Supply	One 725-watt Power Supply

Omni-3wx Power Supplies

The Omni-3wx uses a built-in AC or DC power supply that can provide 150 Watts of output power. The Omni-3wx may also be connected to a Backup Power Supply (BPS) to provide power redundancy. A power connector is provided on the back of the Omni-3wx that connects to a BPS.

The Omni-3wx chassis is available in the following AC and DC versions.

- Omni-3wx The standard Omni-3wx with an AC power supply. It can provide 150 Watts of power.
- Omni-3wx-48V A -48 volt (input voltage) DC version of the Omni-3wx. This power supply can provide 150 Watts of power. It requires the use of 18 to 20 gauge wire for connections to the DC power source.
- Omni-3wx Depending on product configuration, some Omni-3wx products may feature an optional AC power supply that can provide 150 Watts of power.

◆ Caution ◆

Do not connect the power connector on the back of the Omni-3wx to data communication equipment.

◆ VORSICHT ◆

NICHT MIT DATEN-KOMMUNIKATIONSGERATEN VERBINDEN.

See *Backup Power System (BPS)* on page 5-30 for more information on the BPS.

Omni-3wx Power Supply Specifications	
Voltage Range	90-270 VAC, 47 to 63 Hz
Current Draw	3.5 Amps at 100/115 VAC 1.5 Amps at 230 VAC
Watts (Output)	150
Current Provided	25 Amps at +5 Volts; 2 amps at +12 Volts
Heat Generation	Approximately 512 BTUs per hour
Agency Listings	See Chapter 4, "The OmniSwitch Chassis," for agency listings.

Optional 150W AC/DC Power Supply

Depending on product configuration, some Omni-3wx products may feature the following power supply specifications:

Omni-3wx Power Supply Specifications	
Voltage Range	85-270 VAC, 47 to 63 Hz
Current Draw	3.5 Amps at 100/115 VAC 1.5 Amps at 230 VAC
Watts (Output)	150
Current Provided	25 Amps at +5 Volts; 5 amps at +12 Volts
Heat Generation	Approximately 512 BTUs per hour
Agency Listings	UL 1950; CSA-C22.2 #950-M90; TUV EN60950; CB Certification IEC 950; FCC Title 47 CRF Part 15, Subpart B (Class A & Class B); IEC EN55022, 1995 (Class A & Class B) CISPR 22, 1995; IEC 1000-3-2; IEC 1000-3-3 (EN60555-2); IEC 1000-4-2 (EN61000-4-2, per EN50082-1, 1992); IEC 1000-4-3 (EN61000-4-3, per EN50082-1, 1992); IEC 1000-4-4 (EN61000-4-4) Level 4; IEC 1000-4-5 (EN61000-4-5) Level 4; IEC 1000-4-6 (EN61000-4-6); IEC 1000-4-8 (EN61000-4-8); IEC 1000-4-11 (EN61000-4-11); VCCI V-3/94.04 (Class A & Class B); ENV 50204: 1996

Omni-5 Power Supplies

The Omni-5 provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to the operation.

◆ Caution ◆

This unit may be equipped with two power connections. To reduce the risk of electrical shock, disconnect both power connections before servicing the unit.

◆ VORSICHT ◆

Das Gerät kann mit zwei Netzanschlüssen ausgestattet sein. Um einen elektrischen Schlag zu vermeiden, immer beide Anschlüsse vor der Wartung vom Netz trennen.

The Omni-5 may use one of two types of power supplies.

PS5 The standard power supply. It can provide 150 Watts of power.

PS5-DC48 A -48 volt (input voltage) DC version of the PS5 power supply. This power supply can provide 150 Watts of power. It requires the use of 18 to 20 gauge wire for connections to the DC power source.

Neither of these power supplies can be used in an Omni-5e chassis.

Some combinations of switching modules (those that include CDDI and Fast Ethernet modules) may exceed the power provided by one Omni-5 power supply. Use the amp figure for your modules (in the tables beginning on page 5-18) to determine the type and number of modules your 5-slot chassis will power. See *Power Requirements* on page 5-15 for further information.

Omni-5 PS5 and PS5-DC-48 Specifications	
Current Draw	3.5 Amps at 100/115 VAC 1.5 Amps at 230 VAC
Watts (Output)	150
Current Provided	25 Amps at 5 Volts
Heat Generation	Approximately 512 BTUs per hour (one power supply)
Agency Listings	See Chapter 4, "The OmniSwitch Chassis," for agency listings.

Omni-5e Power Supplies

The Omni-5e provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to the operation.

◆ **Caution** ◆

This unit may be equipped with two power connections. To reduce the risk of electrical shock, disconnect both power connections before servicing the unit.

◆ **VORSICHT** ◆

Das Gerät kann mit zwei Netzanschlüssen ausgestattet sein. Um einen elektrischen Schlag zu vermeiden, immer beide Anschlüsse vor der Wartung vom Netz trennen.

The Omni-5e can use one of two types of power supplies.

PS5-250 The standard power supply. It can provide 250 Watts of power, and can support any possible combination of frame switching modules.

PS5-DC250 A -48 volt (input voltage) DC version of the PS5-250 power supply. This power supply can provide 250 Watts of power. It requires the use of 12 to 14 gauge wire for connections to the DC power source. See *Connecting a DC Power Source* on page 5-23 for more information.

Omni-5e PS5-250 and PS5-DC250 Technical Specifications	
Voltage Range	90-265 VAC, 47 to 63 Hz auto-ranging and auto-sensing.
Current Draw	4 Amps at 100/115 VAC 2 Amps at 230 VAC
Watts (Output)	250
Current Provided	45 Amps at 5 Volts 2 Amps at 12 Volts 5.1 Amps at 1.2 Volts 3 Amps at 3.3 Volts
Heat Generation	Approximately 853 BTUs per hour (one power supply)
Agency Listings	See Chapter 4, "The OmniSwitch Chassis," for agency listings.

Omni-5x Power Supplies

The Omni-5x provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to operation.

◆ Caution ◆

This unit may be equipped with two power connections. To reduce the risk of electrical shock, disconnect both power connections before servicing the unit.

◆ VORSICHT ◆

Das Gerat kann mit zwei Netzanschlussen ausgestattet sein. Um einen elektrischen Schlag zu vermeiden, immer beide Anschlusse vor der Wartung vom Netz trennen.

The Omni-5x can use one of two types of power supplies.

PS5-250 The standard power supply. It can provide 250 Watts of power, and can support any possible combination of switching modules.

PS5-DC250 A -48 volt (input voltage) DC version of the PS5-250 power supply. This power supply can provide 250 Watts of power. It requires the use of 12 to 14 gauge wire for connections to the DC power source. See *Connecting a DC Power Source* on page 5-23 for more information.

Omni-5x PS5-250 and PS5-DC250 Specifications	
Voltage Range	90-265 VAC, 47 to 63 Hz auto-ranging and auto-sensing.
Current Draw	4 Amps at 100/115 VAC 2 Amps at 230 VAC
Watts (Output)	250
Current Provided	45 Amps at 5 Volts 2 Amps at 12 Volts 5.1 Amps at 1.2 Volts 3 Amps at 3.3 Volts
Heat Generation	Approximately 853 BTUs per hour (one power supply)
Agency Listings	See Chapter 4, "The OmniSwitch Chassis," for agency listings.

Omni-5wx Power Supplies

The Omni-5wx provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to the operation.

◆ **Caution** ◆

This unit may be equipped with two power connections. To reduce the risk of electrical shock, disconnect both power connections before servicing the unit.

◆ **VORSICHT** ◆

Das Gerät kann mit zwei Netzanschlüssen ausgestattet sein. Um einen elektrischen Schlag zu vermeiden, immer beide Anschlüsse vor der Wartung vom Netz trennen.

The Omni-5wx can use one of two types of power supplies.

PS5-250 The standard power supply. It can provide 250 Watts of power.

PS5-DC250 A -48 volt (input voltage) DC version of the PS5-250 power supply. This power supply can provide 250 Watts of power. It requires the use of 12 to 14 gauge wire for connections to the DC power source. See *Connecting a DC Power Source* on page 5-23 for more information.

Omni-5wx PS5-250 and PS5-DC-250 Technical Specifications	
Voltage Range	90-265 VAC, 47 to 63 Hz auto-ranging and auto-sensing.
Current Draw	4 Amps at 100/115 VAC 2 Amps at 230 VAC
Watts (Output)	250
Current Provided	45 Amps at 5 Volts 2 Amps at 12 Volts 5.1 Amps at 1.2 Volts 3 Amps at 3.3 Volts
Heat Generation	Approximately 853 BTUs per hour (one power supply)
Agency Listings	See Chapter 4, "The OmniSwitch Chassis," for agency listings.

Omni-9 Power Supply

The Omni-9 provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to the operation.

◆ Caution ◆

This unit may be equipped with two power connections. To reduce the risk of electrical shock, disconnect both power connections before servicing the unit.

◆ VORSICHT ◆

Das Gerät kann mit zwei Netzanschlüssen ausgestattet sein. Um einen elektrischen Schlag zu vermeiden, immer beide Anschlüsse vor der Wartung vom Netz trennen.

The Omni-9 uses a power supply called the PS9-350T. The PS9-350T can provide 350 Watts of power. Some combinations of switching modules (those that include CDDI and Fast Ethernet modules) may exceed the power provided by one power supply. Use the amp figure for your modules (in the tables beginning on page 5-18) to determine the type and number of modules your Omni-9 chassis will power. See *Power Requirements* on page 5-15 for further information.

The Omni-9 and Omni-9e power supply may not be used interchangeably.

Omni-9 PS9-350T Specifications	
Voltage Range	85-270 VAC, 47 to 63 Hz auto-ranging and auto-sensing.
Current Draw	6 Amps at 100/115 VAC 3 Amps at 230 VAC
Watts (Output)	350
Current Provided	50 Amps at 5 Volts 8 Amps at 12 Volts 5 Amps at 3.3 Volts
Heat Generation	Approximately 1195 BTUs per hour (one power supply)
Agency Listings	See Chapter 4, "The OmniSwitch Chassis," for agency listings.

Omni-9e Power Supplies

The Omni-9e provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to the operation.

◆ **Caution** ◆

This unit may be equipped with two power connections. To reduce the risk of electrical shock, disconnect both power connections before servicing the unit.

◆ **VORSICHT** ◆

Das Gerät kann mit zwei Netzanschlüssen ausgestattet sein. Um einen elektrischen Schlag zu vermeiden, immer beide Anschlüsse vor der Wartung vom Netz trennen.

The Omni-9e can use one of the following power supply types. Power supply types cannot be mixed in the same chassis.

PS9-500 The standard power supply. It can provide 500 Watts of power, and can support any possible combination of frame switching modules.

PS9-DC500 A -48 volt (input voltage) DC version of the PS9-500 power supply. This power supply can provide 500 Watts of power. It requires 10 to 12 gauge wire for connections to the DC power source.

Omni-9e PS9-500 and PS9-DC500 Specifications	
Voltage Range	85-270 VAC, 47 to 63 Hz auto-ranging and auto-sensing.
Current Draw	8 Amps at 100/115 VAC 4 Amps at 230 VAC
Watts (Output)	500
Current Provided	75 Amps at 5 Volts 8 Amps at 12 Volts 5 Amps at 3.3 Volts 6 Amps at 1.2 Volts
Heat Generation	Approximately 1707 BTUs per hour (one power supply)
Agency Listings	See Chapter 4, "The OmniSwitch Chassis," for agency listings.

Omni-9x Power Supplies

The Omni-9x provides bays for two power supplies. The power supplies are self-enclosed to allow safe hot-insertion and hot-removal. When two power supplies are installed, they share the electrical load. If one should fail, the remaining power supply automatically takes up the load without any disruption to operation.

◆ **Caution** ◆

This unit may be equipped with two power connections. To reduce the risk of electrical shock, disconnect both power connections before servicing the unit.

◆ **VORSICHT** ◆

Das Gerät kann mit zwei Netzanschlüssen ausgestattet sein. Um einen elektrischen Schlag zu vermeiden, immer beide Anschlüsse vor der Wartung vom Netz trennen.

The Omni-9x can use the PS9-500P, PS9-500T, and PS9-DC500 power supplies, which are described in *Omni-9wx*, *Omni-9wx-PLUS* & *Omni-9wxp Power Supplies* on page 5-12. Power supply types cannot be mixed in the same chassis.

Omni-9wx, Omni-9wx-PLUS & Omni-9wxp Power Supplies

The Omni-9wx can use one of the power supply types listed below. Power supply types cannot be mixed in the same chassis.

- PS9-500T An earlier version of the standard power supply. It can provide 375 Watts of power.
- PS9-500P The standard power supply. It can provide 450 Watts of power.
- PS9-DC500 A DC version of the PS9-500 power supply. This power supply can provide 500 Watts of power. It requires 10 to 12 gauge wire for connections to the DC power source.
- PS9-650P The power supply designed for use with CSM-622 modules. It can provide 650 Watts of power.
- PS9-725 This AC power supply can provide 725 Watts of power.

The Omni-9wx-PLUS uses one of the power supply types listed below.

- PS9-650P The power supply designed for use with CSM-622 modules. It can provide 650 Watts of power.
- PS9-725 This AC power supply can provide 725 Watts of power.

The Omni-9wxp uses the power supply type listed below.

- PS9-725 This AC power supply can provide 725 Watts of power.

◆ Caution ◆

This unit may be equipped with two power connections. To reduce the risk of electrical shock, disconnect both power connections before servicing the unit.

◆ VORSICHT ◆

Das Gerät kann mit zwei Netzanschlüssen ausgestattet sein. Um einen elektrischen Schlag zu vermeiden, immer beide Anschlüsse vor der Wartung vom Netz trennen.

Omni-9wx PS9-500T Specifications	
Voltage Range	90-264 VAC, 47 to 63 Hz auto-ranging and auto-sensing.
Current Draw	8 Amps at 100/115 VAC; 4 Amps at 230 VAC
Watts (Output)	375
Current Provided	75 Amps at 5 volts 8 Amps at 12 Volts 5 Amps at 3.3 Volts 6 Amps at 1.2 Volts
Heat Generation	Approximately 1707 BTUs per hour (one power supply)
Agency Listings	See Chapter 4, "The OmniSwitch Chassis," for agency listings.

Omni-9wx PS9-500P and PS9-DC500 Specifications	
Voltage Range	40-60 Volts D.C.
Current Draw	20 Amps at 40 Volts D.C.
Watts (Output)	500
Current Provided	75 Amps at 5.35 volts 8 Amps at +12 Volts 4 Amps at -12 Volts 5 Amps at 5.2 Volts
Heat Generation	Approximately 1450 BTUs per hour (one power supply)
Agency Listings	See Chapter 4, "The OmniSwitch Chassis," for agency listings.

Omni-9wx-PLUS PS9-650P Specifications	
Voltage Range	90-264 VAC, 47 to 63 Hz auto-ranging and auto-sensing.
Current Draw	10 Amps at 100/115 VAC; 5 Amps at 230 VAC
Watts (Output)	650
Current Provided	120 Amps at 5 Volts 4 Amps at 12 Volts 6 Amps at 3.3 Volts 8 Amps at 1.2 to 1.5 Volts
Heat Generation	Approximately 2219 BTUs per hour (one power supply)
Agency Listings	See Chapter 4, "The OmniSwitch Chassis," for agency listings.

Omni-9wxp PS9-725 Specifications	
Voltage Range	85-270 VAC, 47 to 63 Hz
Current Draw	12 Amps at 100/115 VAC; 6 Amps at 230 VAC
Watts (Output)	725
Current Provided	120 Amps at 5 Volts 6 Amps at 12 Volts 6 Amps at 3.3 Volts 8 Amps at 1.2 Volts
Heat Generation	Approximately 2219 BTUs per hour (one power supply)
Agency Listings	UL 1950; CSA-C22.2 #950-M90; TUV EN60950; CB Certification IEC 950; FCC Title 47 CRF Part 15, Subpart B (Class A & Class B); IEC EN55022, 1995 (Class A & Class B) CISPR 22, 1995; IEC 1000-3-2; IEC 1000-3-3 (EN60555-2); IEC 1000-4-2 (EN61000-4-2, per EN50082-1, 1992); IEC 1000-4-3 (EN61000-4-3, per EN50082-1, 1992); IEC 1000-4-4 (EN61000-4-4) Level 4; IEC 1000-4-5 (EN61000-4-5) Level 4; IEC 1000-4-6 (EN61000-4-6); IEC 1000-4-8 (EN61000-4-8); IEC 1000-4-11 (EN61000-4-11); VCCI V-3/94.04 (Class A & Class B); ENV 50204: 1996

Power Requirements

Depending on the combination of modules installed in a chassis, it is possible to exceed the power capacity of a single power supply. Always make sure that the total power requirements of the modules in your chassis do not exceed the limits of your power supply.

To check the power consumption of your configuration, refer to the tables on pages 5-18 through 5-21 and add up the **DC Current Draw** of all modules in your switch. This sum should be below the current provided by your power supply, which is listed with the “Technical Specifications” for each chassis in the corresponding section earlier in this chapter.

For example, if you had the following modules installed in an Omni-9wx:

- 1 x MPM-1G (draws 3 amps)
- 1 x FCSM (draws 5.5 amps)
- 2 x CSM-155 (each draws 10 amps for a total of 20 amps)
- 4 x CSM-622 (each draws 14 amps for a total of 56 amps)

you would be within the power constraints of one power supply. An Omni-9wx power supply can provide up to 120 amps of current and the above configuration requires 84.5 amps. However, if you were using the Omni-9wx power supply that provides only 90 amps of current (i.e., PS9-500P) and added another CSM-622 (or any other module requiring more than 5.5 amps), then you would exceed that power supply's limit.

◆ Caution ◆

It is possible, but *not recommended*, to have a configuration in which the current draw of the installed modules exceeds the power provided by a single power supply. However, such a configuration would *require two power supplies and would not allow you to have power redundancy*.

CSM-622 Modules

If you are using CSM-622 modules in the Omni-5x, Omni-5wx, Omni-9x, Omni-9wx, Omni-9wx-PLUS or Omni-9wxp chassis, you should follow these guidelines:

- In Omni-5x or Omni-5wx chassis, you cannot install more than two (2) CSM-622 modules without exceeding the current provided by one power supply.
- In Omni-9x or Omni-9wx chassis, you can install up to six (6) CSM-622 modules if you are using the PS9-500P or PS9-DC500 power supply, which can provide 500 watts of power.
- The PS9-650 power supply for the Omni-9wx-PLUS chassis provides enough power for up to eight (8) CSM-622 modules.
- In the Omni-9wxp chassis, the PS9-725 power supply can provide 725 watts of power, enough for up to eight (8) CSM-622 modules.

Omni-5, Omni-9, Omni-9e (350 watt) Chassis

If you are using 8-port Ethernet 100Base-Tx modules in an Omni-5, Omni-9, or some older Omni-9e (350 watt) chassis, then you must abide by the following restrictions:

- **Eight-port Fast Ethernet modules.** Install no more than six (6) 8-port Ethernet 100Base-Tx modules in an Omni-9 or older Omni-9e (350 watt) chassis, and no more than three (3) such modules in an Omni-5 chassis.

◆ Warning ◆

If you exceed these limitations, then your power supplies will not be able to provide enough power to all the modules in the chassis and network interruptions may result. In addition, exceeding these restrictions may also cause overheating problems in an Omni-5 or Omni-9 chassis.

Omni-5e and Omni-9e (500 watt) Chassis

Power consumption and overheating are not an issue in the Omni-5e and newer model Omni-9e (500 watt) chassis and power supplies. Any combination of frame switching modules can be used in these chassis without exceeding the current provided by one power supply.

FCC Class B Approvals

The Omni-3wx, Omni-5e, Omni-5x, Omni-5wx, Omni-9e, Omni-9x, Omni-9wx and Omni-9wxp chassis have met FCC Class B requirements. In addition, the MPM module and several Switching Modules have also met Class B requirements. The table on the following page indicates the FCC Class for which a module has been approved.

Individual modules were tested in a fully loaded chassis that included two or more copper-based modules. The ESM-U-6 module was tested with fiber (10BaseFL) and UTP adapter boards. Also note that some class approvals were met using STP cable, UTP cable, or a ferrite clip as specified in the table.

“HSM” in this table refers to the High-Speed Module to which 100 Mbps Ethernet, Token Ring, ATM, and Frame Relay boards attach. (The HSM module is described in Chapter 7, “OmniSwitch Switching Modules.”) The values in this table apply to the original HSM (HSM) and the newer HSMs (HSM2 and HSM3).

Module Power Requirements and FCC Class Approvals

Module	Description	DC Current Draw (Amps)	FCC Class Approval
MPM/II/1G	Management Processor Module.	3.0	B
MPM-C	Cell Switching Management Processor Module	3.5	B
MPM-III	Advanced Management Processor Module	7.0	B
ESM-C-8	Ethernet module with eight 10BaseT UTP ports.	3.0	A
ESM-C-12	Ethernet module with twelve 10BaseT UTP ports.	4.0	B (STP cable) A (UTP cable)
ESM-F-8	Ethernet module with eight Fiber (ST) ports.	5.5	B
ESM-T-12	Ethernet module with one Telco 50-pin port.	3.5	B (STP cable) A (UTP cable)
ESM-U-6	Ethernet Universal module with six port slots.	5.0	B (fiber, UTP)
ESM-100C	100BaseTx card, 4 ports, on HSM. 100BaseTx card, 8 ports, on HSM.	5.5 7.0	A A
ESM-100C-FD	100BaseTx full-duplex card, 1 port, on HSM. 100BaseTx full-duplex card, 2 ports, on HSM.	3.5 4.5	A A
ESM-100FM-FD	100BaseFx full-duplex multimode, 1 port, on HSM. 100BaseFx full-duplex multimode, 2 ports, on HSM.	3.5 4.5	B B
ESM-100FS-FD	100BaseFx full-duplex single mode, 1 port, on HSM. 100BaseFx full-duplex single mode, 2 ports, on HSM.	3.5 4.5	B B
ESM-100C-12	10/100 Ethernet module with 12 auto-sensing ports	9.0	B (STP cable)
ESM-C-16	Ethernet module with 16 10BaseT ports	6.5	A (UTP cable)
ESM-C-32	Ethernet module with 32 10BaseT ports.	7.0	A (UTP cable)
ESM-100FM-8	100BaseFx multimode, 8 ports	7.5	A
ESM-FM-16W	Ethernet module with 16 10 Mbps Fiber ST ports	7.75	B
ESM-T-24W	Ethernet module with two Telco 50-pin ports.	3.25	A
ESM-100C-32W	Ethernet module with 32 10/100 RJ-45ports.	5.75	A (UTP cable)
GSM-FM-2W	Gigabit Ethernet multimode, 2 SC ports	6.75	B
GSM-FS-2W	Gigabit Ethernet intermediate-reach single mode, 2 SC ports	6.75	B
GSM-FH-2W	Gigabit Ethernet long-reach single mode, 2 SC ports	6.75	B

continued on next page...

Module Power Requirements and FCC Class Approvals

Module	Description	DC Current Draw (Amps)	FCC Class Approval
ASM-155F	ATM OC-3 card, 1 fiber port, on HSM. ATM OC-3 card, 2 fiber ports, on HSM.	3.0 4.0	B B
ASM2-155F (narrow faceplate)	ATM OC-3 card, SAHI chip, 1 fiber port, on HSM. ATM OC-3 card, SAHI chip, 2 fiber ports, on HSM.	4.0 5.0	A A
ASM2-155F (wide faceplate)	ATM OC-3 card, SAHI chip, 1 fiber port, on HSM. ATM OC-3 card, SAHI chip, 2 fiber ports, on HSM.	3.0 4.0	A A
ASM2-155RF	ATM OC-3 card, 1 redundant fiber port, on HSM. ATM OC-3 card, 2 redundant fiber ports, on HSM.	3.5 5.0	A A
ASM-155C	ATM UTP card, 1 copper port, on HSM. ATM UTP card, 2 copper ports, on HSM.	3.0 4.0	B (STP cable) A (UTP cable)
ASM2-622F	ATM OC-12 card, 1 fiber port, on HSM. ATM OC-12 card, 2 fiber ports, on HSM.	4.0 6.0	A A
ASM2-622-RF	ATM OC-12 card, 1 fiber port, on HSM. ATM OC-12 card, 2 fiber ports, on HSM.	5.0 8.0	A A
ASM2-E3	ATM E3 card, 1 BNC port, on HSM. ATM E3 card, 2 BNC ports, on HSM.	4.0 5.5	A A
ASM-DS3	ATM DS-3 card, 1 BNC port, on HSM. ATM DS-3 card, 2 BNC ports, on HSM.	3.0 4.0	A A
ASM-E3	ATM E3 card, 1 BNC port, on HSM. ATM E3 card, 2 BNC ports, on HSM.	3.0 4.0	B B
ASM-CE-155F-2S2T	ATM Circuit Emulation, 1 OC-3, 2 serial, 2 T1 ports	4.5	A
ASM-CE-155F-2S2E	ATM Circuit Emulation, 1 OC-3, 2 serial, 2 E1 ports	4.5	B
ASM-CE-DS3-2S2T	ATM Circuit Emulation, 1 DS-3, 2 serial, 2 T1 ports	4.5	A
ASM-CE-E3-2S2T	ATM Circuit Emulation, 1 E3, 2 serial, 2 E1 ports	4.5	B
ASM2-DS3	ATM DS-3 card, 1 BNC port, on HSM. ATM DS-3 card, 2 BNC ports, on HSM.	4.0 5.5	B B
ASM2-E3	ATM E3 card, 1 BNC port, on HSM. ATM E3 card, 2 BNC ports, on HSM.	4.0 5.5	B B

continued on next page...

Module Power Requirements and FCC Class Approvals “continued”

Module	Description	DC Current Draw (Amps)	FCC Class Approval
TSM-C-6	Token Ring, 6-port UTP/STP card, on HSM.	5.0	A (STP cable)
TSM-F-6	Token Ring, 6-port fiber card, on HSM.	5.0	A
TSM-CD-6	Token Ring, 6-port STP card, on HSM.	5.0	B (UTP cable)
TSM-CD-16W	Token Ring, 16-port UTP/STP ports	8.0	B (STP cable) A (UTP cable)
WSM	WAN module, 2 serial ports on HSM. WAN module, 4 serial ports on HSM. WAN module, 8 serial ports on HSM.	3.5 4.0 6.0	B B B
WSM-BRI	WAN ISDN module, 1 serial, 1 BRI port on HSM. WAN ISDN module, 2 serial, 2 BRI ports on HSM.	4.5 5.0	B B
WSM-FT1	WAN T1 module, 1 serial, 1 T1 port on HSM. WAN T1 module, 2 serial, 2 T1 ports on HSM.	3.5 5.0	A A
WSM-FE1	WAN E1 module, 1 serial, 1 T1 port on HSM. WAN E1 module, 2 serial, 2 T1 ports on HSM.	3.5 5.0	B B

continued on next page...

Module Power Requirements and FCC Class Approvals “continued”

Module	Description	DC Current Draw (Amps)	FCC Class Approval
FCSM I	Frame-to-Cell Switching Module (155 Mbps)	5.5	B
FCSM II	Frame-to-Cell Switching Module (622 Mbps)	7.75	B
CSM-A25-12	Cell Switching Module with 12 x ATM 25 Mbps ports	4.5	A
CSM-A25-24W	Cell Switching Module with 24 x ATM 25 Mbps ports	6.5	A
CSM-155-8	Cell Switching Module with 8 x OC-3 fiber ports	10.0	B
CSM-155C-8	Cell Switching Module with 8 x OC-3 copper ports	10.0	A
CSM-622	Cell Switching Module with 2 x OC-12 fiber ports	14.0	A
CSM-U	Universal Cell Switching Module, no adapter boards	3.5	B
CSM-U+	Advanced Universal Cell Switching Module, no adapter boards	3.5	B (STP cable) A (UTP cable)
CSM-AB-155C	CSM-U/CSM-U+ Adapter Board, 2 OC-3 multimode copper ports	1.0	A
CSM-AB-155FM	CSM-U/CSM-U+ Adapter Board, 2 OC-3 multimode fiber ports	1.2	B
CSM-AB-155FS	CSM-U/CSM-U+ Adapter, 2 OC-3 single mode fiber ports	1.3	B
CSM-AB-155FH	CSM-U/CSM-U+ Adapter Board, 2 OC-3 single mode (long reach) fiber ports	1.4	B
CSM-AB-DS3	CSM-U/CSM-U+ Adapter Board, 2 DS-3 ports	0.7	A
CSM-AB-E3	CSM-U/CSM-U+ Adapter Board, 2 E3 ports	0.7	B
CSM-AB-DS1	CSM-U/CSM-U+ Adapter Board, 4 DS-1 ports	0.5	A
CSM-AB-E1	CSM-U/CSM-U+ Adapter Board, 4 E1 ports	0.5	B
CSM-AB-CE-T1	CSM-U/CSM-U+ Adapter Board, 4 T1 ports	0.9	A
CSM-AB-CE-E1	CSM-U/CSM-U+ Adapter Board, 4 E1 ports	0.9	B
CSM-AB-IMA-DS1	CSM-U/CSM-U+ Adapter Board, 8 IMA DS-1 (T1) ports	2.5	A
CSM-AB-IMA-E1	CSM-U/CSM-U+ Adapter Board, 8 IMA E1 ports	2.5	A

continued on next page...

Removing and Installing a Power Supply

You can remove or install a power supply even when power is being supplied to an OmniSwitch. You will need a slotted and a Phillips screwdriver to remove or install a power supply.

Removing a Power Supply

1. Turn the On/Off switch to the O (Off) position on the power supply that you want to remove. Power may still be provided to the power supply you are not removing, but it cannot be applied to the one you are removing.
2. Remove the power cord attached to the AC input socket on the power supply. Even with power Off, the switch backplane could be damaged if the power cord is attached and a power surge occurs.
3. Each power supply is attached to the chassis with four screws. Two of the screws are attached to springs and cannot be removed from the power supply. The other two screws are loose and can be separated from the power supply.

Loosen and remove the two loose screws. These screws will be located at the top of a 5-slot power supply and on the right side (or top, depending on the chassis type) of a 9-slot power supply.

4. Loosen the two screws attached to the power supply by springs.
5. Holding onto the two screws attached to the power supply, pull the power supply out and away from the chassis. Do not hesitate when removing the power supply.
6. Place the power supply in a safe, static-free location until it is re-installed.

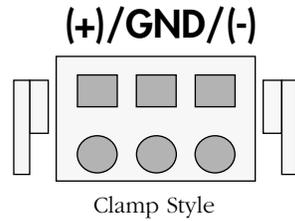
Installing a Power Supply

1. Ensure that the On/Off switch on the power supply is in the O (Off) position.
2. Holding the power supply with both hands, align it with the card guides in the slot where it is to be installed.
3. Gently slide the power supply into the chassis along the card guides. The power supply should slide easily as long as you keep it level and within the card guides. Keep sliding it back until it snaps into place against the switch backplane. The power supply should fit snugly into its slot.
4. Tighten the two screws attached to the power supply.
5. Insert and tighten the two loose screws into the top two holes of a 5-slot power supply and the right (or top, depending on the chassis type) two holes of a 9-slot power supply.
6. Attach the power cord to the AC input socket.
7. Turn the On/Off switch to the I (On) position when you are ready to provide power to the chassis through this power supply.

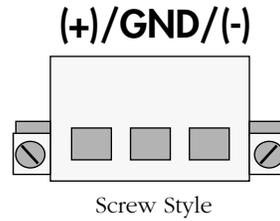
Connecting a DC Power Source

The DC power supply on your switch contains a female power connector. Five-slot OmniSwitches use the 48-volt Omni-PS5-DC250 power supply, which can contain one of the two power connectors pictured below. Nine-slot OmniSwitches use the 48-volt Omni-PS9-DC500 power supply, which uses the power connector pictured below.

Omni-PS5-DC250

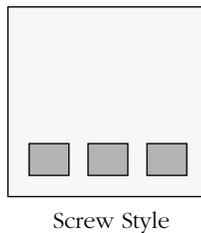


**Omni-PS5-DC250,
Omni-3wx-48V, and
BPS-DC-PS-250**



Omni-PS9-DC500

(-)/(+)/GND



GND =

OmniSwitch DC Power Supply Connector Styles

All power connector styles require the use of 12 gauge wire. A clamp inside each connector keeps the power wire tightly in place during operation.

The Omni-PS5-DC250 style shown above on the left has side clamps that can be pinched to remove the connector. The Omni-PS5-DC250 style on the right has side screws that can be used to remove the connector.

The procedure for plugging a power source into each connector type will be different. For purposes of this procedure, the Omni-PS5-DC250 connector on the left will be referred to as the “clamp-style” connector and the Omni-PS5-DC250 connector on the right will be referred to as the “screw-style” connector. Although the Omni-PS9-DC500 connectors do not have attachment screws, it will be referred to as the “screw-style” since the procedure is the same.

Installing DC Power Source Wire Leads

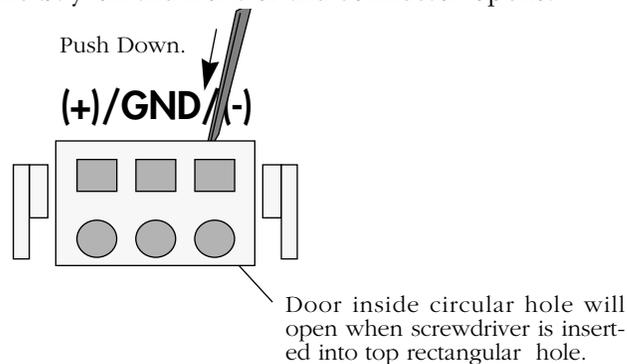
These instructions describe how to connect your 3-wire DC power source to the power connector on your DC power supply. A small flat-tip screwdriver and a wire stripper are required for this procedure.

1. Prepare the three (3) wires—12 gauge—that will plug into the power supply. First make sure they are not plugged into the 48-volt power source. Next, use a wire stripper to carefully strip about a half-inch off the end of each wire, removing the outer insulation to expose the copper core.
2. Twist the loose strands of copper wire together so that they form a tight braid. If possible, solder the entire braid of wire together for better conductivity.
3. Open the wire bay door for one of the three (3) power connector holes. The procedure for opening the bay door is different for each power connector style. Follow the instructions on the next page for your connector style.

“Clamp” Style Connector

This connector contains a row of square holes and row of circular holes. It also contains three rectangular holes on top; these top rectangular holes are used to open the circular holes on the connector front so that you can insert the wire lead.

- a. Insert a flat-tip screwdriver into one of the top three (3) square holes. Use some force so that the door for the wire bay on the front of the connector opens.

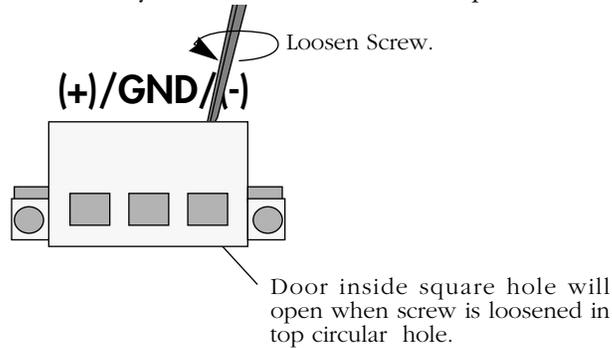


Opening Wire Bay on Clamp-Style Connector

"Screw" Style Connector

The front of this connector contains a row of square holes. It also contains three circular holes on top containing screws; you loosen the screws in these holes to open the square holes on the connector front so that you can insert the wire lead.

- a. Insert a small flat-tip screwdriver into one of the top three (3) screw holes. Loosen the screw so that the door for the wire bay on the connector front opens.



Opening Wire Bay on Screw-Style Connector

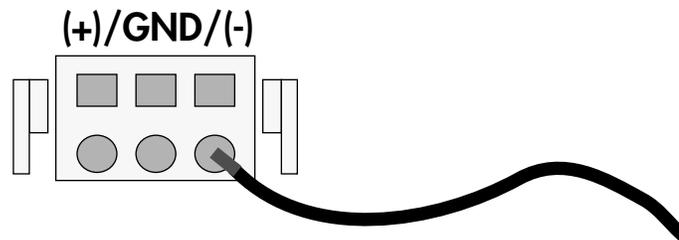
4. Insert the appropriate wire lead into the open circular hole. The silkscreen above each hole indicates which power lead—positive (+), ground (GND), or negative (-)—to plug into which hole. The lead you insert *must* match the lead attached to the 48-volt power source (i.e., positive to positive, negative to negative, ground to ground).

◆ Warning ◆

You must plug DC wire leads into the correct holes in the DC power connector. Use the labels above the DC power connector as a guide to positive, negative, and ground connections.

If you plug wire leads into wrong holes the power supply will not work and could result in damage.

Push the wire in far enough such that it reaches the back wall of the connector, about a half inch inside.



This end would plug into the negative (-) power source. The rightmost lead would plug into the positive (+) power source and the middle lead would plug into the ground (GND).

Inserting the Wire Lead Into the Circular Hole

5. Close the wire bay. The procedure for closing the bay door is different for each power connector style. Follow the instructions below for your connector style.

“Clamp” Style Connector

Remove the screwdriver from the rectangular hole on top of the power connector. The wire lead should be securely attached inside the connector. You should be able to pull on the wire and not dislodge it.

“Screw” Style Connector

Using the small screwdriver from Step 3a, tighten the screw above the wire bay into which you inserted a wire lead. The wire lead should be securely attached inside the connector. You should be able to pull on the wire and not dislodge it.

6. Repeat Steps 3 through 5 for the remaining two wire leads. Be sure that the end of each lead attaches to the same power source that you connected to on the power supply (i.e., positive to positive, negative to negative, ground to ground).

Replacing a Power Supply Fuse (older chassis models)

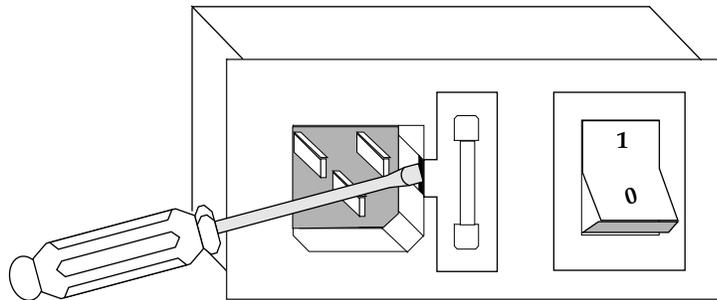
◆ Important Note ◆

This procedure applies only to the older chassis versions, Omni-5 and Omni-9. Other chassis do not contain replaceable fuses.

On the Omni-5, the fuse for each power supply is located in a holder immediately to the right of the power cable receptacle. On the Omni-9, the fuse for each power supply is located in a holder immediately below the power cable receptacle. The holder also contains one spare fuse. When you replace the fuse, replace it with a fuse of the same type and rating for continued protection against fire. Each power supply uses a 250 volt, 3.15 amp fuse.

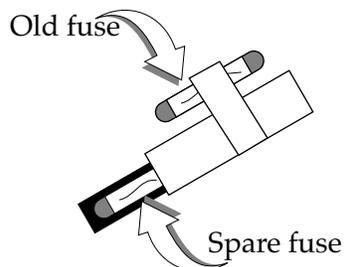
Follow these steps to replace the fuse:

1. Turn the On/Off switch to the O (Off) position on the power supply where you want to replace the fuse. Power may still be provided to the other power supply.
2. Remove the power cord from the power supply.
3. Using a small screwdriver, remove the fuse holder by pulling outward on the small recess (located on the right of the power receptacle).



Removing the Fuse Holder

4. Remove the old fuse that is held in place by the fuse clip and throw it away.
5. To access the spare fuse, slide the box open by pushing on one end of the fuse holder.



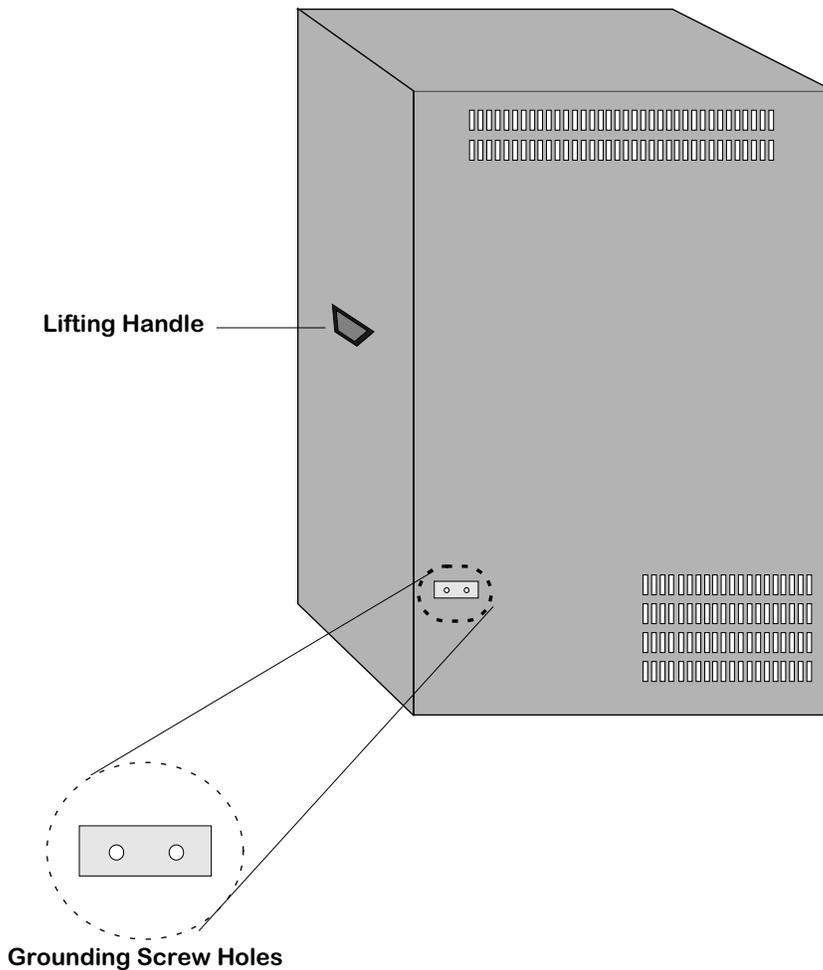
Removing the Fuse Holder

6. Put the spare fuse in the fuse clip.
7. Replace the fuse holder in the power receptacle.

Grounding a Chassis

Wide-format chassis (Omni-3wx, Omni-5wx, and Omni-9wx) have two grounding screw holes on the back of the chassis. These holes use 10-32 screws and are approximately 1 inch apart. In addition, these holes do not have paint and are surrounded by a small paint-free rectangular section, which provides for a good connection contact.

The figure below shows the location of the grounding screw holes on the back of a newer Omni-9wx. They are located approximately four (4) inches from the bottom of the chassis and approximately one (1) inch from the left-hand side of the rear of the chassis.



Grounding Screw Holes on an Omni-9wx

On an Omni-5wx, they are located about one (1) inch from the bottom of the chassis and approximately one (1) inch from the left-hand side of the rear of the chassis. On an Omni-3wx, they are located about four (4) inches from the bottom of the chassis and approximately 1/2-inch from the left-hand side of the rear of the chassis.

Power Cords

The power cord is the main disconnect device. It should be plugged into an easily accessible outlet. In the event that your power cord is lost or damaged, refer to the specifications below.

Das Netzkabel ist das hauptsächliche Trennungsmittel fuer den Netzanschluss. Es sollte in eine leicht erreichbare Steckdose gesteckt werden. Im Falle des Verlustes oder Beschädigung beziehen Sie sich auf unten stehende Spezifikationen.

Specifications

The power cord to be used with 115-Volt configuration is a minimum type SJT (SVT)18/3, rated at 250 Volts ac, 10 Amps with a maximum length of 15 feet. One end terminates in an IEC 320 attachment plug and the other end terminates in a NEMA 5-15P plug.

The power cord to be used with 230-Volt configuration is minimum type SJT (SVT) 18/3, rated 250 Volts ac, 10 Amps with a maximum length of 15 feet. One end terminates in an IEC 320 attachment plug and the other end terminates as required by the country where it will be installed.

European cords must be Harmonized (HAR) type.

In einer 230 Volt Umgebung ist ein Netzkabel vom Type VDE oder HAR, minimal 3 x 1.00 mm², 250 VAC, 10 Amps, maximal 4.5 m Laenge, zu verwenden. Ein Ende entspricht dem Stecker IEC 320. Das andere Ende den Anforderungen des Jeweiligen Landes.

Backup Power System (BPS)

The Backup Power System (BPS) is a chassis that accepts one or two power supplies and provides primary or redundant power for up to three Omni-3wx switches. The following power supplies can be installed in the BPS:

BPS-AC-PS-250 An AC power supply providing 50 Amps and 250 Watts of power at 5 Volts.

BPS-DC-PS-250 A 48 volt (input voltage) DC version of the BPS-AC-PS-250 power supply, also providing 50 Amps and 250 Watts of power at 5 Volts. It requires the use of 12 to 14 gauge wire for connections to the DC power source. See *Connecting a DC Power Source* on page 5-23 for more information.

Both of these power supplies are self-enclosed to allow safe hot-insertion and hot-removal.

Operation with One Power Supply Installed in the BPS

Connecting up to three Omni-3wx switches to an AC power source and the BPS provides “secondary power redundancy” where the BPS shares the electrical load with the attached switches. If the power supply in any connected Omni-3wx switch fails, the BPS picks up the load without disrupting service.

Note, however, that a switch with a failed power supply should be replaced as expeditiously as possible because the BPS may not be able to support a second failure. This would be particularly true if the aggregate power requirements of the modules installed in all attached Omni-3wx switches exceeded 50 amps.

Alternatively, you could connect up to three Omni-3wx switches to the BPS without plugging those switches into any other power source (i.e., not use the switches’ internal power supplies). The BPS provides enough power to run up to three Omni-3wx switches as long as all installed modules do not require more than 50 amps of current. (See the tables in *Power Requirements* on page 5-15 to find out the power requirements of each module.)

Operation with Two Power Supplies Installed in the BPS

Connecting up to three Omni-3wx switches to an AC power source and the BPS provides “secondary power redundancy” where the BPS shares the electrical load with the attached switches. If the power supply in any connected Omni-3wx switch fails, the BPS picks up the load without disrupting service.

Connecting up to three Omni-3wx switches to the BPS and then connecting the switches themselves to one independent power source and the BPS to another independent power source provides “primary power redundancy” as well as “secondary power redundancy.” If the power supply in any connected Omni-3wx switch fails, the BPS picks up the load without disrupting service (secondary power redundancy). If one power source fails (for example the electrical circuit connected to the Omni-3wx switches) the second power source (in our example, the electrical circuit connected to the BPS) prevents the switches from failing (primary power redundancy).

With two power supplies, the BPS can provide power redundancy for up to three switches (i.e., the BPS backs up the switches’ built-in power supplies) or the BPS can provide the power for up to three switches (i.e., the switches’ built-in power supplies are not plugged in and the switches depend on the BPS for all power).

If the BPS is providing all power (i.e., the switches’ built-in power supplies are not plugged in), one BPS power supply can fail without disrupting service as long as the aggregate power requirements of all modules in all attached switches do not exceed 50 amps. If three Omni-3wx switches are connected to the BPS and their power requirements exceed 50 amps, losing one power supply would cause all three connected switches to fail since the three switches require more power than one BPS power supply provides.

The BPS does not require that both power supplies be the same type (i.e., if desired, you can install an AC and DC power supply in the same BPS).

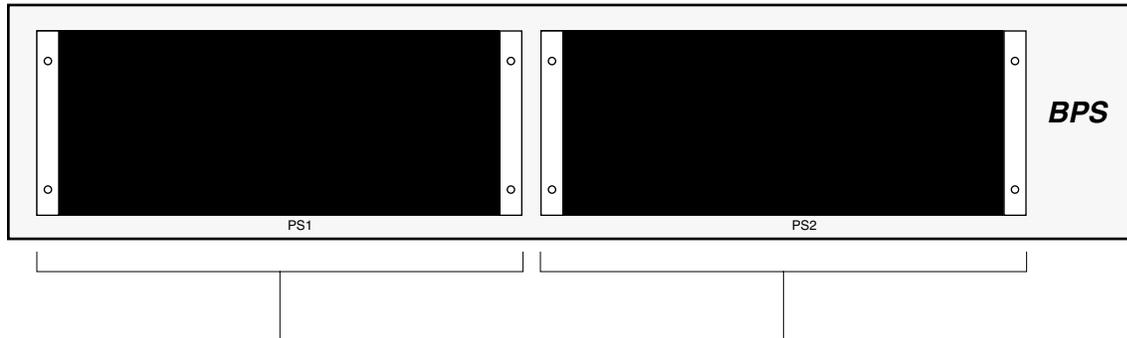
As mentioned before, with the exception of Omni-3wx switches that collectively draw more than 50 amps, the BPS can support up to three failed power supplies in the connected switches without disrupting service. However, regardless of this capability, a switch with a failed power supply should be replaced as expeditiously as possible.

◆ Important ◆

The power supplies in the BPS must be turned on
BEFORE the BPS is connected to an Omni-3wx switch.

Front Panel

The front panel provides two power supply bays, as shown in the following illustration.

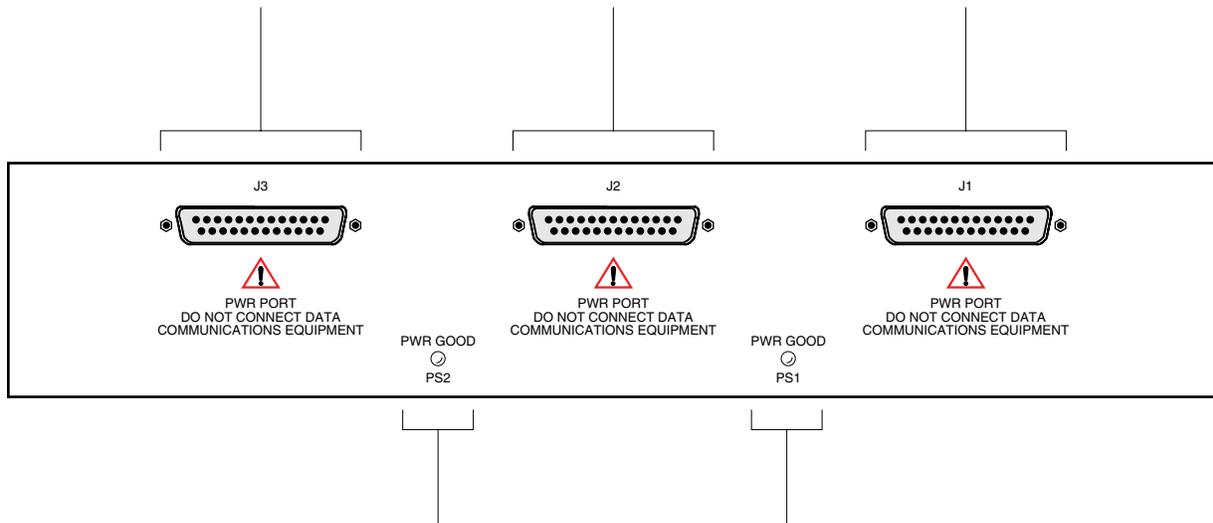


These power supply bays accept BPS-AC-PS-250 or BPS-DC-PS-250 power supplies. You can install the same type of power supply in each bay or install one of each type in each bay (i.e., you can install a BPS-AC-PS-250 in one bay and a BPS-DC-PS-250 in the other bay). If you are only installing one power supply, you can use either bay.

Rear Panel

These BPS power connectors require a unique cable (model name BPS-EXP-CBL, part number 120086-00). Do NOT attempt to use a standard DB-25 to DB-25 datacom cable to connect the BPS to the Omni-3wx switches.

If you are connecting less than three Omni-3wx switches, you can use any of the BPS power connectors.



PS1 PS2 PWR GOOD LEDs. The PWR GOOD **PS1** LED reports the status of the power supply in bay one. The PWR GOOD **PS2** LED reports the status of the power supply in bay two.

If a power supply is not installed in bay one or two, the corresponding LED is off. If a power supply is installed, but not receiving power or has failed, the corresponding LED is off.

If a power supply is installed in bay one or two and operating normally, the corresponding LED is green.

◆ Caution ◆

Do NOT connect any data communications equipment to these DB-25 BPS connectors. Although similar in appearance to a standard datacom DB-25 connector, connecting anything other than an Omni-3wx switch to these connectors may cause damage to the attached equipment.

NICHT MIT DATEN-KOMMUNIKATIONSGERÄTEN VERBINDEN.

The unit may be equipped with two power connections. To reduce the risk of electrical shock, disconnect both power connections before servicing unit.

Das Gerät kann mit zwei Netzanschlüssen ausgestattet sein. Um einen elektrischen Schlag zu vermeiden, immer beide Anschlüsse vor der Wartung vom Netz trennen.

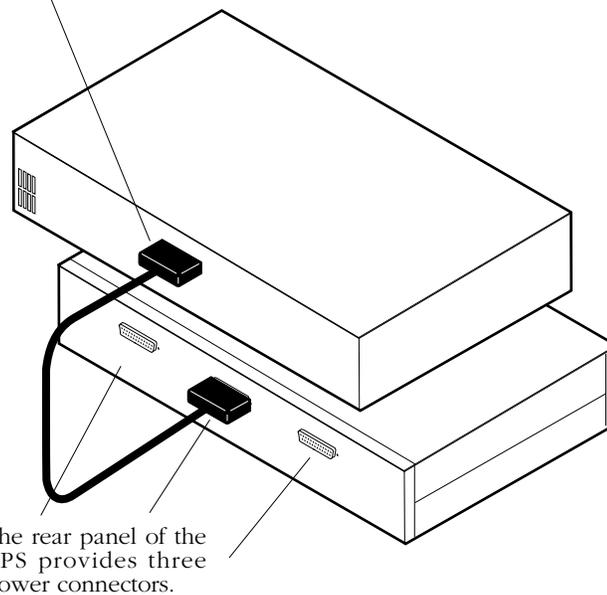
Connecting a BPS to an Omni-3wx

The BPS provides three power connectors on the rear panel. If you are connecting fewer than three Omni-3wx switches, you can use any of the BPS power connectors.

◆ Warning ◆

The BPS power connectors on the rear panel require a unique cable (Alcatel part number 120086-00). Do NOT attempt to use a standard DB-25 to DB-25 datacom cable to connect the BPS to the Omni-3wx switches.

Every Omni-3wx switch provides a BPS power connector on the rear panel.



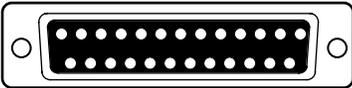
Follow the steps below to connect a BPS to an Omni-3wx.

1. Using the power cable provided with the BPS chassis, connect the female end of the cable to one of the male **PWR PORT** connectors on the rear panel of the BPS.
2. Connect the other end of cable (i.e., the male end) to the female **PWR PORT** connector on the rear panel of the Omni-3wx switch.
3. If you are connecting more than one Omni-3wx switch to the BPS, repeat steps 1 and 2.

◆ Warning ◆

The power supplies in the BPS must be turned on BEFORE the BPS is connected to the switch.

BPS Technical Specifications

Backup Power System (BPS) Technical Specifications																					
Dimensions	3.475" (8.83 cm) high x 17.125" (43.50 cm) wide x 12.46" (31.65 cm) long																				
Number of power supply bays	2																				
Rear panel power connectors	3 male DB-25 connectors																				
Power Supplies Supported	BPS-AC-PS-250, BPS-DC-PS-250																				
Maximum +5V operating current per power connector	25 Amps																				
Maximum +12V operating current per power connector	1 Amp																				
Maximum +5V operating current for all three power connectors	One Power Supply: 50 Amps Two Power Supplies: 75 Amps																				
Maximum +12V operating current for all 3 power connectors	One Power Supply: 1.5 Amps Two Power Supplies: 3 Amps																				
Heat Generation	approximately 853 BTUs per hour																				
Number of Omni-3wx supported	3																				
Cable Supported	BPS-EXP-CBL, part number 120086-00																				
Pin-outs	<p>Power connector:</p>  <table border="0"> <tr> <td>Pin 1</td> <td>Connection Detect 1</td> </tr> <tr> <td>Pins 2 thru 5</td> <td>Power Ground</td> </tr> <tr> <td>Pin 6</td> <td>+12 VDC</td> </tr> <tr> <td>Pin 7</td> <td>Key</td> </tr> <tr> <td>Pins 8 thru 13</td> <td>Power Ground</td> </tr> <tr> <td>Pins 14 thru 18</td> <td>+5 VDC</td> </tr> <tr> <td>Pin 19</td> <td>BPS Present</td> </tr> <tr> <td>Pin 20</td> <td>BPS Power Fail</td> </tr> <tr> <td>Pins 21 thru 24</td> <td>+5 VDC</td> </tr> <tr> <td>Pin 25</td> <td>Connection Detect 2</td> </tr> </table>	Pin 1	Connection Detect 1	Pins 2 thru 5	Power Ground	Pin 6	+12 VDC	Pin 7	Key	Pins 8 thru 13	Power Ground	Pins 14 thru 18	+5 VDC	Pin 19	BPS Present	Pin 20	BPS Power Fail	Pins 21 thru 24	+5 VDC	Pin 25	Connection Detect 2
Pin 1	Connection Detect 1																				
Pins 2 thru 5	Power Ground																				
Pin 6	+12 VDC																				
Pin 7	Key																				
Pins 8 thru 13	Power Ground																				
Pins 14 thru 18	+5 VDC																				
Pin 19	BPS Present																				
Pin 20	BPS Power Fail																				
Pins 21 thru 24	+5 VDC																				
Pin 25	Connection Detect 2																				

BPS Power Supplies

The Backup Power System (BPS) supports two different power supplies:

BPS-AC-PS-250 The standard power supply. It has a capacity of 50 Amps and can provide 250 Watts of power at 5 Volts. It can support any possible combination of switches.



BPS-DC-PS-250 A 48 volt (input voltage) DC version of the BPS-AC-PS-250 power supply. This power supply has a capacity of 50 Amps and can provide 250 Watts of power at 5 Volts. It requires the use of 12 to 14 gauge wire for connections to the DC power source. It supports an input voltage range of -40 to -60 VDC (-48 VDC nominal). It can support any possible combination of switches.



6 The Management Processor Module (MPM)

The MPM is the core of the distributed management functionality of the OmniSwitch. It provides such system services as maintenance of user configuration information, downloading of switching module software, basic bridge management functions, basic routing functions, the SNMP management agent, and access to the User Interface software.

Switching modules are dependent on the MPM for downloading software and for receiving initialization and configuration information. In addition, the Network Management System (NMS), which includes Switch Manager and AutoTracker software, depends on the MPM to send and receive SNMP messages for managing the switch.

Redundant storage of system configurations is available through the use of redundant Management Processor Modules. Each MPM in a redundant configuration stores information for the switch. If one MPM fails, the other MPM automatically assumes all management responsibilities. After initialization, the new MPM will read the configuration information from the existing MPM as long as you set automatic configuration synchronization to active.

There are five (5) versions of the MPM: the original MPM, the MPM-II, the MPM-1G, the MPM-III, and the MPM-C. The MPM-1G is also available in a wide version, the MPM-1GW, that fits in the new wide chassis. The MPM-III and MPM-C are available in wide format only. The following sections describe the five types (see also *MPM Types Matrix* on page 6-3).

◆ Note ◆

If you want to use an MPM-C or MPM-III in an Omni-3wx, the Omni-3wx *must* be Rev. B (part no. 180548-10) or later.

Original MPM

The original MPM has been discontinued, but it is still supported. Some previous versions of the original MPM came standard with 2 MB of flash memory and 4 MB of DRAM. Flash memory on these older versions can be upgraded to 4 MB and DRAM can be upgraded to 8 MB. The DRAM upgrade is required to run OmniSwitch software release 2.0 and 2.1. The flash memory upgrade is recommended but not required unless the OmniSwitch contains all types of Switching Modules. The original MPM supports version 3.0 and later of OmniSwitch software as long as 16 MB of DRAM has been installed.

MPM-II

The MPM-II has been discontinued, but it is still supported. The MPM-II contains additional hardware logic to support Advanced Routing features and clocking for ATM cell switch configurations. The MPM-II comes standard with 4 MB of flash memory and 8 MB of DRAM. This standard configuration is normally adequate for most configurations even those with ATM modules employing Switched Virtual Circuits (SVCs). ATM cell switching and Advanced Routing configurations require 16 MB of DRAM. *Version 3.0 of OmniSwitch software and later requires 16 MB of DRAM and 4 MB of flash memory.*

MPM-1G

The original MPM and the MPM-II support a backplane switching capacity of 640 Mbps. The MPM-1G expands this capacity to 960 Mbps. The MPM-1G supports either 640 or 960 backplanes so it is backward compatible with the original MPM and the MPM-II. The MPM-1G also supports Advanced Routing and ATM cell switching configurations.

The MPM-1G is also available in a wide version, the MPM-1GW, that fits in the new wide chassis (Omni-5wx and Omni-9wx). Both versions of the MPM-1G come standard with 4 MB of flash memory and 16 MB of DRAM. They each also contain a socket for the Hardware Routing Engine (HRE), which is described in *MPM-II and MPM-1G HRE and HRE-Plus* on page 6-17.

MPM-III

The MPM-III can be used in wide chassis versions of the OmniSwitch. It contains a high-speed CPU and it supports the 960 Mbps backplane speed. The MPM-III supports Advanced Routing and ATM cell switching configurations.

◆ Note ◆

The MPM-III does *not* support the 640 Mbps backplane speed.

The MPM-III also has an Ethernet management port that provides high-speed software transfers and user access to switch management functions. (See *MPM-III Ethernet Management Port* on page 6-10 for more information on the Ethernet management port.) The MPM-III also has a connector for the HRE-VX hardware routing engine, which is described in *MPM-III HRE-VX* on page 6-18.

MPM-C

The MPM-C can be used in wide-chassis versions of the OmniSwitch for ATM cell switching only. It combines the management functions of an MPM with cell switching matrix of a Frame to Cell Switching Module (FCSM). It comes standard with 8 MB of flash memory and 32 MB of DRAM. And it supports a cell switching fabric up to 13.2 Gbps.

Since the MPM-C is designed for ATM cell switching only; it does not support any frame switching modules (e.g., ESMs, FSMs, TSMs, etc.) and it does not support Advanced Routing software. See Chapter 40, “Cell Switching Modules (CSMs),” for more information on the MPM-C.

MPM Types Matrix

There are five (5) different versions of the Management Processor Module (MPM). The following table summarizes the five types.

	Original MPM	MPM-II	MPM-1G	MPM-III	MPM-C
VBUS Speed (Mbps)	640	640	640 or 960	960	N/A
Cell Bus Capacity (Gbps)	N/A	N/A	N/A	N/A	Up to 13.2
Standard Flash Memory	2 MB (upgrades to 4 MB)	4 MB (upgrades to 12 MB)	4 MB (upgrades to 12 MB)	8 MB (upgrades to 32 MB)	8 MB (upgrades to 32 MB)
Standard DRAM	4 MB (upgrades to 16 MB)	8 MB (upgrades to 16 MB)	16 MB (upgrades to 64 MB)	32 MB (upgrades to 128 MB)	32 MB (upgrades to 128 MB)
Standard SDRAM	N/A	N/A	N/A	64 MB	64 MB
Original HRE Supported?	No	Yes (with 16 MB DRAM)	Yes	No	No
HRE-Plus Supported?	No	No	Yes	No	No
HRE-VX Supported?	No	No	No	Yes	No
Ethernet Management Port?	No	No	No	Yes	Yes
Frame Switching Supported?	Yes	Yes	Yes	Yes	No
ATM Cell Switching Supported?	No	Yes (with 16 MB DRAM)	Yes	Yes	Yes
FCSM Required for ATM Cell Switching?	N/A	Yes	Yes	Yes	No
Advanced Routing Supported?	Yes (with 16 MB DRAM)	Yes (with 16 MB DRAM)	Yes	Yes	No
3.0-3.2 Software Supported?	Yes (with 16 MB DRAM)	Yes (with 16 MB DRAM)	Yes	No	No
4.1 and above Software Supported?	Yes (with 16 MB DRAM)	Yes (with 16 MB DRAM)	Yes	Yes	Yes
Narrow Version Available?	Yes	Yes	Yes	No	No
Wide Version Available?	No	No	Yes	Yes	Yes

OK1 (Hardware Status). This dual-state LED is on Green when the MPM has passed power-on hardware diagnostics successfully. On Amber when the hardware has failed diagnostic tests. If the **OK1** LED is alternating Green and Amber, then file system compaction is in progress.

Caution

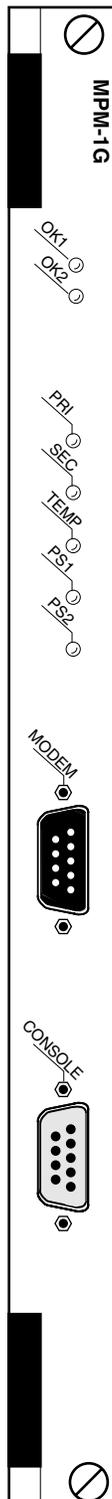
Do not power down the switch or insert any modules while the **OK1** LED is alternating Green and Amber. If you do, file corruption may result and you will not be able to restart the switch.

OK2 (Software Status). Blinking Green when the MPM has successfully loaded software to the Switching Modules. Blinking Amber when the MPM is in a transitional state, such as when it first boots up. If the **OK2** LED blinks Amber for an extended period of time (i.e., more than a minute), then you should reboot the switch.

Caution

Do not insert or remove any modules while the MPM **OK2** LED is blinking amber. If you do, file corruption may result and you will not be able to restart the switch.

Module Status LEDs



Label. This label will indicate the MPM version. It will read either **MPM** (original MPM), **MPM-II**, or **MPM-1G**.

PRI (Primary MPM). On Green when this MPM is the active, or controlling, MPM. It is also on Green when this is the only MPM installed in the switch.

SEC (Secondary MPM). On Green when this MPM is the secondary MPM in a redundant MPM configuration. As the secondary MPM, this module is in hot standby mode.

TEMP (Temperature). On Amber to warn that the internal switch temperature is approaching operating limits. Note that this LED comes on *before* the temperature limit is reached.

PS1 (Power Supply 1 Status). This dual-state LED is on Green when the switch is receiving the proper voltage from Power Supply 1. It is On amber when Power Supply 1 is on, but not supplying the correct amount of voltage to power the switch. The **PS1** LED is Off when the Power Supply 1 is not present.

PS2 (Power Supply 2 Status). This dual-state LED is on Green when the switch is receiving the proper voltage from Power Supply 2. It is On amber when Power Supply 2 is on, but not supplying the correct amount of voltage to power the switch. The **PS2** LED is Off when Power Supply 2 is not present.

Module Status LEDs

The Management Processor Module (MPM , MPM-II, and MPM-1G)

Warning Label. This label indicates that the module contains an optical transceiver (MPM-III-FL only).

OK1 (Hardware Status). This dual-state LED is on Green when the MPM-III has passed power-on hardware diagnostics successfully. On Amber when the hardware has failed diagnostic tests. If the **OK1** LED is alternating Green and Amber, then file system compaction is in progress.

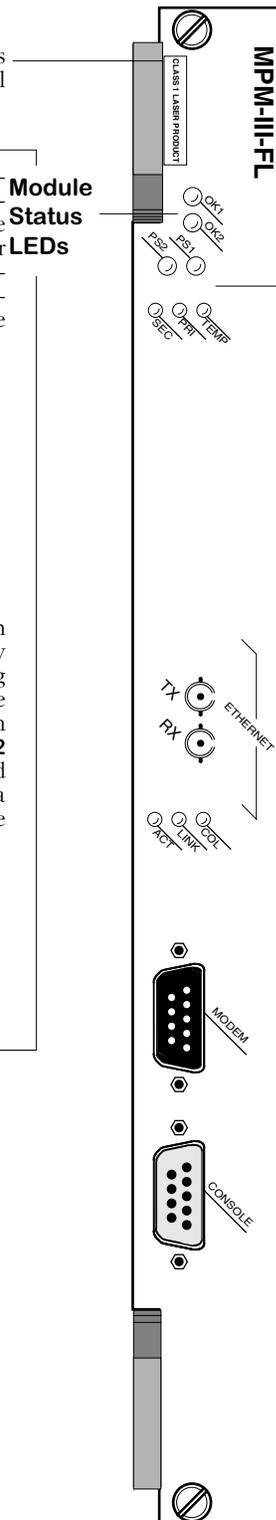
Caution

Do not power down the OmniSwitch or insert any modules while the **OK1** LED is alternating Green and Amber. If you do, file corruption may result and you will not be able to restart the switch.

OK2 (Software Status). Blinking Green when the MPM-III has successfully loaded software to the switching modules. Blinking Amber when the MPM-III is in a transitional state, such as when it first boots up. If the **OK2** LED blinks Amber for an extended period of time (i.e., more than a minute), then you should reboot the switch.

Caution

Do not insert or remove any modules while the MPM-III **OK2** LED is blinking Amber. If you do, file corruption may result and you will not be able to restart the switch.



Module Status LEDs

PS1 (Power Supply 1 Status). This dual-state LED is on Green when the switch is receiving the proper voltage from Power Supply 1. It is on Amber when Power Supply 1 is on, but not supplying the correct amount of voltage to power the switch, or is installed and turned off. The **PS1** LED is Off when the Power Supply 1 is not present.

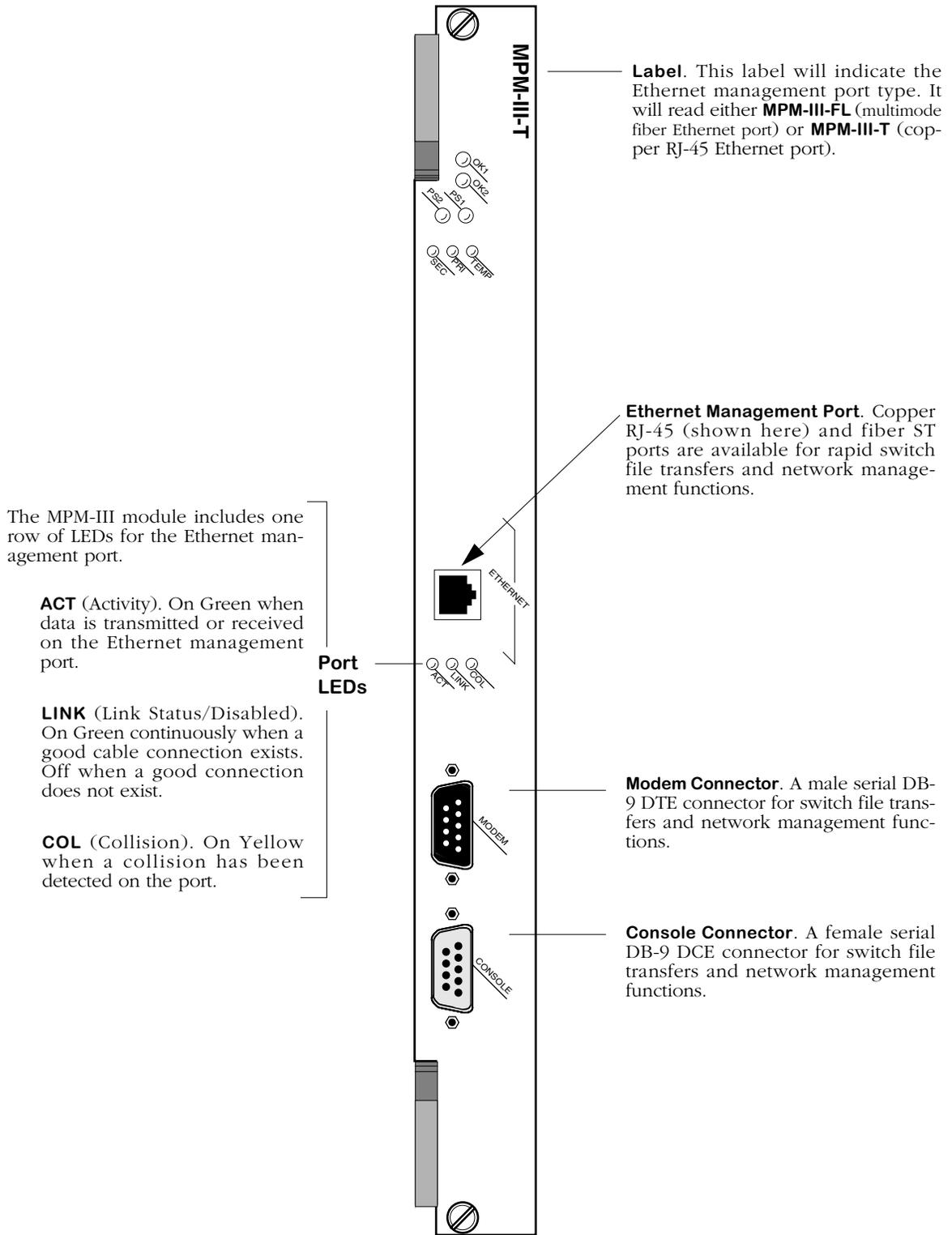
PS2 (Power Supply 2 Status). This dual-state LED is on Green when the OmniSwitch is receiving the proper voltage from Power Supply 2. It is on Amber when Power Supply 2 is on, but not supplying the correct amount of voltage to power the switch, or is installed and turned off. The **PS2** LED is Off when Power Supply 2 is not present.

TEMP (Temperature). On Yellow to warn that the internal switch temperature is approaching maximum operating limits. Note that this LED comes on *before* the temperature limit is reached.

PRI (Primary MPM-III). On Green when this MPM-III is the active, or controlling, MPM-III. It is also on Green when this is the only MPM-III installed in the switch.

SEC (Secondary MPM-III). On Green when this MPM-III is the secondary MPM-III in a redundant MPM-III configuration. As the secondary MPM-III, this module is in hot standby mode.

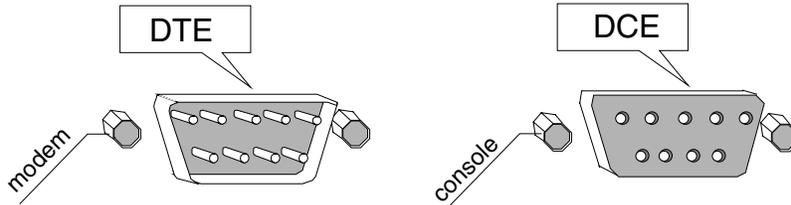
MPM-III Status LEDs



MPM-III Management Connectors

Serial and Ethernet Management Ports

You can gain access to switch management software through one of the two serial (RS-232C) ports on the MPM. The two console ports are configured with 9-pin “D” connectors (DB-9) per the IBM AT serial port specification. One port is male and the other is female.

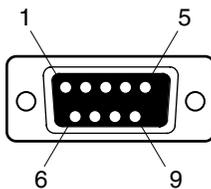


MPM Serial Ports

The male connector is a Data Terminal Equipment (DTE), which is typically connected to a modem. You can also connect directly from this port to a PC or terminal with a standard null-modem cable available in most computer equipment stores.

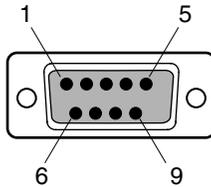
The female connector is a Data Communication Equipment (DCE), which is directly connected to a PC, terminal, or printer.

If the connecting device does not conform to the IBM AT serial port specification, then you may need to use a special cable or adapter. The pinouts for the console and modem ports are shown below and on the following page.



MPM Console Port Specifications		
Pin Number	Standard Signal Name	Direction
1	Not Used	
2	RD	From MPM
3	TD	To MPM
4,	Not Used	
5	GND	
6	Not Used	
7	Not Used	
8	Not Used	
9	Not Used	
Shell	Shield GND	

MPM Console Port



MPM Modem Port Specifications		
Pin Number	Standard Signal Name	Direction
1	Not Used	
2	RD	To MPM
3	TD	From MPM
4,	DTR	From MPM
5	GND	
6	DSR	To MPM
7	RTS	From MPM
8	CTS	To MPM
9	Not used	
Shell	Shield GND	

MPM Modem Port

Each Console port supports serial data rates of 1200, 9600, 19200, and 38400 bps. By default, each is set to 9600 bps. You can change this setting using the **ser** command that is described in Chapter 10, “Configuring Management Processor Modules.” You can connect or disconnect a serial cable to this port at any time without disrupting the switch.

◆ Note ◆

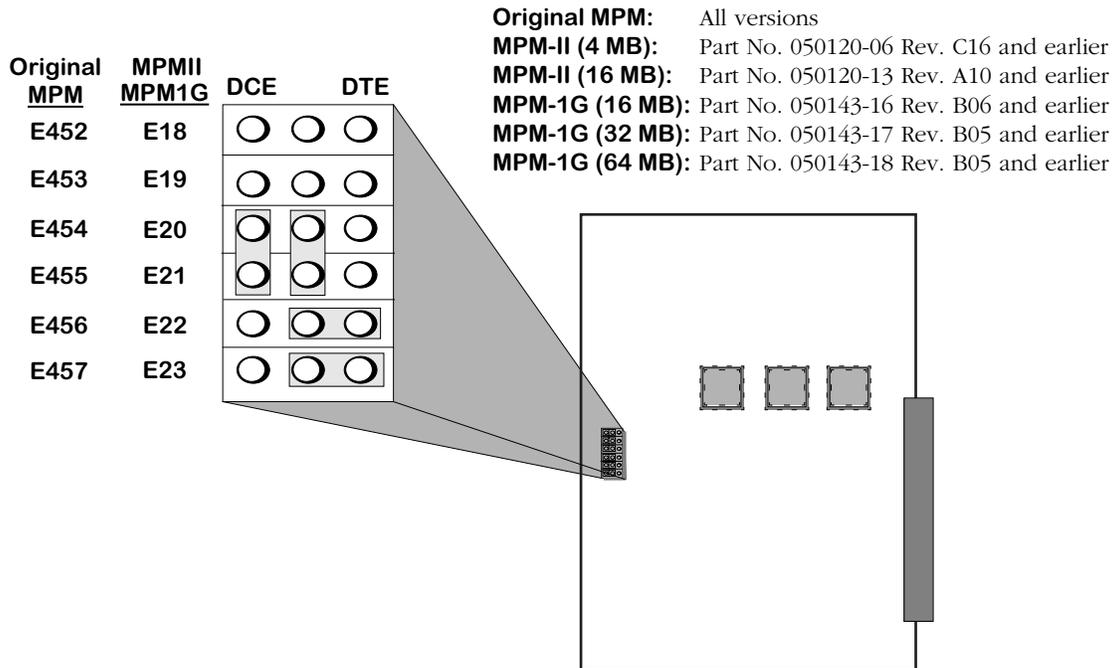
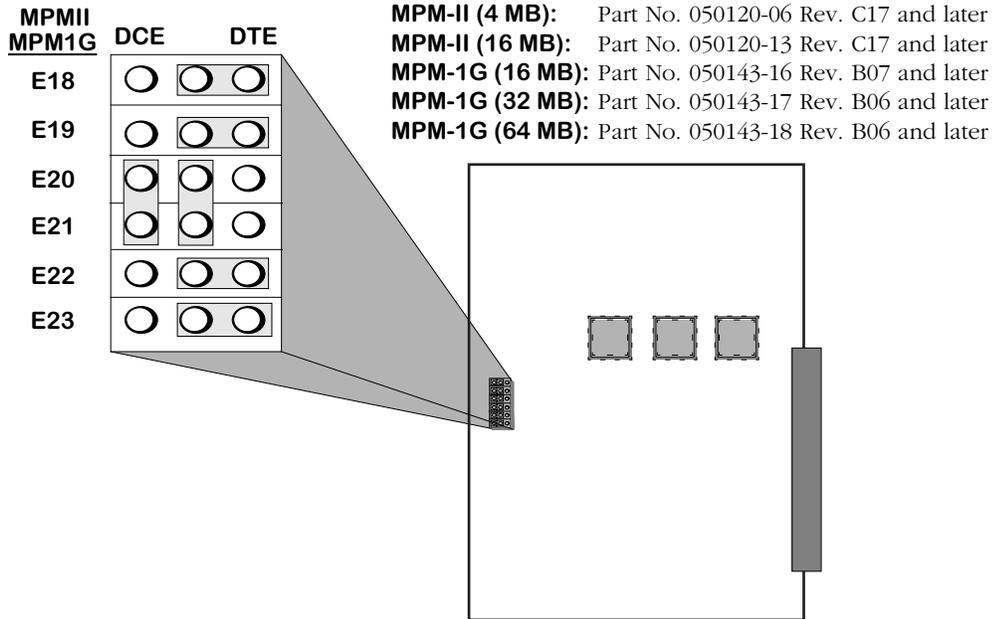
On the MPM-C and MPM-III, you must remove the default baud rate shunt (E1), which fixes the baud rate at 9600 bps, before you can change the baud rate. This shunt is located near the Ethernet management port.

Modem Port Jumpers

When using the modem port, jumpers must be set correctly. The MPM has one user-configurable jumper block. For the original MPM this block is labelled E452-457. For the MPM-II and MPM-1G this block is labelled E18-23. All remaining jumpers on the board are for internal use only. Do not alter any other jumper settings. By default, jumpers for the modem port are configured as shown in one of the figures below. Newer boards use the configuration in the top illustration and older boards use the configuration in the bottom illustration; refer to revision levels in the drawings for the correct configuration.

◆ Note ◆

The MPM-C and MPM-III are hard wired for DTE communications. You do not set jumpers on these modules.



Jumper settings on this block determine whether the modem port is configured for DCE or DTE operation. By default, they are configured for DTE operation, which is standard for a modem port. These jumpers also accommodate various loopback and null modem configurations.

Make sure the jumper block is set as shown in the figure on the following page before using the modem port. This default configuration allows you to connect the modem port to a modem using a straight-through cable, or to connect to a terminal, such as a PC, using a cross-over cable.

MPM-III Ethernet Management Port

The MPM-III also supports an out-of-band Ethernet port for high-speed uploads and switch management functions. With this port, you can access the OmniSwitch over a network via Telnet or FTP.

Before you can access an OmniSwitch through the Ethernet management port, you must assign an IP address to it first. You can use the Boot prompt to configure an IP address for the Ethernet management port or you can use the **ethernetc** command, which is described in Chapter 10, “Configuring Management Processor Modules.” After you have assigned an IP address to the Ethernet management port, you can use it to Telnet into the UI.

See Appendix A, “The Boot Line Prompt,” for documentation on configuring the Ethernet management port with the boot prompt.

See the table below for available Ethernet management port types.

MPM-III Model	Ethernet Management Port Type (Cable Type)	Max. Cable Distance
MPM-III-T	RJ-45 (UTP)	100 meters
MPM-III-FL	ST (Multimode fiber)	2 kilometers

◆ **Note** ◆

The Ethernet management port has a default IP address of 192.168.11.1, which can be used for initial connectivity.

Flash Memory and Switch Software

Flash memory on the MPM holds the OmniSwitch's executable images and configuration data for each image file. When a Switching Module comes online, the MPM downloads the appropriate image file for that module to that module's SIMM memory. Image files (those with the .img extension) contain executable code for different switching modules and software features. In addition, Programmable Gate Array (PGA) files (those with the .pga extension) are currently used with the Token Ring fiber module (TSM-F-6) for specialized configurations.

The following table lists all the files that may be present in MPM flash memory along with the module(s) or feature with which the file is used.

File Name	Modules/Function Used With
mpm.img	MPM, MPM-II, MPM-1G
mpm3.img	MPM-III
mpmc.img	MPM-C
mpm.cmd	MPM, MPM-II, and MPM-1G command file
mpm3.cmd	MPM-III command file
mpmc.cmd	MPM-C command file
mpm.cfg mpm.cnf	MPM, MPM-II, MPM-1G, MPM-III, MPM-C configuration files
asm.img	All ASM modules, all ASM2 modules, FCSM I (ASM functions), FCSM II (ASM functions)
asmc.img	MPM-C ("FCSM" functions)
asm_mpg.img	Multi-peer group PNNI operation for FCSM I and FCSM II and all CSMs if used with an MPM-1G or MPM-III
asmc_mpg.img	Multi-peer group PNNI operation for all CSMs if an MPM-C is installed.
asmce.img	Circuit emulation (ASM-CE, CSM-AB-CE)
asmcedrv.img	Circuit emulation (ASM-CE, CSM-AB-CE)

continued on next page...

File Name	Modules/Function Used With (Cont.)
cell.img	CSM-155, CSM-622, CSM-A25, FCSM, FCSM-II, MPM-C
cell_mpg.img	CSM-155, CSM-622, CSM-A25, FCSM, FCSM-II, MPM-C used with multi-peer group PNNI operation
diag.img	Diagnostics software (MPM, MPM-II, MPM-1G)
diag3.img	Diagnostics software (MPM-III)
diagc.img	Diagnostics software (MPM-C)
dmesm.img	Ethernet (Mammoth) port stress test software
dni.img	Diagnostics software for non Mammoth switching modules
ds3e3drv.img	ASM-DS3, ASM-E3, CSM-AB-DS3, CSM-AB-E3
e12.img	ESM-C-12, ESM-T-12, ESM-F-8
esm.img	ESM-C-8, ESM-U
fesm.img	ESM-100-C, ESM-100-C-FD, ESM-100-Fx-FD, ESM-100C-5, ESM-100CFx-5 (on HSM)
fesm2.img	ESM-100-C, ESM-100-C-FD, ESM-100-Fx-FD, ESM-100C-5, ESM-100CFx-5 (on HSM2)
fpx3.img	IP Fastpath and Firewall software (MPM-III)
frlmi.img	FRF/FR-LMI software
fwd.img	IP Firewall software (MPM-1G)
fwdx3.img	IP Fastpath and Firewall software (MPM-III)
fwk.img	IP Firewall software (MPM-1G)
gated.img	Advanced Routing software
ima.img	Inverse Multiplexing over ATM (IMA) software
ipcctrl.img	IP control software
ipms.img	IPMS software
isdn.img	WSM-BRI-SC

continued on next page...

File Name	Modules/Function Used With (Cont.)
lsm.img	LES/BUS software
lsm_mpg.img	LES/BUS software used with multi peer group PNNI operation
mesm.img	ESM-C-100-12, ESM-C-16, ESM-C-32, ESM-100FM-8, ESM-FM-16W, ESM-100C-32W, ESM-T-24W, GSM-FM/FS-2W
mpc.img	Multi-Protocol Over ATM (MPOA) software
mrd.img	Advanced Routing software
mtsm.img	TSM-CD-16W
ntp.img	Network Time protocol (NTP) software
pm_ctm.eexe	CSM-ABT-155F
qos.img	Quality of Service (QOS) software
rav.img	RADIUS authentication software
sonet.img	SONET error collection software
t1e1drv.img	WSM-FT1/E1, ASM-CE, CSM-AB-T1, CSM-AB-E1
text_cfg.img	Text-based configuration software
tsm.img	TSM-C-6, TSM-F-6, TSM-CD-6
tsm.pga	TSM-F-6
vrrp.img	VRRP software
web.img	HTTP browser client software
wsm.img	WSM-S (Frame Relay and PPP software)

Flash Memory Guidelines

The switch alters flash memory contents when a software command requests a configuration change, when a remote administrator downloads a new executable image, or when the switch fails and a record of the failure is written to flash memory. These operations require available space in flash memory.

In general the flash memory on the switch should always have at least 75000 bytes available at all times. In a switch with 4 MB of flash memory, for example, the images in flash should never exceed 3.45 MB. (You can view how much flash memory is available through the **ls** command.) This will allow enough room in flash for booting and configuration file expansions. If your flash memory exceeds this amount, then you need to delete some images from flash.

In addition, the flash file system has a limit of 32 files, including configuration, logging, and other files. When this 32-file limit is reached, configuration file expansions will cease and new files will not be able to be loaded. This file limit applies even if there is enough memory available in flash.

Not all image files in flash memory are required—only those that must be used with the switching modules in your OmniSwitch. You can remove any files that are not required for your OmniSwitch configuration by using the **rm** command. For example, if you did not have a Token Ring fiber module (TSM-F-6), then you could remove all PGA files (about 56K). If you do not have any Token Ring modules, you could remove the **tsm.img** file.

MPM Redundancy

In order to provide greater reliability, the OmniSwitch supports two MPMs in a primary/secondary redundant configuration. If the primary MPM fails, the secondary MPM takes over without any operator intervention.

When you have two MPMs in one chassis, they must be installed in slots 1 and 2, and only one can be active. MPMs will assume one of the following roles.

- Primary - The MPM that is currently active and processing commands. It is also the MPM that is communicating via Telnet, FTP, etc.
- Secondary - An MPM that is currently not the primary. It has sufficient software to communicate with the primary MPM. (For full redundancy, the secondary MPM should also have the same software version as the primary and its configuration should be in sync with the primary.) In this state, it is capable at any time of assuming the primary role.

The LEDs on each MPM reflect the same status with the exception that the primary's **PRI** LED is on whereas the secondary's **SEC** LED is on. Also, the secondary MPM's **OK2** LED will not flash amber during board transitions.

Change-Over Procedure

The secondary MPM continuously monitors the primary MPM. This monitoring serves two purposes: 1) to notify the secondary MPM that the primary is alive and processing, and 2) to update the configuration and thus keep the two MPMs in sync. If the secondary MPM detects that the primary is no longer operational, it can begin to take over as primary within a few seconds. When a secondary MPM becomes primary it resets all the other modules in the chassis and performs a primary MPM initialization.

There are four states for an MPM configuration. You can view the current MPM state through the **slot** command. These states are described in the table below. Note that for a primary/secondary configuration to be in a "redundant" state, the relationship between the two MPMs must meet the conditions shown in the table.

MPM State	Requirement for State
Redundant	Both MPMs are running the same version of software and the configurations are in sync.
Configuration Fallback	Both MPMs are running the same version of software but the configurations are different.
Software Fallback	The MPMs are running different versions of software, and their configurations may be the same or different.
None	There is only one MPM installed in the chassis.

The primary MPM has the ability to transfer files to and from the secondary MPM. In the condition where the secondary MPM has an older version of software, it is not desirable to update the configuration file of the secondary. It is therefore the default not to update the configuration file on the secondary if the secondary is running an earlier version of software. You can force the update using the appropriate command.

◆ **Note** ◆

Do *not* remove a primary MPM without performing a **renounce** command (described in Chapter 10, “Configuring Management Processor Modules”) first.

MPM Redundancy Commands

A set of commands exists to monitor the primary and secondary MPMs. These commands are covered in detail in Chapter 10, “Configuring Management Processor Modules.” Note that you can attach a terminal to both MPMs in a chassis; however, you will see a different set of commands depending on which is primary and which is secondary.

Hardware Routing Engines

Hardware Routine Engines (HREs) are submodules that plug into a socket on the MPM-III, MPM-1G, or MPM-II to significantly enhance routing performance. An MPM without an installed HRE routes packets between Groups and VLANs by sending them up the IP protocol stack for processing and then back down the protocol stack for transmission. This method can be slow and routing performance is limited by the available MPM CPU cycles.

With an installed HRE, routing is performed in hardware making it unnecessary for the MPM to process all packets and saving valuable CPU cycles. The HRE is free to perform routing at full VBUS speeds.

◆ Note ◆

If a switch contains only one HRE, then the MPM on which that HRE is a daughterboard *must* be installed in Slot 1 of the chassis. Slot 1 is optimized for high-performance routing.

There are three versions of the HRE:

- The original HRE for the MPM-II and MPM-1G
- The HRE-Plus for the MPM-II and MPM-1G
- The HRE-VX for the MPM-III.

Approximately 100 K 64-byte packets per second (bidirectional) can be processed by these HREs. The HRE versions are described in the subsections below.

◆ Note ◆

The MPM-C and original MPM do not support any version of the HRE.

MPM-II and MPM-1G HRE and HRE-Plus

There are two versions of the HRE for the MPM-II and MPM-1G: HRE and HRE-Plus. The HRE and HRE-Plus include a 2K CAM and 2048-entry header cache table. The HRE-Plus supports redundant configurations in which two MPMs, each with an HRE-Plus, are installed in a single chassis. The standard HRE does not support redundant configurations.

◆ Note ◆

You must have at least 16 MB of DRAM and 4 MB of flash memory on your MPM-II or MPM-1G to use an HRE or HRE-Plus.

MPM-III HRE-VX

The HRE-VX is an HRE designed specifically to run on an MPM-III. The HRE-VX includes 8 MB of SDRAM and 64 K of SRAM. The HRE-VX supports redundant configurations in which two MPM-IIIs, each with an HRE-VX are installed in a single chassis.

◆ Note ◆

Although the HRE-VX is similar in appearance to the Omni Switch/Router HRE-X, it *cannot* be used on any Omni Switch/Router module.

HRE-VX Router Registers versus Feature Limitations

The HRE-VX has three (3) registers that can be programmed with a MAC address and mask that allows it to recognize which destination MAC addresses it should act as a router for. IP Routing, Virtual Router Redundancy Protocol (VRRP), ATM Classical IP (CIP), and Channelized DS3 (i.e., M013) utilize at least one of these registers for their operation. This leads to a restriction of the combination of these features that can be supported on an MPM-III at any given time.

◆ Important Note ◆

In Release 4.4 and later, M013 is no longer supported on the OmniSwitch.

The HRE-VX registers are programmed on a first come, first served basis. Any attempt to program more than three registers fails. In current release, the order which these features program the HRE-VX is as follows:

1. ATM CIP
2. IP Routing (**Note:** If there is a second base MAC configured on the MPM-III, then it will also take a second register.)
3. M013
4. VRRP

For example, if a switch has two base MACs and a CIP group, then no other features can be configured. Any combination of the above features will work given the available HRE-VX registers. IP routing always takes one register (two in the dual base MAC case), leaving the other features to compete for the remaining two (one in the dual base MAC case). The other features attempt to program a register only if they are enabled.

◆ Note ◆

ATM CIP is limited to 128 end node route cache entries.

7 OmniSwitch Switching Modules

Switching modules are available for Ethernet, ATM, Token Ring and WAN interfaces. A variety of connector, speed, and signalling options is available for each network interface type.

Each switching module port is assigned a dedicated amount of bandwidth. For example, a 10 Mbps Ethernet module contains ports that each provide the full 10 Mbps of bandwidth. Likewise, an ATM OC-3 module contains ports that each provide the full 155 Mbps of bandwidth. Translations are provided for all interfaces contained in an OmniSwitch chassis. For example, if your OmniSwitch contained Ethernet, Token Ring, and ATM switching modules then all devices from all three network interfaces would be able to communicate through the OmniSwitch.

Since the OmniSwitch employs a distributed architecture, each switching module you add increases the processing and memory power of the entire switch. The Management Processor Module (MPM) handles central functions such as software storage, VLAN MAC learning, routing, and SNMP/User Interface management. But the MPM passes off much of the processing and memory functions to individual switching modules. Switching modules perform software filtering, translations between dissimilar network interfaces (e.g., Token Ring and Ethernet, Ethernet and ATM, ATM, and Frame Relay), and hardware-based switching.

Each switching module contains at least one RISC processor, RAM for software storage, ASICs for performing hardware-based switching, and content addressable memory (CAM) for storing the MAC addresses of source devices. A MAC address for a single source device only needs to be stored once in the CAM of the switching module that received the original frame. The memory on each switching module can be leveraged over an entire switch since all switching modules can communicate with each other. Each module's CAM is capable of storing up to 1,024 MAC addresses, and you can optionally add CAM to boost the total addresses stored by the module to 4,096.

All switching modules provide front panel LEDs that give a quick view of the status of the board, ports, connections and traffic. All switching modules may be hot swapped as long as you re-insert a module of the same type. The following lists the available switching modules:

High-Density and 10/100 Ethernet Modules (see "High-Density, 10/100, and Gigabit Ethernet Modules" on page 7-17)

- ESM-100C-12 Twelve auto-sensing 10/100 Mbps connections using RJ-45 ports.
- ESM-100FM-8 Eight 100BASE-FX connections using multimode fiber (SC) ports.
- ESM-C-16 Sixteen 10BASE-T connections using RJ-45 ports.
- ESM-C-32 Thirty-two 10BASE-T connections using RJ-45 ports.
- ESM-FM-16W Sixteen 10BASEFL connections using multimode fiber (ST) ports.
- ESM-100C-32W 32-port auto-sensing 10/100 Ethernet switching module
- ESM-T-24W Two Telco connectors supporting 24 UTP or STP ports.

Gigabit Ethernet Modules (see "GSM-F-2W Gigabit Ethernet Module" on page 7-33)

- GSM-FM/FS/FH-2W 2-port Gigabit Ethernet switching module.

ATM Access Modules (see "ATM Access Modules" on page 7-36)

- ASM-155Fx One or two port fiber single mode or multimode OC-3 module. **(Discontinued)**
- ASM2-155Fx One or two port fiber single mode or multimode OC-3 switching module. This is a higher performance version of the ASM-155Fx.
- ASM-155C One or two port UTP OC-3 module. **(Discontinued)**
- ASM2-622F One or two port fiber single mode or multimode OC-12 switching module. **(Discontinued)**
- ASM2-622FR Two or four port redundant fiber single mode or multimode OC-12 switching module. Each port pair includes a primary and backup port.
- ASM-DS3 One or two port DS-3 module. **(Discontinued)**
- ASM-E3 One or two port E3 module. **(Discontinued)**
- ASM-CE One ATM uplink port (OC-3, DS-3 or E3), two T1/E1 ports, and two serial ports supporting ATM circuit emulation. **(Discontinued)**
- ASM2-DS3 One- or two-port ATM DS3 uplink module.
- ASM2-E3 One- or two-port ATM E3 uplink module.

Token Ring Modules (see "Token Ring Modules" on page 7-74)

- TSM-C-6 Six-port UTP or STP Station connections. **(Discontinued)**
- TSM-F-6 Six-port fiber that supports Station, Lobe, Ring Out, Ring In/Ring Out connections.
- TSM-CD-6 Six-port UTP or STP that supports Station or Lobe connections. **(Discontinued)**
- TSM-CD-16W 16-port Token Ring (Lobe and Station) switching module.

WAN Modules (These modules are described in detail in Chapter 48, "Managing WAN Switching Modules.")

- WSM-S Two, four, or eight serial ports that support the frame relay or PPP protocol.
- WSM-FT1/E1 One or two T1/E1 ports and one or two serial ports that support the frame relay or PPP protocol.
- WSM-BRI One UPS (Universal Serial Port) and one ISDN-BRI port that support Frame Relay or PPP.

Cell Switching Modules (These modules are described in detail in Chapter 40, "Cell Switching Modules (CSMs)")

- FCSM I Frame-to-Cell Switching Module.
- FCSM II The OC-12c/STM-4c version of the original FCSM.
- CSM-155F Eight-port 155 Mbps cell switching module.
- CSM-622 Two-port 622 Mbps cell switching module.
- CSM-155C Eight-port 155 Mbps cell switching module.
- CSM-A25-12 Twelve-port ATM 25 Mbps cell switching module.
- CSM-A25-24 Twenty-four port ATM 25 Mbps cell switching module.
- CSM-U Universal cell switching module with three adapter board positions. Adapter boards include support for OC-3 fiber and copper ports, T1/E1 ports, DS3/E3 ports, T1/E1 circuit emulation ports, Stratum-3 hardware clocking, and Inverse Multiplexing over ATM (IMA).
- CSM-U+ Advanced version of the CSM-U with 15-bit VPI/VCI support.

Original Ethernet (10 Mbps) Modules (see "Original 10 Mbps Ethernet Modules" on page 7-88)

- ESM-C-12 Twelve 10BASE-T connections using RJ-45 ports. **(Discontinued)**
- ESM-C-8 Eight 10BASE-T connections using RJ-45 ports. **(Discontinued)**
- ESM-F-8 Eight 10BASE-FL connections using fiber (ST) ports. **(Discontinued)**
- ESM-T-12 One Telco connector supporting 12 UTP or STP ports. **(Discontinued)**
- ESM-U Universal Ethernet module supporting six connections that may be a combination of AUI (full- or half-duplex), RJ-45, fiber, or BNC ports.

Original Fast Ethernet (100 Mbps) Modules (see "Original Fast Ethernet (100 Mbps) Modules (Discontinued)" on page 7-100)

- ESM-100C Four or eight 100BASE-Tx connections using RJ-45 ports. **(Discontinued)**
- ESM-100C-FD One or two full-duplex 100BASE-Tx connections using RJ-45 ports. **(Discontinued)**
- ESM-100Fx-FD One or two full-duplex 100BASE-Fx fiber connections (single mode or multimode) using SC connectors. **(Discontinued)**
- ESM-100C-5 Five 100BASE-Tx connections using RJ-45 ports. One of the five ports supports full-duplex operation. **(Discontinued)**
- ESM-100CFx-5 One fiber 100BASE-Fx connection and four 100Base-Tx connections. The fiber port supports full-duplex operation and can be configured with single mode or multimode connectors. **(Discontinued)**

Required Image Files

See the table on the following page for the required images files for the MPM, MPM-III, and frame-based switching modules. (See Chapter 40, “Cell Switching Modules (CSMs),” for information on the MPM-C, FCSM-I, FCSM-II, and CSM modules.) You *must* load the image file (or files) listed for the corresponding module or it will not run.

◆ **Note** ◆

On CSM modules, the **sonet.img** file is a required image file. On ATM access modules (ASM and ASM2 modules), you must load the **sonet.img** file to run SONET error collection. However, this image file is not required to run these modules.

Required Image Files

Module	Image File(s)
MPM-II/MPM-1G	mpm.img
MPM-III	mpm3.img, fpx3.img
ASM-155C	asm.img
ASM-155F	asm.img
ASM-DS3	asm.img, ds3e3drv.img
ASM-E3	asm.img, ds3e3drv.img
ASM-CE-155F	asm.img, asmce.img, asmcedrv.img
ASM-CE-DS3-2S2T	asm.img, asmce.img, asmcedrv.img, ds3e3drv.img
ASM-CE-E3-2S2T	asm.img, asmce.img, asmcedrv.img, ds3e3drv.img
ASM2-155F	asm.img
ASM2-155RF	asm.img
ASM2-622F	asm.img
ASM2-622RF	asm.img
ASM2-E3	asm.img, ds3e3drv.img
ASM2-DS3	asm.img, ds3e3drv.img
ASM2-E3	asm.img, ds3e3drv.img

continued on next page...

Required Image Files (continued)

Module	Image File(s)
ESM-C-8	e12.img
ESM-C-12	e12.img
ESM-F-8	e12.img
ESM-T-12	e12.img
ESM-U-6	esm.img
ESM-100C (HSM)	fesm.img
ESM-100C (HSM2)	fesm2.img
ESM-100C-FD	esm.img
ESM-100FM-FD	esm.img
ESM-100FS-FD	esm.img
ESM-100C-12	mesm.img
ESM-C-16	mesm.img
ESM-C-32	mesm.img
ESM-100FM-8	mesm.img
ESM-FM-16W	mesm.img
ESM-T-24W	mesm.img
ESM-100C-32W	mesm.img
GSM-FM-2W	mesm.img
GSM-FS-2W	mesm.img
GSM-FH-2W	mesm.img
TSM-C-6	tsm.img
TSM-F-6	tsm.img, tsm.pga
TSM-CD-6	tsm.img
TSM-CD-16W	mtsm.img

continued on next page...

Required Image Files (continued)

Module	Description
WSM	wsm.img
WSM-BRI	wsm.img, isdn.img
WSM-FT1	wsm.img, t1e1drv.img
WSM-FE1	wsm.img, t1e1drv.img

Installing a Switching Module

All switching modules can be inserted and removed from the switch chassis while power is on or off without disrupting the other modules. *A standard screwdriver is required for installing and removing switching modules.* You can also hot swap modules of the same type while the switch is active.

Switching modules may be installed in any slot. If the MPM is installed in Slot 2, you can install a Switching Module in Slot 1 or any other slot but 2. If it is installed in Slot 1, a Switching Module can be installed in Slot 2 or any other slot but 1. In a setup with redundant MPM modules, Slots 1 and 2 are reserved for the MPMs. Additional modules can be installed in any available slot. (Omni-5 slots are numbered 1 to 5 starting from the topmost slot. Omni-9 slots are numbered 1 to 9 starting from the left.)

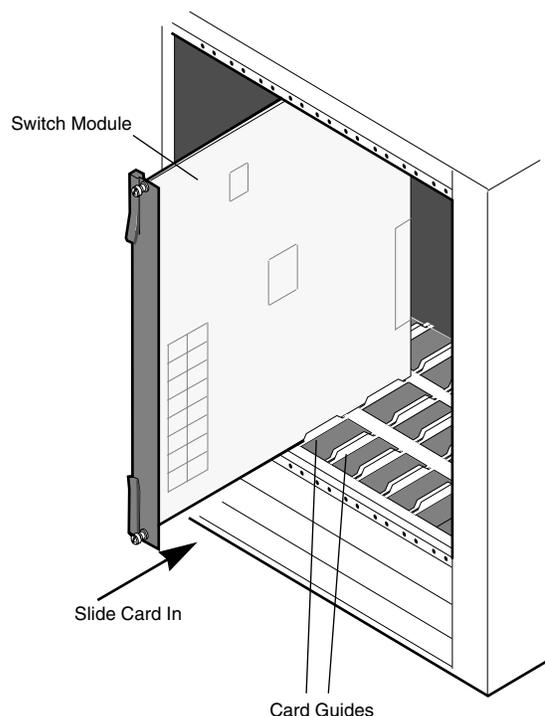
◆ Anti-Static Warning ◆

Before handling a switching module, free your hands of static by wearing a grounding strip, or by grounding yourself properly. Static discharge can damage the components on the switching module.

To insert a switching module follow these instructions:

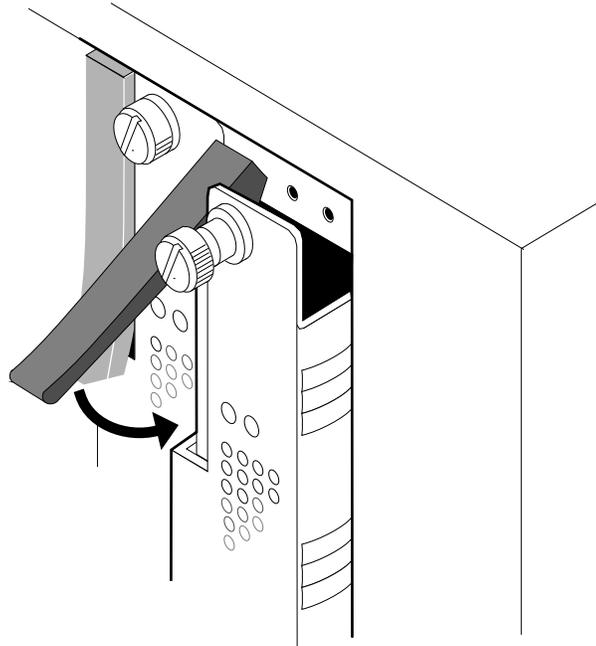
1. Holding the module firmly in both hands, carefully slide it into the card guide. The front panel connectors and LEDs should face outward. In a 9-slot OmniSwitch, the component side of the board should face right (toward the power supply). In a 5-slot OmniSwitch, the component side should face up.

The module should slide in easily. A large amount of force is not necessary and should not be used. If any resistance is encountered, check to be sure that the module is aligned properly in the card guide.

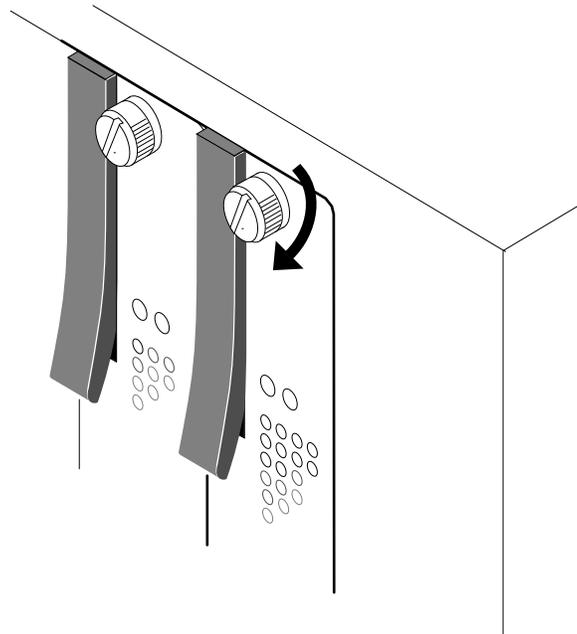


Installing a Switching Module

2. Once the module is in the slot, close the two card ejectors (one on each end of the module) by pressing them in toward the module until they snap into place.



3. Use a standard screwdriver to tighten the two screw fasteners to secure the module inside the chassis. The screws should be tight enough such that a screwdriver would be necessary to loosen the screws.



Removing a Switching Module

To remove a switching module, follow the instructions below. If you are “hot swapping” the modules (i.e., removing and inserting while power is on), see *Hot Swapping a Switching Module* on page 7-10.

◆ Anti-Static Warning ◆

Before handling a switching module, free your hands of static by wearing a grounding strip, or by grounding yourself properly. Static discharge can damage the components on your switching module.

1. Loosen the screw fasteners at the top and bottom of the switching module using a standard screwdriver.
2. Gently unlock the two card ejectors by pulling them out away from the module.
3. With both hands, carefully pull the module free of the chassis enclosure.

Hot Swapping a Switching Module

You may remove and insert switching modules while the switch is running. This technique is referred to as “hot swapping.” When you hot swap, you must replace the module with the same module type as the one you removed. For example, if you remove an ASM switching module you must replace it with another ASM switching module.

◆ **Note** ◆

You *cannot* hot swap a module into a previously empty slot. To use an empty slot, you *must* power down your chassis.

Perform the following steps to safely hot swap a switching module. (You cannot hot swap a primary MPM module.) Since this procedure could possibly disrupt the network, it is best to hot swap during network down times.

1. At the system prompt, enter

swap on <minutes>

where **minutes** is the number of minutes you want the switch to be in swap mode (the default is 5 minutes). A message similar to the following will be displayed.

Swap is ON for 5 minutes

The swap mode *must* be enabled (**ON**) to insert a switching module. If not, the system may halt or restart. (See Chapter 10, “Configuring Management Processor Modules,” for more information on the **swap** command.)

If you have an ATM access module (e.g., ASM, ASM2, or ASX) or a CSM module, proceed to step 3. Otherwise, proceed to step 2.

◆ **Caution** ◆

Modules can only be reset and hot-swapped when the MPM’s **OK2** light is in its normal flashing green state.

2. Enter **reset**, followed by the slot number of the switching module you want to hot swap, then followed by the word **disable**. (See Chapter 58, “Running Hardware Diagnostics,” for more information on the **reset** command.) For example, if you want to hot swap the switching module in slot 4, you would enter

reset 4 disable

at the system prompt. Next, the switch will prompt you to confirm the reset. The following is an example of the display for an ESM Mammoth module. The display for other types of switching modules will be similar.

**Resetting slot of type F-Ether/M may crash system
Attempt reset anyway {Y/N}? (N) :**

Press **y** and then press **<Enter>**. If the switching module is in slot 4, a message similar to the following will be displayed.

resetting slot 4 to disable

3. The MPM’s **OK2** LED will flash amber 1 or 2 times, then return to normal flashing green. The switching module’s **OK1** LED will turn amber and the **OK2** LED will *not* be illuminated. Remove all cables attached to ports on the switching module that you are going to swap out.

4. Carefully remove the switching module from the chassis and put it in a safe place. (See *Removing a Switching Module* on page 7-9 for instructions on removing a switching module.) The MPM's **OK2** LED will flash amber 1 or 2 times, then return to normal flashing green. In addition, the swap time will reset to its original value. (For example, if you set the swap time to 15 minutes in step 1, you will have 15 minutes again, regardless of how much time has elapsed.)

◆ **Warning** ◆

Removing or inserting the switching module while the MPM's **OK2** LED is flashing amber can cause the system to reset.

5. Carefully insert the new switching module into the chassis. (See *Installing a Switching Module* on page 7-7 for instructions on inserting a switching module.)

◆ **Caution** ◆

When re-installing a module during a hot swap, it must make a proper connection to the switch backplane. The connection is made when you close the card ejectors. Always close the card ejectors firmly and briskly, without hesitation. Closing them too slowly can cause the switch to halt or restart.

The MPM's **OK2** LED will flash amber 1 or 2 times, then return to normal flashing green. If, after hot-swapping modules, the MPM's **OK2** LED continues to flash amber for more than about 8 seconds, it means that the switch needs to be reset.

The swap time will again reset to its original value.

6. Re-insert the cables that were removed in step 3 into the new switching module. If you have an ATM access module (e.g., ASM, ASM2, or ASX) or a CSM module, proceed to step 8. Otherwise, proceed to step 7.
7. Enter **reset** followed by the slot number for the new switching module. For example, if the new switching module is in slot 4, you would enter

reset 4

at the system prompt. Next, the switch will prompt you to confirm the reset. The following is an example of the display for an ESM Mammoth module. The display for other types of switching modules will be similar.

**Resetting slot of type F-Ether/M may crash system
Attempt reset anyway {Y/N}? (N) :**

Press **y** and then press **<Enter>**. If the switching module is in slot 4, a message similar to the following will be displayed.

resetting slot 4 to enable

8. The MPM's **OK2** LED will flash amber 1 or 2 times, then return to normal flashing green. The switching module's **OK1** LED will turn from amber to solid green and the **OK2** LED will be blinking green. If the **OK1** LED on the switching module is amber, then the hardware has failed diagnostics or the corresponding image file for the module is not in flash memory. If the **OK2** LED on the switching module is solid amber, then the module failed to download software from the MPM.

9. If the hot swapping mode has not timed out, enter

swap off

at the system prompt. Something like the following will then be displayed.

```
Swap is OFF, timeout is 5 minutes
usage swap { ON [ minutes ] | OFF [ minutes ] }
```

◆ **Note** ◆

Auto-activated LAN Emulation Clients (LECs) will not re-initialize after hot swapping an OmniSwitch ASM or ASM2 module or after hot swapping an Omni Switch/Router ASX module. Reboot the switch to re-initialize the auto-activated LECs.

Diagnostic Tests

All switching modules are subjected to extensive power-on diagnostics during the Power-On Self-Test cycle (POST). These diagnostics are designed to be as extensive as possible without causing disruption to external networks or requiring special test connections. While the diagnostics are running, the MPM **OK2** LED will be flashing green. LEDs on the switching module can provide information on the success or failure of these tests. See *Module LEDs* on page 7-16 for information on these LEDs. Also refer to Chapter 57, “Troubleshooting,” for information on error conditions reflected in the LED displays.

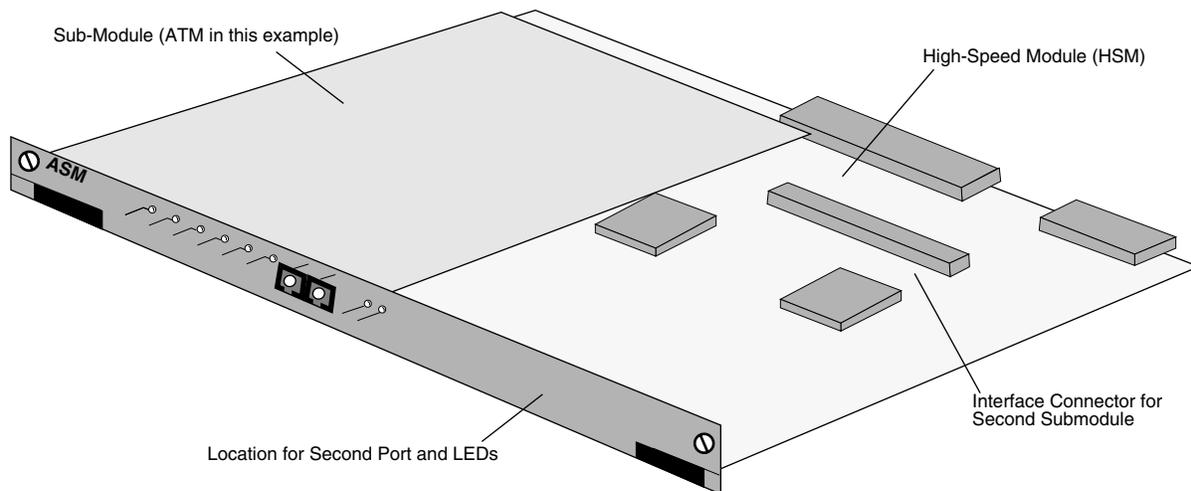
More extensive diagnostic tests are available for off-line testing of switching modules. See Chapter 58, “Running Hardware Diagnostics,” for further information.

High-Speed Module (HSM)

Many switching modules that operate at speeds in excess of 10 Mbps are actually submodules that attach to a High-Speed Module (HSM). These switching modules include ATM, Frame Relay modules, some 100 Mbps Ethernet and most Token Ring modules. The HSM provides the base memory and processing power for these high throughput switching modules.

The HSM contains RISC processors, RAM for holding software image files, ASICs for performing switching, and Content Addressable Memory (CAM) for storing MAC addresses. The HSM comes in three versions—HSM, HSM2, and HSM3.

You have the option of factory installing either one or two submodules on an HSM. Two submodules double the port count for a particular module. For example, a one-port ATM module contains one submodule attached to an HSM, and a two-port ATM module has two submodules attached to an HSM. The illustration below shows an HSM with an attached submodule.



The HSM and Attached Submodule

You plug cable directly into a submodule, but it is the HSM module that connects to the switch backplane.

Content Addressable Memory (CAM)

Each switching module is shipped with 1K, 2K, or 4K of Content Addressable Memory (CAM). CAM is used to claim frames from the VBUS for forwarding to the ports on that switching module. Modules with 1K of CAM can store 1,024 addresses, modules with 2K of CAM can store 2,048 addresses, and modules with 4K of CAM can store 4,096 addresses.

CAM is located directly on some Ethernet module boards; it is located on the HSM boards for ATM, Token Ring, and Frame Relay modules. Two CAM sockets are available for all 10 Mbps Ethernet modules and all HSM modules.

In a configuration where all switching modules use the standard 1K of CAM, the OmniSwitch can actively manage up to 8,192 MAC addresses in a 9-slot chassis, and up to 4,096 addresses in a 5-slot chassis.

Because the CAM is actually a cache of most recently observed addresses and not all of the addresses in the network, even a 1K CAM can often support networks with many more than 1,024 stations. However, a module with only 1K of CAM can cause problems in networks with large shared media backbones in which more than 1,024 addresses are simultaneously active.

The 2K and 4K CAM options address this limitation by allowing up to 2,048 or 4,096 addresses per switching module. This option provides a larger CAM for address recognition logic, which makes the OmniSwitch more robust in networks with large shared media backbones. This option is supported on most switching modules.

Note

ESM-U-6 modules must be at least Rev. F1 to support the 2K CAM option. Older versions of the board do not contain an extra CAM socket.

The switch software recognizes if more than 1K of CAM is installed on a switching module. The switch can support up to 16K of CAM among all switching modules. If you have more than 16K of CAM installed on all switching modules in your chassis, then you can view each module's CAM usage through the **camstat** command. In such configurations, you may also need to configure each slot's CAM usage through the **camcfg** command (see the section on **camcfg** in Chapter 13, "Configuring Switch-Wide Parameters," for further information). If you have 16K CAM or less, then no special configuration is required.

The 2K or 4K CAM option is not normally required unless a port on that module is plugged into a backbone, such as an ATM backbone, in which a large number of addresses are simultaneously active. Each network is different and the traffic patterns should be observed to best decide when this is used. Another alternative to greatly improve both CAM utilization and network performance is to split the backbone into multiple networks and switch between them.

Source Learning and CAM Capacity

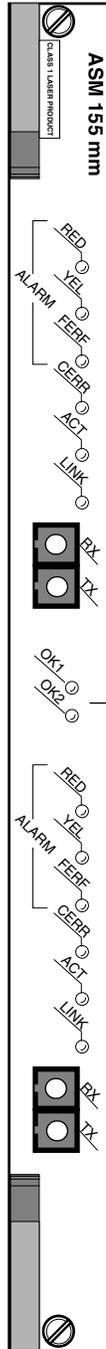
Learning of source addresses is affected by the amount of space available in CAM. When CAM capacity is less than 85 percent (870 or fewer entries in a 1K CAM), normal source learning occurs. When CAM capacity is 85 percent or more (870 or more entries in 1K CAM), the source addresses for broadcast frames are not learned; non-broadcast frames are still learned. At the 95 percent level (972 or more entries in 1K CAM), the CAM will not learn source addresses for frames sent to unknown destinations; frames destined to a known address are still learned.

Note

Learning returns to normal once the CAM returns to below the 85 percent capacity.

Module LEDs

LEDs on switching modules vary by the network interface type and by a module's application. However, two LEDs are common to all switching modules. These LEDs, **OK1** and **OK2**, provide information on the hardware and software status, respectively, of the module. These two LEDs are normally located in the middle of the module, as shown below. However, on 10 Mbps Ethernet modules they are located at the top or the bottom of the module.



Module LEDs

OK1 (Hardware Status). On Green when the module has passed diagnostic tests successfully. On Amber when the hardware has failed diagnostics or if the corresponding image file for the module is not in flash memory.

OK2 (Software Status). Blinking Green when the module software was downloaded successfully and the module is communicating with the MPM. Blinking Amber when the module is in a transitional state. On solid Amber if the module failed to download software from the MPM.

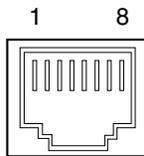
High-Density, 10/100, and Gigabit Ethernet Modules

The following Ethernet modules take advantage of new Ethernet/Fast Ethernet ASIC technology. Software commands are available to view and configure Ethernet ports on all modules. The modules are as follows:

- ESM-100C-12 Twelve auto-sensing 10/100 Mbps connections using RJ-45 ports.
- ESM-100FM-8 Eight 100BASE-FX connections using multimode fiber (SC) ports.
- ESM-C-16 Sixteen 10BASE-T connections using RJ-45 ports.
- ESM-C-32 Thirty-two 10BASE-T connections using RJ-45 ports.
- ESM-FM-16W Sixteen 10BASE-FL connections using fiber (ST) ports.
- ESM-100C-32W Thirty-two auto-sensing 10/100 Mbps connections using RJ-45 ports.
- ESM-T-24W Two Telco connectors supporting twenty-four (24) 10 Mbps ports.
- GSM-FM/FS/FH-2W Two (2) Gigabit Ethernet connections using fiber (SC) connectors.

Ethernet Pinouts

The figure and table below illustrate the pinouts for an Ethernet RJ-45 port.



Ethernet RJ-45 Specifications	
Pin Number	Standard Signal Name
1	RD +
2	RD -
3	TD +
4,	Not Used
5	Not Used
6	TD -
7	Not Used
8	Not Used

ESM-100C-12

The ESM-100C-12 Ethernet switching module contains 12 ports that each support a fully switched 10 or 100 Mbps connection in full- or half-duplex mode. Each port can auto-sense the connection speed and automatically switch at that speed. You configure whether you want to use the auto-sensing functionality through the **10/100cfg** command. By default, each port is configured to operate in half-duplex, auto-sensing mode. You can configure full-duplex mode on each port through **10/100cfg**. Auto-sensing may be disabled to allow you to manually configure ports through the **10/100cfg** command. An additional software command, **10/100vc**, allows you to view the current line speed and link mode of each port connection. The **10/100cfg** and **10/100vc** commands are described in Chapter 19, “Managing Ethernet Modules.”

The 12 RJ-45 ports may connect to unshielded twisted pair (UTP) cable. Each port may connect to a single high-speed device or a hub serving multiple devices. In a fully populated 5-slot switch, you could have up to 48 switched Ethernet connections, and in a fully populated 9-slot switch you could have up to 96 switched connections

The ESM-100C-12 is best used in networks with a mix of 10 Mbps and 100 Mbps Ethernet devices that are transitioning to higher speed connections. As more 100 Mbps connections are added, the ESM-100C-12 automatically senses the higher speed and switches at that speed.

ESM-100C-12 Technical Specifications	
Number of ports	12
Connector Type	RJ-45
Standards Supported	IEEE 802.3; IAB RFCs 826, 894
Data Rate	10 or 100 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024 or 2,048 with ESM-100C-12-2C
Connections Supported	10/100BASE-T hub or device
Cable Supported	10BASE-T Unshielded twisted-pair (UTP) 100BASE-T Unshielded twisted-pair: Category 5, EIA/TIA 568 Shielded twisted-pair Category 5, 100 ohm
Cable Distance	100 m

This ESM module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number.

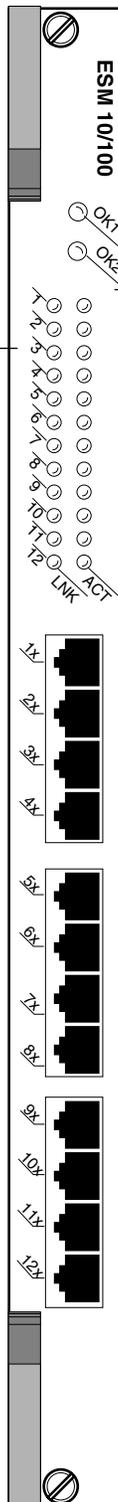
LNK (Link). On Green continuously when a good cable connection exists to an attached device. Off when a good connection does not exist. Blinks Green slowly when the port has been disabled.

ACT (Activity). On Green when data is transmitted or received on the corresponding port.

Port LEDs

Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.



Ethernet 12-Port 10/100 Module

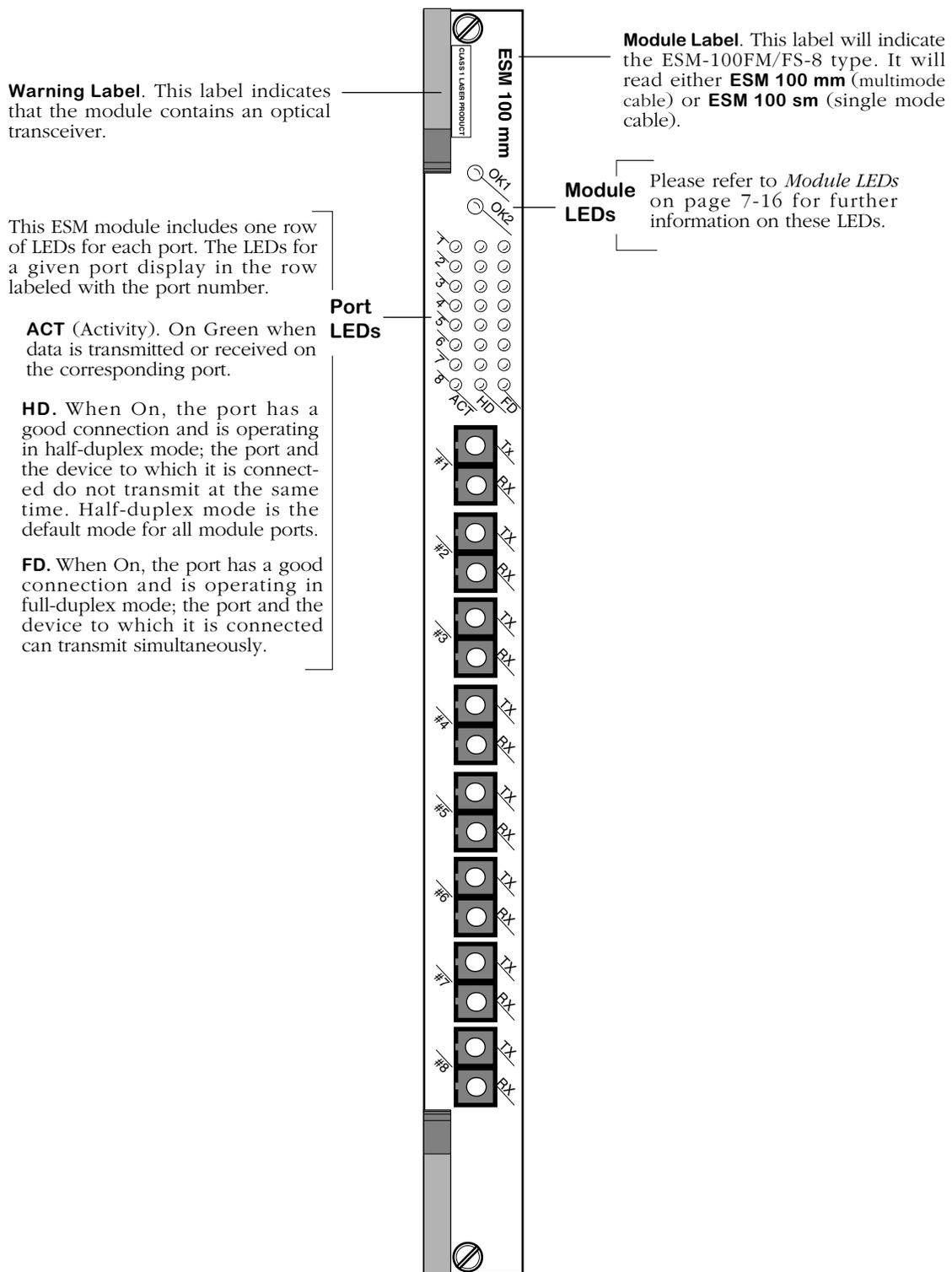
ESM-100FM/FS-8

The ESM-100FM/FS-8 Ethernet switching module contains eight fiber SC connectors that support eight fully switched 100Base-Fx ports. The ESM-100FM-8 uses multimode fiber ports that are color coded black.

All ports support either half- or full-duplex operation. You configure whether you want a half- or full-duplex connection through the **10/100cfg** command. By default, ESM-100FM-8 ports are configured for half-duplex connections.

The ESM-100FM-8 is best used as a backbone connection in networks where Fast Ethernet is used as the backbone media. In addition to its use as a backbone connection, each 100BaseFx port may connect to a single high-traffic device, such as a mail or file server.

ESM-100FM/FS-8 Technical Specifications	
Number of ports	Eight
Connector Type	SC
Standards Supported	IEEE 100Base-Fx
Data Rate	100 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	4,096
Connections Supported	100Base-Fx device, hub (half-duplex mode only) or bridge port
Cable Supported	Multimode: 62.5 micron multimode fiber Single mode (intermediate reach): single mode fiber
Optical output power	Multimode: -19 to -14 dBm Single mode: -20 to -14 dBm
Optical receiver sensitivity	Multimode: -31 to -14 dBm Single mode: -31 to -14 dBm
Cable Distance	Multimode (12dB) fiber: approximately 4.5 km Single mode: 16.5 km



Ethernet 8-Port 100BASE-FX Module

ESM-C-16

The ESM-C-16 Ethernet switching module contains 16 10BASE-T ports. Each port connection supports one switched Ethernet segment at the full 10 Mbps of bandwidth. The 16 RJ-45 ports may connect to unshielded twisted pair (UTP) or shielded twisted pair (STP) cable. Each port may connect to a single device, such as a workstation or server, or a hub serving multiple devices.

All ports support either half- or full-duplex operation. You configure whether you want a half- or full-duplex connection through the **10/100cfg** command. By default, ESM-C-16 ports are configured for half-duplex connections.

Module ports are divided into two banks of eight (8) ports. Ports are numbered from 1 to 8 within each bank. The banks are labelled **A** and **B**. This grouping simplifies the display of LEDs, which are organized as a matrix. You can find the LED for a particular port by matching the port number with the bank letter within the LED matrix display (see illustration on the next page).

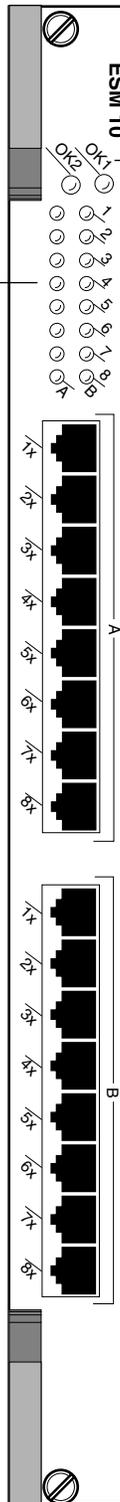
Using ESM-C-16 modules in a fully populated Omni-5wx, you could have up to 64 switched Ethernet connections, and in a fully populated Omni-9wx you could have up to 128 switched connections.

ESM-C-16 Technical Specifications	
Number of ports	16
Connector Type	RJ-45
Standards Supported	IEEE 802.3
Data Rate	10 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024
Connections Supported	10BASE-T hub (half-duplex only) or device
Cable Supported	Unshielded twisted-pair (UTP)—100 ohm Shielded twisted-pair (STP)—100 ohm
Cable Distance	100 m

Each LED corresponds to a port on the module. Rows correspond to one of the two banks of ports (A or B). Columns refer to port numbers within each bank.

Port LEDs

When an LED is on Green continuously, a good cable connection exists to a 10BASE-T device. The LED will flash when traffic is transmitted or received on the port.



Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

Ethernet 16-Port 10BASE-T Module

ESM-C-32W

The ESM-C-32W Ethernet switching module contains 32 10BASE-T ports. Each port connection supports one switched Ethernet segment at the full 10 Mbps of bandwidth. The 32 RJ-45 ports may connect to unshielded twisted pair (UTP) or shielded twisted pair (STP) cable. Each port may connect to a single device, such as a workstation or server, or a hub serving multiple devices.

All ports support either half- or full-duplex operation. You configure whether you want a half- or full-duplex connection through the **10/100cfg** command. By default, ESM-C-32W ports are configured for half-duplex connections.

Module ports are divided into four (4) banks of eight (8) ports. Ports are numbered from 1 to 8 within each of the four banks. The four banks are labelled **A**, **B**, **C**, and **D**. This grouping simplifies the display of LEDs, which are organized as a matrix. You can find the LED for a particular port by matching the port number with the bank letter within the LED matrix display (see illustration on the next page).

Because the ESM-C-32W is a wide-style module, it is only supported in a wide chassis (i.e., Omni-3wx, Omni-5wx or Omni-9wx). Using ESM-C-32 modules in a fully populated Omni-3wx, you could have up to 64 switched connections; in an Omni-5wx, you could have up to 128 switched Ethernet connections; and in a fully populated Omni-9wx, you could have up to 254 switched connections.

ESM-C-32W Technical Specifications	
Number of ports	32
Connector Type	RJ-45
Standards Supported	IEEE 802.3
Data Rate	10 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024
Connections Supported	10BASE-T hub or device
Cable Supported	Unshielded twisted-pair (UTP)—100 ohm Shielded twisted-pair (STP)—100 ohm
Cable Distance	100 m

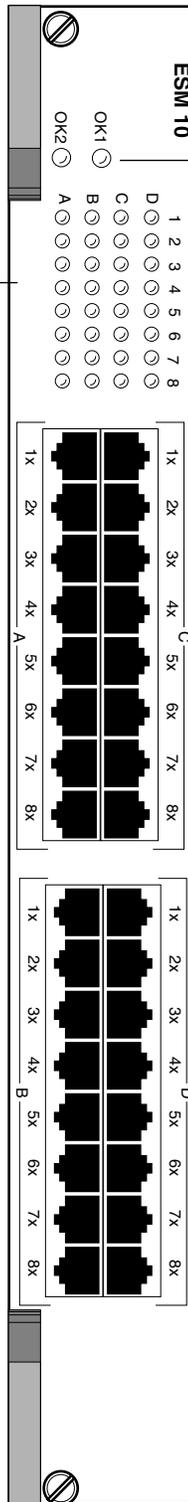
Each LED corresponds to a port on the module. Rows correspond to one of the four banks of ports (A, B, C, or D). Columns refer to port numbers within each bank.

When an LED is on Green continuously, a good cable connection exists to a 10BASE-T device. The LED will flash when traffic is transmitted or received on the port.

Port LEDs

Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.



Ethernet 32-Port 10BASE-T Wide Module

ESM-FM-16W

The ESM-FM-16W Ethernet switching module contains 16 10BASE-FL ports. Each port connection supports one switched Ethernet segment at the full 10 Mbps of bandwidth. The 16 dual ST connector ports connect to multimode fiber optic cable. Each port may connect to a single high-traffic device, such as a mail or file server, or a hub serving multiple devices.

Because the ESM-FM-16W is a wide-style module, it is only supported in a wide chassis (i.e., Omni-3wx, Omni-5wx or Omni-9wx). In a fully populated 3-slot switch, you could have up to 32 switched connections, in a fully populated 5-slot switch, you could have up to 64 switched Ethernet connections, and in a fully populated 9-slot switch you could have up to 128 switched connections.

ESM-FM-16W Technical Specifications	
Number of ports	16
Connector Type	ST
Standards Supported	IEEE 802.3, 802.3i; IAB RFCs 826, 894, 1398
Data Rate	10 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	2,048
Connections Supported	10BASE-FL hub or device; full or half duplex Ethernet-to-Ethernet
Optical output power	-20 to -12 dBm
Optical receiver sensitivity	-32.5 to -12 dBm
Power Budget	12.5 dB
Cable Supported	62.5 micron multimode fiber (12.5 dBm)
Cable Distance	2 km

Warning Label. This label indicates that the module contains an optical transceiver.

This ESM module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number.

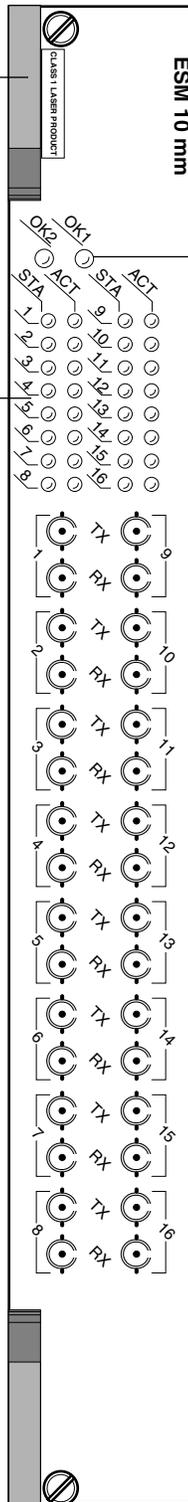
STA (Status). On Green continuously when a good cable connection exists, per the 10BASE-FL specification, to a 10BASE-FL device. Off when a good connection does not exist. Flashes Green slowly when the port has been disabled.

ACT (Activity). On Green when data is transmitted or received on the corresponding port.

Port LEDs

Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.



Ethernet 16-Port Fiber Wide Module

ESM-100C-32W Ethernet Module

The ESM-100C-32W Ethernet module contains 32 ports. Each port supports a fully-switched, high-density 10 or 100 Mbps desktop connection in either half- or full-duplex mode.

The flexibility of 10/100 Mbps ports allows users to support their current 10BaseT devices and gradually upgrade to 100BaseTx without having to replace their switch ports. Also, users who want high-density 10/100 with an ATM PNNI backbone can use the ESM-100C-32W in conjunction with a CSM switching module installed in the OmniSwitch chassis.

◆ Important Note ◆

While the ESM-100C-32W offers similar functionality to the Omni Switch/Router ESX-100C-32W module, the ESM-100C-32W is compatible *only* with the OmniSwitch chassis. (Note that OmniSwitch modules are distinguished by the letter **M** in the module name on the front panel, whereas Omni Switch/Router modules are distinguished by the letter **X**.)

In addition, the ESM-100C-32W is intended for use *only* with MPM-III or MPM-1G management processor modules.

Each of the thirty-two (32) Ethernet ports on the ESM-100C-32W can auto-sense the connection speed and automatically switch at that speed. By default, each port is configured to operate in auto-sensing, half-duplex mode. However, each port may be manually configured via the **10/100cfg** command. (The **10/100cfg** command allows you to disable or enable auto-sensing, set the line speed, and set the link mode to half- or full-duplex.)

An additional software command, **10/100vc**, allows you to view the current line speed and link mode of each port connection. For more information on the **10/100cfg** and **10/100vc** commands, refer to Chapter 19, “Managing Ethernet Modules.”

The 32 RJ-45 ports on the ESM-100C-32W support either unshielded twisted pair (UTP) or shielded twisted pair (STP) cable (see *ESM-100C-32W Technical Specifications* on page 7-29 for more information). Each port may be connected to a single high-speed device or to a hub that is serving multiple devices. In addition, the ESM-100C-32W can be used in the wiring closet with a mix of 10 Mbps Ethernet devices and 100 Mbps Fast Ethernet devices.

Module ports are divided into four (4) banks, with eight (8) ports per bank. Ports are numbered from 1 to 8 within each of the four banks. Banks are labelled **A**, **B**, **C**, and **D**. The ESM-100C-32W software automatically numbers the port/bank locations—1 through 32—with Port **A1** labeled as 1, Port **B1** as 9, **C1** as 17, **D1** as 25, etc. This grouping simplifies the module’s LED display, which is organized as a matrix (for more details, refer to the illustration on page 7-30).

◆ Note ◆

Because it is intended to support high-density desktop connections, rather than backbone connections, the ESM-100C-32W does not support OmniChannel.

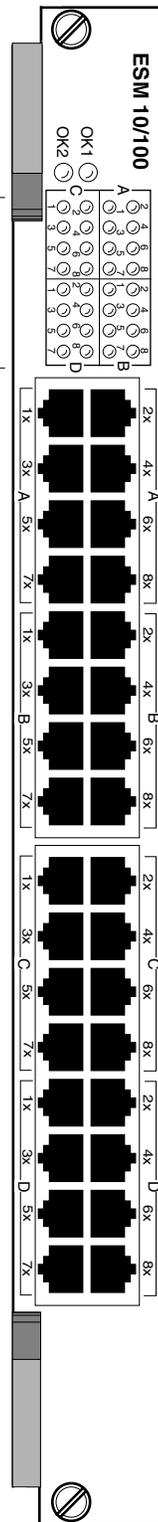
ESM-100C-32W Technical Specifications	
Ports	(32) 10BaseT/100BaseTx Ethernet ports
Connector Type	RJ-45
Standards Supported	IEEE 802.3; IAB RFCs 826, 894, IEEE 10BaseT, 100BaseTx
Data Rate	10 or 100 Mbps (auto-sensing)
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024 (2,048 with CAM upgrade option)
Connections Supported	10BaseT hub or device; 100BaseTx hub or device
Cables Supported	Unshielded twisted-pair (UTP)—100 ohms (Category 5, EIA/TIA 568); Shielded twisted-pair (STP)—100 ohms (Category 5)
Current Draw	5.75 amps
Cable Distance	100 m

Port LEDs (Port Connection Status). Each port LED corresponds numerically to a port on the module.

When an LED displays green continuously, a good cable connection exists.

A port LED will blink green when traffic is transmitted or received on the port.

Port LEDs



Module LEDs

OK1 LED (Hardware Status). This dual-state LED displays Green when the switch has passed hardware diagnostic tests that are initiated at boot-up.

The **OK1** LED displays Amber when the hardware has failed diagnostic tests.

OK2 LED (Software Status). This dual-state LED displays Green when software has loaded successfully and the module is ready to execute commands.

The **OK2** LED blinks Amber when the switch is in a transitional state, such as when it first boots up. [If the **OK2** LED blinks Amber for an extended period of time (i.e., more than a minute), you should reboot the switch.]

The **OK2** LED displays solid Amber when software was not loaded successfully.

32-Port Auto-Sensing 10/100 Ethernet Switching Module

ESM-T-24W

The ESM-T-24W Ethernet switching module contains two 50-pin connectors that support 24 switched 10BaseT Ethernet ports. Each of the 12 ports uses the full 10 Mbps of dedicated bandwidth. The 50-pin RJ-21 connectors provide a convenient cabling solution for networks with existing punch down blocks and patch panels.

All ports support either half- or full-duplex operation. You configure whether you want a half- or full-duplex connection through the **10/100cfg** command, which is explained in Chapter 19, “Managing Ethernet Modules.” By default, ESM-T-24W ports are configured for half-duplex connections.

Port LEDs are divided into two (2) banks of twelve (12). LEDs are numbered from 1 to 12 within each of the two banks and each LED corresponds to a port. The two sets are labelled **A** and **B** (see illustration on the next page).

Because the ESM-T-24W is a wide-style module, it is only supported in a wide chassis (i.e., Omni-3wx, Omni-5wx, or Omni-9wx). Using ESM-T-24W modules in a fully populated Omni-5wx, you could have up to 96 switched Ethernet connections, and in a fully populated Omni-9wx you could have up to 192 switched connections.

ESM-T-24W Technical Specifications	
Number of ports	(2) Telco supporting 24 end devices
Connector Type	Telco 50-pin (RJ-21)
Standards Supported	IEEE 802.3, 802.3i; IAB RFCs 826, 894, 1398
Data Rate	10 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024
Connections Supported	Telco patch panel or punch down block
Cable Supported	Unshielded twisted pair (UTP) Shielded twisted pair (STP)—100 ohm
Cable Distance	100 m

Each LED corresponds to a port on the module.

Letters correspond to the Telco connector through which a port connects. **A** corresponds to the top RJ-21 connector and **B** corresponds to the bottom RJ-21 connector.

The numbers correspond to port numbers attached to either the **A** or **B** connector.

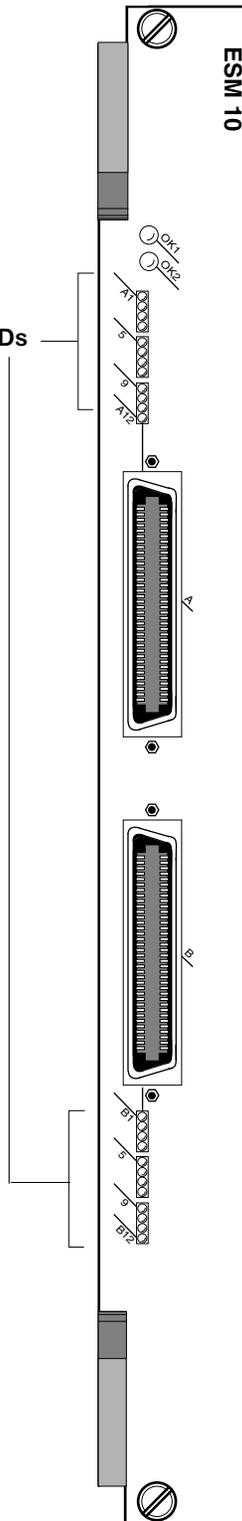
When an LED displays Green continuously, a good cable connection exists to a 10BASE-T device.

An LED will flash when traffic is transmitted or received on the port.

Port LEDs

Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.



Ethernet 24-Port Telco Module

GSM-F-2W Gigabit Ethernet Module

The GSM-F-2W is a 2-port Gigabit Ethernet module designed to support fully-switched Gigabit backbone connections into the OmniSwitch.

This module allows users to maintain their current OmniSwitch(es) in the wiring closet while upgrading their core switch(es) to the Omni Switch/Router.

◆ Important Note ◆

While the GSM-F-2W offers similar functionality to the Omni Switch/Router GSX-F-2W module, the GSM-F-2W is compatible *only* with the OmniSwitch chassis. (Note that OmniSwitch modules are distinguished by the letter **M** in the module name on the front panel, whereas Omni Switch/Router modules are distinguished by the letter **X**.)

In addition, the GSM-F-2W is intended for use *only* with MPM-1G or MPM-III management processor modules.

GSM-F-2W modules are factory configured with either two (2) multimode, two (2) long-reach single mode, or two (2) 1000BASE-LX single mode fiber ports. The model number for each configuration is as follows:

GSM-FM-2W: Factory configured with two (2) 1000BASE-SX multimode fiber ports.

GSM-FH-2W: Factory configured with two (2) long-reach single mode fiber ports.

GSM-FS-2W: Factory configured with two (2) intermediate-reach single mode fiber ports.

Each port configuration is color-coded in order to differentiate between modes: Black for multimode fiber connections; blue for intermediate-reach single mode fiber connections; yellow for long-reach single mode fiber connections. (See the “Handling Fiber and Fiber Optic Connectors” section in Chapter 3, “Omni Switch/Router Switching Modules,” for information on proper handling of SC connectors and fiber-optic cable.)

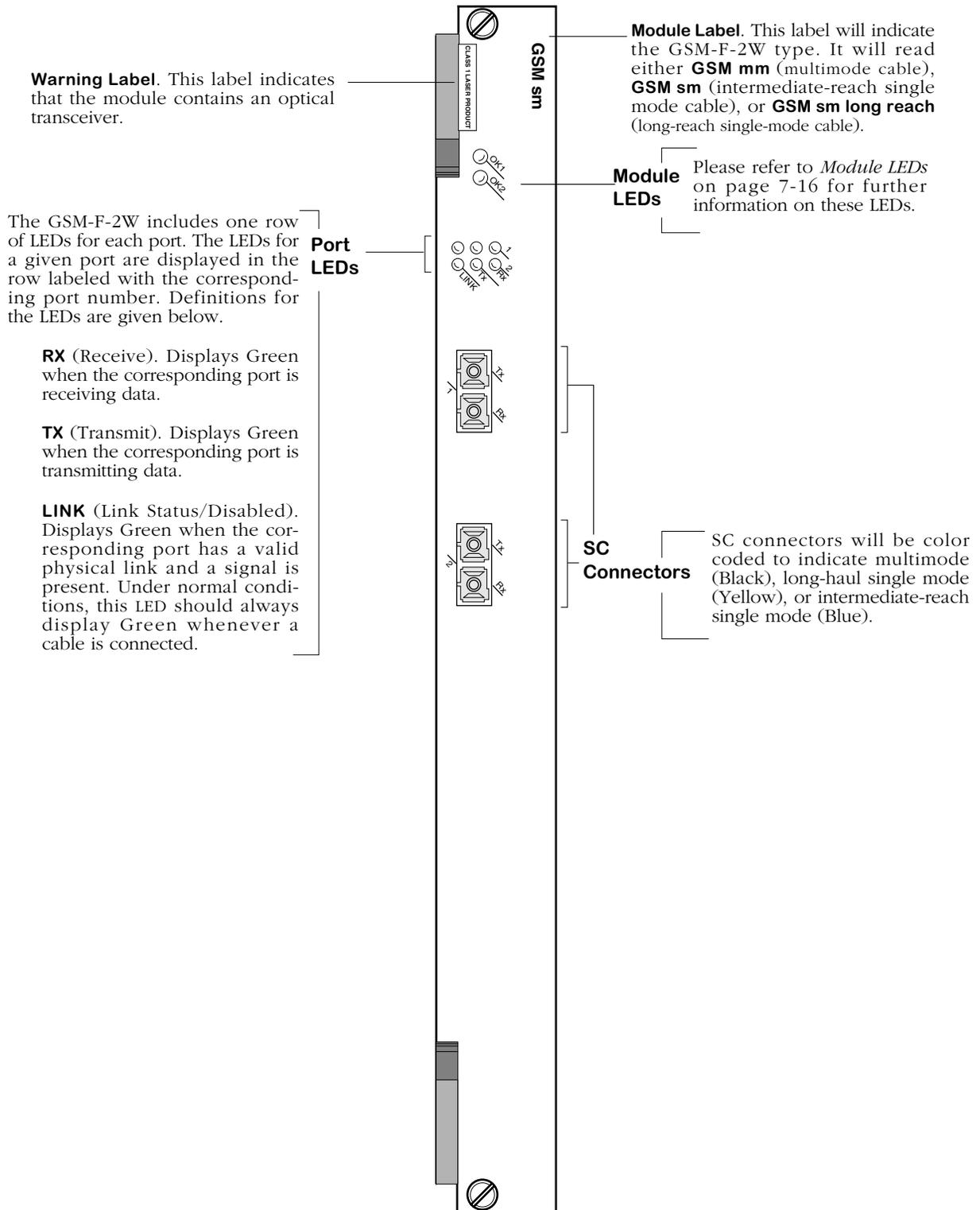
GSM-F-2W Technical Specifications	
Number of ports	2
Connector Type	SC
Standards Supported	802-3z, 1000Base-LX, and 1000Base-SX
Data Rate	1 Gigabit per second (full duplex)
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	4,096
Connections Supported	1000Base-LX or 1000Base-SX connection to backbone or server
Cable Supported	Multimode and single mode
Output Optical Power	-9.5 to -4 dBm (Multimode) -9.5 to -3 dBm (Intermediate-reach single mode) 0 to +5 dBm (Intermediate-reach single mode)
Input Optical Power	-17 to 0 dBm (Multimode) -20 to -3 dBm (Intermediate-reach single mode) -24 to -3 dBm (Intermediate-reach single mode)
Cable Distance	Multimode fiber: \approx 220 m Intermediate-reach single mode fiber: \approx 10 km Long-reach single mode fiber: \approx 70 km

◆ Special Note ◆

The single mode version of this module has been deemed:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.



2-Port Gigabit Ethernet Switching Module

ATM Access Modules

ATM access switching modules allow you to connect the OmniSwitch to ATM servers, backbones and switches. ATM modules support OC-3, DS-3, and E3 interfaces (155, 44.736, and 34.368 Mbps respectively) and include the following:

- ASM-155F*x* One or two port fiber single mode or multimode OC-3 switching module. **(Discontinued)**
- ASM2-155F*x* One or two port fiber single mode or multimode OC-3 switching module. This is a higher performance version of the ASM-155F*x*.
- ASM-155C One or two port UTP OC-3 switching module. **(Discontinued)**
- ASM2-622F **(Discontinued)** One or two port fiber single mode or multimode OC-12 switching module. **(Discontinued)**
- ASM2-622FR Two or four port redundant fiber single mode or multimode OC-12 switching module. Each port pair includes a primary and backup port.
- ASM-DS3 One or two port DS-3 switching module. **(Discontinued)**
- ASM-E3 One or two port E3 switching module. **(Discontinued)**
- ASM-CE One ATM uplink port (OC-3, DS-3 or E3), two T1/E1 ports, and two serial ports supporting ATM circuit emulation. **(Discontinued)**
- ASM2-DS3 One or two port DS-3 switching module. This is a higher performance version of the ASM-DS3.
- ASM2-E3 One or two port E3 switching module. This is a higher performance version of the ASM-E3.

The OC-3 modules are suited for connecting the switch to an ATM campus backbone or directly to an ATM server.

Through the use of Point-to-Point Bridging (RFC 1483), you can extend all LAN traffic over the ATM backbone. Several OmniSwitches could be connected over one or more backbones. In such a configuration, you combine the flexibility of the OmniSwitch's any-to-any switching with the power and speed of the ATM backbone without the use of an ATM backbone switch.

If you are connecting the OmniSwitch directly to an ATM server, then all non-ATM devices in the LAN can communicate with the high-speed ATM server through the OmniSwitch.

If your network uses ATM backbone switches, then the OmniSwitch ATM modules allow all non-ATM devices in the network to have access to the ATM network through the use of LAN Emulation (LANE) or an Alcatel version of LANE called XLANE, or "VLAN Clusters." XLANE connects OmniSwitches and OmniStacks together across ATM and legacy LAN networks to gain the benefits of LANE while eliminating interoperability issues. Classical IP (RFC 1577) may also be used to extend LAN traffic over ATM.

The DS-3 and E3 modules are well suited for connecting the switch to ATM carrier services offered by Telco service providers.

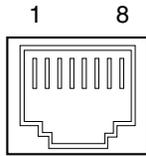
Software controls on the switch allow you to control and monitor activity on ATM modules. On each ATM port, you can configure the connection type (SVC or PVC), Virtual Channel Connections (VCC), segment sizes, and loopback controls. On each VCC, you can configure Quality of Service (QoS), Best Effort, Traffic Descriptor, and Peak Cell Rate variables. In addition, you can configure all ATM bridging and trunking services (Point-to-Point Bridging, LANE, XLANE, Classical IP). See Chapter 33, "Managing ATM Access Modules," and Chapter 36, "Configuring ATM Services," for further information on ATM software controls.

◆ Note ◆

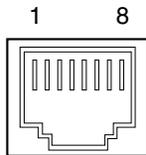
Peak cell rates will not be initialized if you replace an ASM module with a slower-speed ASM module in the same slot. (For example, you replace an ASM2-155FM-1W with an ASM2-DS3-1W.)

ATM Pinouts

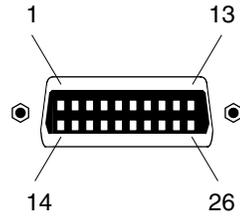
The following figures and table illustrate the pinouts for copper-based connector ports.



ATM RJ-45 Specifications	
Pin Number	Standard Signal Name
1	Xmit Data +
2	Xmit Data -
3	
4	
5	
6	
7	Receive Data +
8	Receive Data -



ATM CE RJ-48C Specifications	
Pin Number	Standard Signal Name
1	Tx_Ring
2	Tx_Tip
3	Chassis GND
4	Rx_Ring
5	Rx_Tip
6	Chassis GND
7	Chassis GND (A jumper is provided for connecting Pins 7 and 8 to the chassis ground, if required.)
8	Chassis GND (A jumper is provided for connecting Pins 7 and 8 to the chassis ground, if required.)



Circuit Emulation Serial Port Numbering

Serial Port Specifications							
Generic Signal Name	Source	Alcatel SPI		EIA-530		RS-449	
		Mnemonic	Pin	Mnemonic	Pin	Mnemonic	Pin
Shield	--	Shield	1	--	1	--	1
Signal Ground	--	AB	7	AB	7	SG	19
Transmitted Data	DTE	TD(A)	2	BA(A)	2	SD(A)	4
		TD(B)	14	BA(B)	14	SD(B)	22
Received Data	DCE	RD(A)	3	BB(A)	3	RD(A)	6
		RD(B)	16	BB(B)	16	RD(B)	24
Transmit Clock	DCE	TC(A)	15	DB(A)	15	ST(A)	5
		TC(B)	12	DB(B)	12	ST(B)	23
Receive Clock	DCE	TC(A)	17	DD(A)	17	RT(A)	8
		TC(B)	9	DD(B)	9	RT(B)	26
Ext. Transmit Clock	DTE	XC(A)	24	DA(A)	24	TT(A)	17
		XC(B)	11	DA(B)	11	TT(B)	35
Request To Send	DTE	RS(A)	4	CA(A)	4	RS(A)	7
		RS(B)	19	CA(B)	19	RS(B)	25
Clear To Send	DCE	CS(A)	5	CB(A)	5	CS(A)	9
		CS(B)	13	CB(B)	13	CS(B)	27
Data Set Ready	DCE	DR(A)	6	CC(A)	6	DM(A)	11
		DR(B)	22	CC(B)	22	DM(B)	29
Data Terminal Ready	DTE	TR(A)	20	CD(A)	20	TR(A)	12
		TR(B)	23	CD(B)	23	TR(B)	30
Data Carrier Detect	DCE	CD(A)	8	CF(A)	8	RR(A)	13
		CD(B)	10	CF(B)	10	RR(B)	31
Local Loopback	DTE	LL	18	LL	18	LL	10
Remote Loopback	DTE	RL	21	RL	21	RL	14
Ring Indicator	DCE	RI/TM	25	--	--	--	--
Test Mode	DCE	RI/TM	25	TM	25	TM	18
Cable Type 4	--	CTP4	18		n/c		n/c
Cable Type 3	--	CTP3	26		n/c		n/c
Cable Type 2	--	CTP2	13				
Cable Type 1	--	CTP1	22				
Cable Type 0	--	CTP0	10				

continued on next page...

Serial Port Specifications (cont.)							
Generic Signal Name	Source	X.21/X.26		V.35		RS232	
		Mnemonic	Pin	Mnemonic	Pin	Mnemonic	Pin
Shield	--	--	1	--	A	--	1
Signal Ground	--	G	8	102	B	AB	7
Transmitted Data	DTE	T(A)	2	103(A)	P	BA	2
		T(B)	9	103(B)	S		
Received Data	DCE	R(A)	4	104(A)	R	BB	3
		R(B)	11	104(B)	T		
Transmit Clock	DCE	--	--	114(A)	Y	DB	15
				114(B)	AA		
Receive Clock	DCE	S(A)	6	115(A)	V	DD	17
		S(B)	13	115(B)	X		
Ext. Transmit Clock	DTE	B(A)	7	113(A)	U	DA	24
		B(B)	14	113	W		
Request To Send	DTE	C(A)	3	105	C	CA	4
		C(B)	10				
Clear To Send	DCE	--	--	106	D	CB	5
Data Set Ready	DCE	--	--	107	E	CC	6
Data Terminal Ready	DTE	--	--	108	H	CD	20
Data Carrier Detect	DCE	I(A)	5	109	F	CF	8
		I(B)	12				
Local Loopback	DTE	--	--	141	L	LL	18
Remote Loopback	DTE	--	--	140	N	RL	21
Ring Indicator	DCE	--	--	125	J	CE	22
Test Mode	DCE	--	--	142	NN	TM	25
Cable Type 4	--		n/c		n/c		
Cable Type 3	--		n/c		n/c		
Cable Type 2	--						
Cable Type 1	--						
Cable Type 0	--						

ASM-155F x (Discontinued)

The ASM-155F x switching module can contain one or two fiber (SC) ports that support OC-3 connections. Each port connection provides 155 Mbps of bandwidth and connects to either multimode or single mode cable. The ASM-155F x can be factory configured with single mode (intermediate- or long-reach) or multimode fiber ports. The single mode intermediate-reach version is referred to as the ASM-155FS; the single mode long-reach version is referred to as the ASM-155FH; the multimode version is referred to as the ASM-155FM. Connector types are differentiated by color: multimode connectors are black, single mode intermediate-reach connectors are blue, and single mode long-reach connectors are yellow.

ASM-155F x ports are ideally suited for connections to an ATM campus fiber backbone. Using point-to-point bridging (RFC 1483), you can extend all devices (ATM and non-ATM) connected to an OmniSwitch over the ATM fiber backbone without the use of a high-end ATM switch. This module comes in a high-performance version referred to as the ASM2-155-F x , which is recommended for LANE and point-to-point bridging configurations.

ASM-155Fx Technical Specifications	
Number of ports	1 or 2
Connector Type	SC
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/2.0 MPOA Client
Data Rate	155 Mbps
ATM Adaption Layers	AAL5
MAC Addresses Supported	1,024; 2,048 or 4,096 with CAM upgrade option
Max. No. of VCs Supported	1,024
Connections Supported	OC-3 connections to ATM server, backbone, or switch.
Optical output power	Multimode: -19 to -14 dBm Single mode (intermediate reach): -14 to -8 dBm Single mode (long reach): -20 to -14 dBm
Optical receiver sensitivity	Multimode: -30 to -14 dBm Single mode (intermediate reach): -31 to -8 dBm Single mode (long reach): -34 to -10 dBm
Power Budget	Multimode: 11 dB Single mode (intermediate reach): 16 dB Single mode (long reach): 29 dB
Cable Supported	Multimode: 62.5 micron multimode fiber Single mode (intermediate and long reach): single mode fiber
Cable Distance	Multimode: 4.2 km Single mode (intermediate reach): 24 km Single mode (long reach): 40 km

◆ Special Note ◆

The single mode version of this module is:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

This module includes one set of LEDs for each port. The LEDs for a given port display above the port. If the ASM module includes two ports, then the module contains two sets of LEDs. The second set of LEDs displays above the second port.

Warning Label. This label indicates that the module contains an optical transceiver.

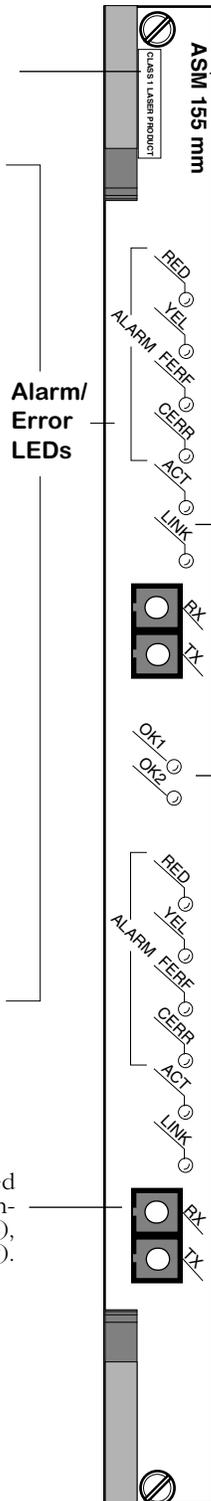
RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the ASM module is plugged in, but no cable has been connected.

YEL (Yellow Alarm). On Amber when a far end receive failure occurs. The recipient of cells from this ASM is not receiving those cells. This error may be due to a transmission error by the ASM or a receive error on the other end of the link.

FERF (Far End Status Alarm). On Amber when a far end receive failure occurs. The recipient of cells from this ASM is not receiving those cells. This error may be due to a transmission error by the ASM or a receive error on the other end of the link. This LED functions the same as the YEL LED.

CERR (Cell Error). On Amber when a cell error occurs. A cell error may result from bad data within a cell or when cells are not being received (receive error). If the RED Alarm LED is On, the CERR LED will also be On since receive errors are also considered cell errors. This LED will be on when the module is plugged in but no cable has been connected.

SC connectors will be color coded to indicate multimode (Black), single mode intermediate-reach (Blue), or single mode long-reach (Yellow).



Module Label. This label will indicate the ASM-155Fx type. It will read either **ASM 155 mm** (multimode cable), **ASM 155 sm** (intermediate-reach single mode cable), or **ASM 155 sm long reach** (long-reach single-mode cable).

ACT (Activity). On Green when the port is transmitting or receiving cells.

LINK (Link Status/Disabled). On Green when the module has a valid physical link and a signal is present. Under normal conditions, this LED should always be on when a cable is connected. It will be off if no cable is connected. It should not be on at the same time as the RED Alarm LED.

Status LEDs

Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

Alarm/Error LEDs

ATM 2-Port Switching Module (Single or Multimode)

ASM-155C (Discontinued)

The ASM-155C switching module can contain one or two RJ-45 ports that support OC-3 connections. Each port connection provides 155 Mbps of bandwidth and connects to unshielded twisted pair (UTP) cable.

ASM-155C ports are suited for connections to ATM servers. By connecting an ASM-155C port to an ATM server, you enable all devices (ATM and non-ATM) connected to an OmniSwitch to communicate with the high-speed ATM server.

The ASM-155C is actually a sub-module, or daughtercard, that attaches to a High-Speed Module (HSM). The HSM contains memory and processing power for switching modules that operate at speeds greater than 10 Mbps. You plug your cable directly into the ASM-155C sub-module, but it is the HSM module that connects to the switch backplane

ASM-155C Technical Specifications	
Number of ports	1 or 2
Connector Type	RJ-45
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/2.0 MPOA Client
Data Rate	155 Mbps
ATM Adaption Layers	AAL5
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Max. No. of VCs Supported	1,024
Connections Supported	OC-3 connections to ATM server, backbone, or switch.
Cable Supported	Unshielded twisted pair (UTP)

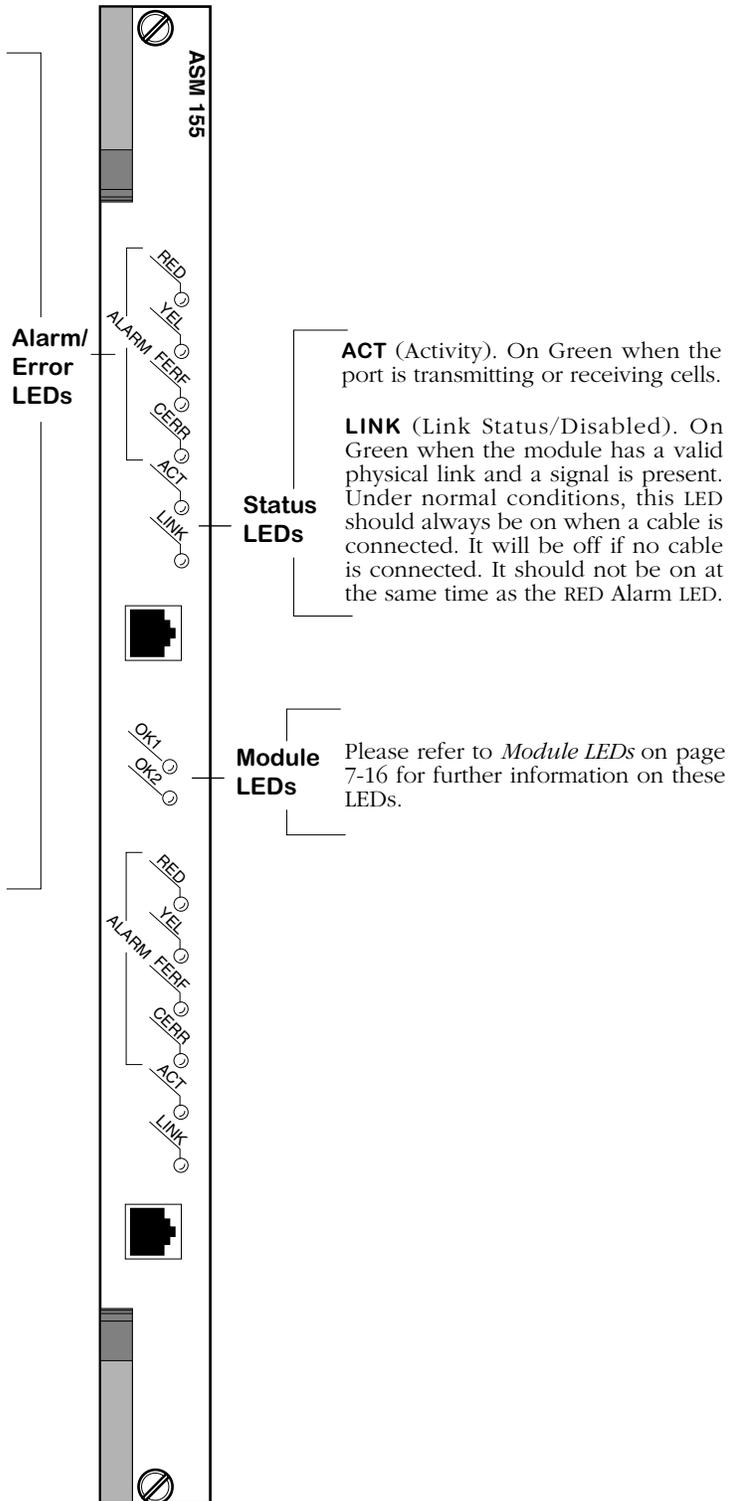
This module includes one set of LEDs for each port. The LEDs for a given port display above the port. If the ASM module includes two ports, then the module contains two sets of LEDs. The second set of LEDs displays above the second port.

RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the ASM module is plugged in, but no cable has been connected.

YEL (Yellow Alarm). On Amber when a far end receive failure occurs. The recipient of cells from this ASM is not receiving those cells. This error may be due to a transmission error by the ASM or a receive error on the other end of the link.

FERF (Far End Status Alarm). On Amber when a far end receive failure occurs. The recipient of cells from this ASM is not receiving those cells. This error may be due to a transmission error by the ASM or a receive error on the other end of the link. This LED functions the same as the YEL LED.

CERR (Cell Error). On Amber when a cell error occurs. A cell error may result from bad data within a cell or when cells are not being received (receive error). If the RED Alarm LED is On, the CERR LED will also be On since receive errors are also considered cell errors. This LED will be on when the module is plugged in but no cable has been connected.



ATM 2-Port UTP Module

ASM2-155F

The ASM2-155F switching module is an enhanced version of the ASM-155F. It contains one or two fiber (SC) ports that support OC-3 connections. Each port connection provides 155 Mbps of bandwidth and connects to either multimode or single mode cable. The ASM2-155F can be factory configured with single mode or multimode fiber ports. The intermediate-reach single mode version is referred to as the ASM2-155FS; long-reach single mode version is referred to as the ASM2-155FH; the multimode version is referred to as the ASM2-155FM. Multimode and single mode connectors are differentiated by color: multimode connectors are black and single mode connectors are blue.

ASM2-155F ports are suited for connections to an ATM campus fiber backbone. Using an ATM service (LANE, point-to-point bridging, etc.), you can extend all devices (ATM and non-ATM) connected to an OmniSwitch over the ATM fiber backbone.

ASM2-155FM/S Technical Specifications	
Number of ports	1 or 2
Connector Type	SC
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/2.0 MPOA Client
Data Rate	155 Mbps
Maximum Frame Size	8,000 bytes
MAC Addresses Supported	4,096
Max. No. of VCs Supported	1,024
Connections Supported	OC-3 connections to ATM server or backbone.
Optical output power	Multimode: -19 to -14 dBm Single mode (intermediate reach): -14 to -8 dBm Single mode (long reach): -20 to -14 dBm
Optical receiver sensitivity	Multimode: -30 to -14 dBm Single mode (intermediate reach): -31 to -8 dBm Single mode (long reach): -34 to -10 dBm
Power Budget	Multimode: 11 dB Single mode (intermediate reach): 16 dB Single mode (long reach): 29 dB
Cable Supported	Multimode: 62.5 micron multimode fiber Single mode (intermediate and long reach): single mode fiber
Cable Distance	Multimode: 4.2 km Single mode (intermediate reach): 24 km Single mode (long reach): 40 km

◆ Special Note ◆

The single mode version of this module is:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

This module includes one set of LEDs for each port. The LEDs for a given port display above the port. If the ASM module includes two ports, then the module contains two sets of LEDs. The second set of LEDs displays above the second port.

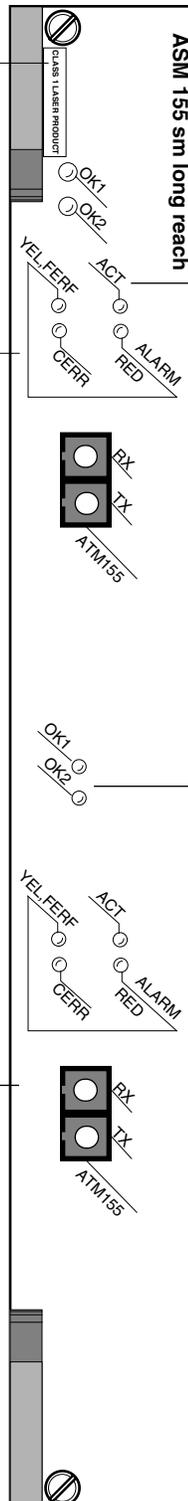
Warning Label. This label indicates that the module contains an optical transceiver.

YEL, FERF (Yellow/Far End Status Alarm). On Amber when a far end receive failure occurs. The recipient of cells from this ASM is not receiving those cells. This error may be due to a transmission error by the ASM or a receive error on the other end of the link.

CERR (Cell Error). On Amber when a cell error occurs. A cell error may result from bad data within a cell or when cells are not being received (receive error). If the RED Alarm LED is On, the CERR LED will also be On since receive errors are also considered cell errors. This LED will be on when the module is plugged in but no cable has been connected.

RED (Red Alarm). This LED describes Red alarm status on the port. The LED is on Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the ASM module is plugged in, but no cable has been connected.

SC connectors will be color coded to indicate multimode (Black), single mode intermediate-reach (Blue), or single mode long-reach (Yellow).



Module Label. This label will indicate the ASM2-F type. It will read either **ASM 155 mm** (multimode cable), **ASM 155 sm** (intermediate-reach single mode cable), or **ASM sm 155 long reach** (long-reach single-mode cable).

ACT (Activity). This LED describes status and activity on this port. The LED will be in one of three states. The following describes each state:

- Off** There is no link and no data transmitting. Possibly the no cable is connected.
- Green (Solid)** The port is enabled and a signal is present, but no data is being transmitted or received.
- Green (Blinking)** Data (ATM cells) are being transmitted or received on this port.

Module LEDs Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

ASM2-155F

ASM2-155RF

The ASM2-155RF switching module can contain one or two sets of dual-redundant fiber (SC) port pairs that support OC-3 connections. Each port connection provides 155 Mbps of bandwidth and connects to either multimode or single mode cable. The ASM2-155RF can be factory configured with single mode or multimode fiber ports. The single mode version is referred to as the ASM2-155RFS; the multimode version is referred to as the ASM2-155RFM. Multimode and single mode connectors are differentiated by color: multimode connectors are black and single mode connectors are blue.

ASM2-155RF ports are ideally suited for mission-critical ATM access connections. The redundant port pairs ensure that critical backbone and server connections are protected against failures on the primary link.

◆ Note ◆

The two-port version of the ASM2-155RF has been discontinued.

ASM2-155RFM/S Technical Specifications	
Number of ports	1 or 2 port pairs (each port pair includes a primary and backup)
Connector Type	SC
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/2.0 MPOA Client
Data Rate	155 Mbps
Maximum Frame Size	8,000 bytes
MAC Addresses Supported	4,096
Connections Supported	OC-3 connections to ATM servers or backbone.
Max. No. of VCs Supported	1,024
Optical output power	Multimode: -19 to -14 dBm Single mode (intermediate reach): -14 to -8 dBm
Optical receiver sensitivity	Multimode: -30 to -14 dBm Single mode (intermediate reach): -31 to -8 dBm
Power Budget	Multimode: 11 dB Single mode (intermediate reach): 16 dB
Cable Supported	Multimode: 62.5 micron multimode fiber Single mode (intermediate reach): single mode fiber
Cable Distance	Multimode: 4.2 km Single mode (intermediate reach): 24 km

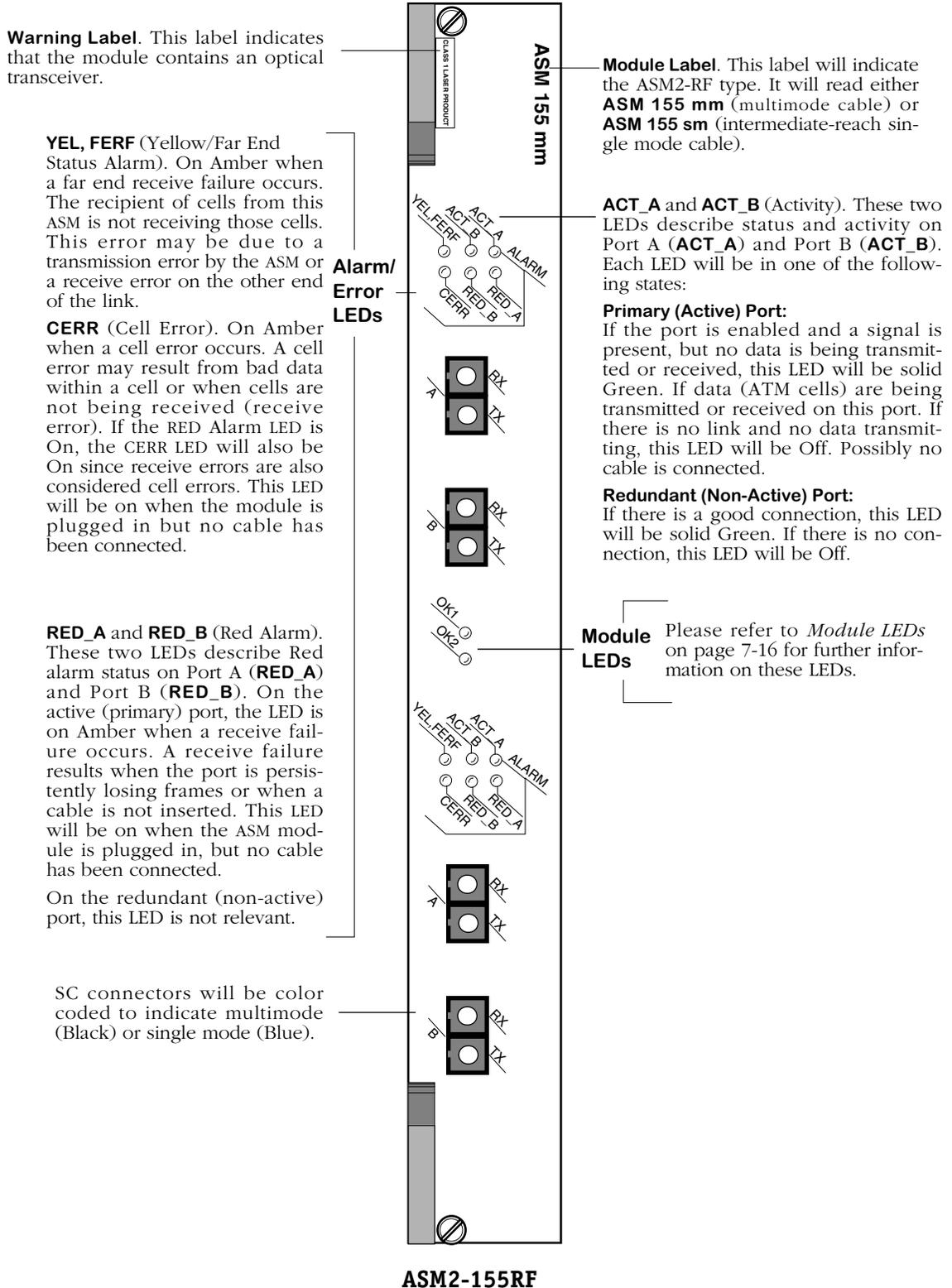
◆ **Special Note** ◆

The single mode version of this module is:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

This module includes one set of LEDs for each redundant port pair. The LEDs for a given pair display above the port. If the ASM2 module includes two sets of ports, then the module contains two sets of LEDs. The second set of LEDs displays above the second port pair.



ASM2-622F (Discontinued)

The ASM2-622F switching module can contain one or two fiber (SC) ports that support OC-12 connections. Each port connection provides 622 Mbps of bandwidth and connects to either multimode or single mode cable. The ASM2-622F can be factory configured with single mode or multimode fiber ports. The single mode version is referred to as the ASM2-622FS; the multimode version is referred to as the ASM2-622FM. Multimode and single mode connectors are differentiated by color: multimode connectors are black and single mode connectors are blue.

ASM2-622F ports are ideally suited for ATM access connections in an ATM campus fiber backbone. The ASM2-622FM/FS switching module can connect to ATM servers and backbones. Its on-board Content Addressable Memory (CAM) supports up to 8,192 MAC addresses, making the module a powerful backbone connection.

◆ Note ◆

The ASM2-622F is supported, but it has been discontinued. For 622 Mbps ATM access, the ASM2-622RF (see *ASM2-622RF* on page 7-56) is recommended.

ASM2-622FM/S Technical Specifications	
Number of ports	1 or 2
Connector Type	SC
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/2.0 MPOA Client
Data Rate	622 Mbps
Maximum Frame Size	8,000 bytes
MAC Addresses Supported	4,096 or 8,192
Max. No. of VCs Supported	1,024
Connections Supported	OC-12 connections to ATM server or backbone.
Optical output power	Multimode: -20 to -14 dBm Single mode: -15 to -8 dBm
Optical receiver sensitivity	Multimode: -26 to -14 dBm Single mode: -28 to -8 dBm
Cable Supported	Multi-Mode: 62.5 micron multimode fiber Single mode: intermediate-reach single-mode fiber
Cable Distance	Multimode: 500 meters Single mode: 15 km (intermediate reach)

◆ Special Note ◆

The single mode version of this module is:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

This module includes one set of LEDs for each port. The LEDs for a given port display above the port. If the ASM2 module includes two ports, then the module contains two sets of LEDs. The second set of LEDs displays above the second port.

YEL, FERF (Yellow/Far End Status Alarm). On Amber when a far end receive failure occurs. The recipient of cells from this ASM2 is not receiving those cells. This error may be due to a transmission error by the ASM2 or a receive error on the other end of the link.

CERR (Cell Error). On Amber when a cell error occurs. A cell error may result from bad data within a cell or when cells are not being received (receive error). If the RED Alarm LED is On, the CERR LED will also be On since receive errors are also considered cell errors. This LED will be on when the module is plugged in but no cable has been connected.

RED (Red Alarm). This LED describes Red alarm status on the ASM2-622 port. The LED is on Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the ASM module is plugged in, but no cable has been connected.

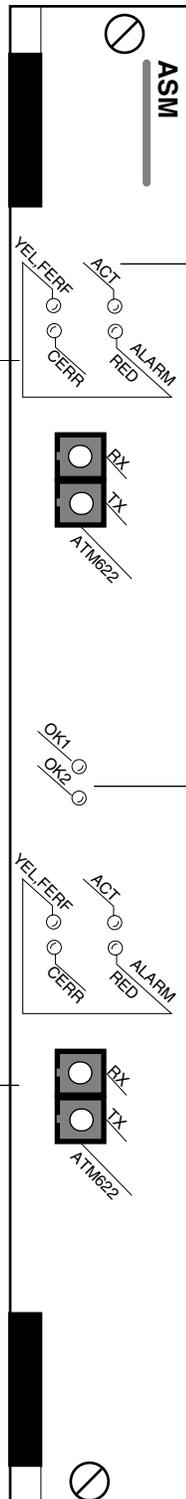
**Alarm/
Error
LEDs**

ACT(Activity). This LED describes status and activity on the ASM2-622 port. The LED will be in one of three states. The following describes each state:

- Off** There is no link and no data transmitting. Possibly the no cable is connected.
- Green (Solid)** The port is enabled and a signal is present, but no data is being transmitted or received.
- Green (Blinking)** Data (ATM cells) are being transmitted or received on this port.

Module LEDs Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

SC connectors will be color coded to indicate multimode (Black) or single mode (Blue).



ASM2-622F

ASM2-622RF

The ASM2-622RF switching module can contain one or two sets of dual-redundant fiber (SC) port pairs that support OC-12 connections. Each port connection provides 622 Mbps of bandwidth and connects to either multimode or single mode cable. The ASM2-622RF can be factory configured with single mode or multimode fiber ports. The single mode version is referred to as the ASM2-622RFS; the multi-mode version is referred to as the ASM2-622RFM. Multimode and single mode connectors are differentiated by color: multimode connectors are black and single mode connectors are blue.

ASM2-622RF ports are ideally suited for mission-critical ATM access connections. The redundant port pairs ensure that critical backbone and server connections are protected against failures on the primary link. In addition, the module's on-board Content Addressable Memory (CAM) supports up to 8,192 MAC addresses, making the module a powerful backbone connection.

◆ Note ◆

The two-port version of the ASM2-622RF has been discontinued.

ASM2-622RFM/S Technical Specifications	
Number of ports	1 or 2 port pairs (each port pair includes a primary and backup)
Connector Type	SC
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/2.0 MPOA Client
Data Rate	622 Mbps
Maximum Frame Size	8,000 bytes
MAC Addresses Supported	4,096 or 8,192
Max. No. of VCs Supported	1,024
Connections Supported	OC-12 connections to ATM servers or backbone.
Optical output power	Multimode: -20 to -14 dBm Single mode: -15 to -8 dBm
Optical receiver sensitivity	Multimode: -26 to -14 dBm Single mode: -28 to -8 dBm
Cable Supported	Multi-Mode: 62.5 micron multimode fiber Single mode: intermediate-reach single-mode fiber
Cable Distance	Multimode: 500 meters Single mode: 15 km (intermediate reach)

◆ **Special Note** ◆

The single mode version of this module is:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

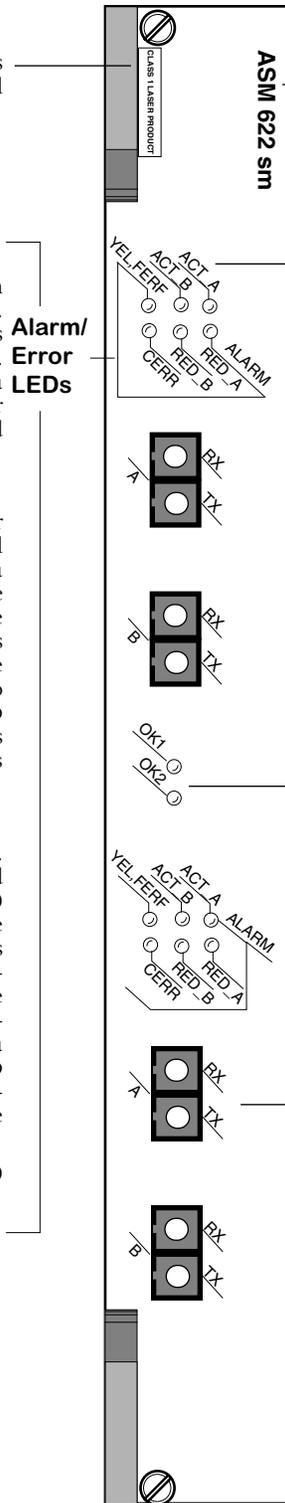
This module includes one set of LEDs for each redundant port pair. The LEDs for a given pair display above the port. If the ASM2 module includes two sets of ports, then the module contains two sets of LEDs. The second set of LEDs displays above the second port pair.

Warning Label. This label indicates that the module contains an optical transceiver.

YEL, FERF (Yellow/Far End Status Alarm). On Amber when a far end receive failure occurs. The recipient of cells from this ASM is not receiving those cells. This error may be due to a transmission error by the ASM or a receive error on the other end of the link.

CERR (Cell Error). On Amber when a cell error occurs. A cell error may result from bad data within a cell or when cells are not being received (receive error). If the RED Alarm LED is On, the CERR LED will also be On since receive errors are also considered cell errors. This LED will be on when the module is plugged in but no cable has been connected.

RED_A and **RED_B** (Red Alarm). These two LEDs describe Red alarm status on Port A (**RED_A**) and Port B (**RED_B**). On the active (primary) port, the LED is on Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the ASM module is plugged in, but no cable has been connected. On the redundant (non-active) port, this LED is not relevant.



Module Label. This label will indicate the ASM2-622RF type. It will read either **ASM 622 mm** (multimode cable) or **ASM 622 sm** (intermediate-reach single mode cable).

ACT_A and **ACT_B** (Activity). These two LEDs describe status and activity on Port A (**ACT_A**) and Port B (**ACT_B**). Each LED will be in one of the following states:

Primary (Active) Port:

If the port is enabled and a signal is present, but no data is being transmitted or received, this LED will be solid Green. If data (ATM cells) are being transmitted or received on this port. If there is no link and no data transmitting, this LED will be Off. Possibly no cable is connected.

Redundant (Non-Active) Port:

If there is a good connection, this LED will be solid Green. If there is no connection, this LED will be Off.

Module LEDs Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

SC connectors will be color coded to indicate multimode (Black) or single mode (Blue).

ASM-DS3 (Discontinued)

The ASM-DS3 switching module can contain one or two BNC ports that support DS-3 connections. Each port connection provides 44.736 Mbps of bandwidth and connects to coaxial (RG-59) cable. ASM-DS3 ports are suited for connections to ATM carrier services offered by North American Telcos. The ASM-DS3 port is a physical DTE (Data Termination Equipment) device that connects to a physical DCE (Data Communication Equipment) device, such as a DSU (Data Service Unit).

DS-3 is a Digital Signal (DS) interface used to implement wide area, public connectivity for ATM networks. There is a hierarchy of DS services based on channel capacity. DS-0, the lowest bandwidth DS channel, provides 64 Kbps of throughput. Twenty-four (24) DS-0 channels combine to form a DS-1 (1.544 Mbps of throughput). Four DS-1 channels combine to form a DS-2 (6.312 Mbps of throughput). And seven DS-2 channels combine to form a DS-3 (44.736 Mbps of throughput).

By default the ASM-DS3 uses B3ZS line encoding. Using the **map** command, you can configure the module to use C-bit parity or M23 parity and configure it for loopback controls. You should configure the ASM-DS3 module to use the same parity as the ATM service provider.

Two different mapping protocols are used to transmit ATM cells over DS-3: PLCP (Physical Layer Convergence Protocol) and ATM Direct Mapped (ADM) System. The two protocols are not compatible. Many existing DS-3 implementations use PLCP as defined in ANSI T1.624-1993, but many new implementations of DS-3 use ADM. The ASM-DS3 module supports both physical layer protocols.

The ASM-DS3 is actually a sub-module, or daughtercard, that attaches to a High-Speed Module (HSM). The HSM contains memory and processing power for switching modules that operate at speeds greater than 10 Mbps. You plug your cable directly into the ASM-DS3 sub-module, but it is the HSM module that connects to the switch backplane.

◆ Note ◆

The ASM-DS3 is supported, but it has been discontinued. For DS3 ATM access, the ASM2-DS3 (see *ASM2-DS3* on page 7-68) is recommended.

ASM-DS3 Technical Specifications	
Number of ports	1 or 2
Connector Type	BNC
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/2.0 MPOA Client ANSI T1.624-1993 (PLCP Mapping)
Data Rate	44.736 Mbps
ATM Adaption Layers	AAL5
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Max. No. of VCs Supported	1,024
Connections Supported	DS-3 connections to ATM carrier service.
Cable Distance	185 m
Cable Supported	Coaxial RG-59 (75 ohm)

This module includes one set of LEDs for each port. The LEDs for a given port display above the port. If the ASM module includes two ports, then the module contains two sets of LEDs. The second set of LEDs displays above the second port.

RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the ASM module is plugged in, but no cable has been connected.

YEL (Yellow Alarm). On Amber when a far end receive failure occurs. The recipient of cells from this ASM is not receiving those cells. This error may be due to a transmission error by the ASM or a receive error on the other end of the link.

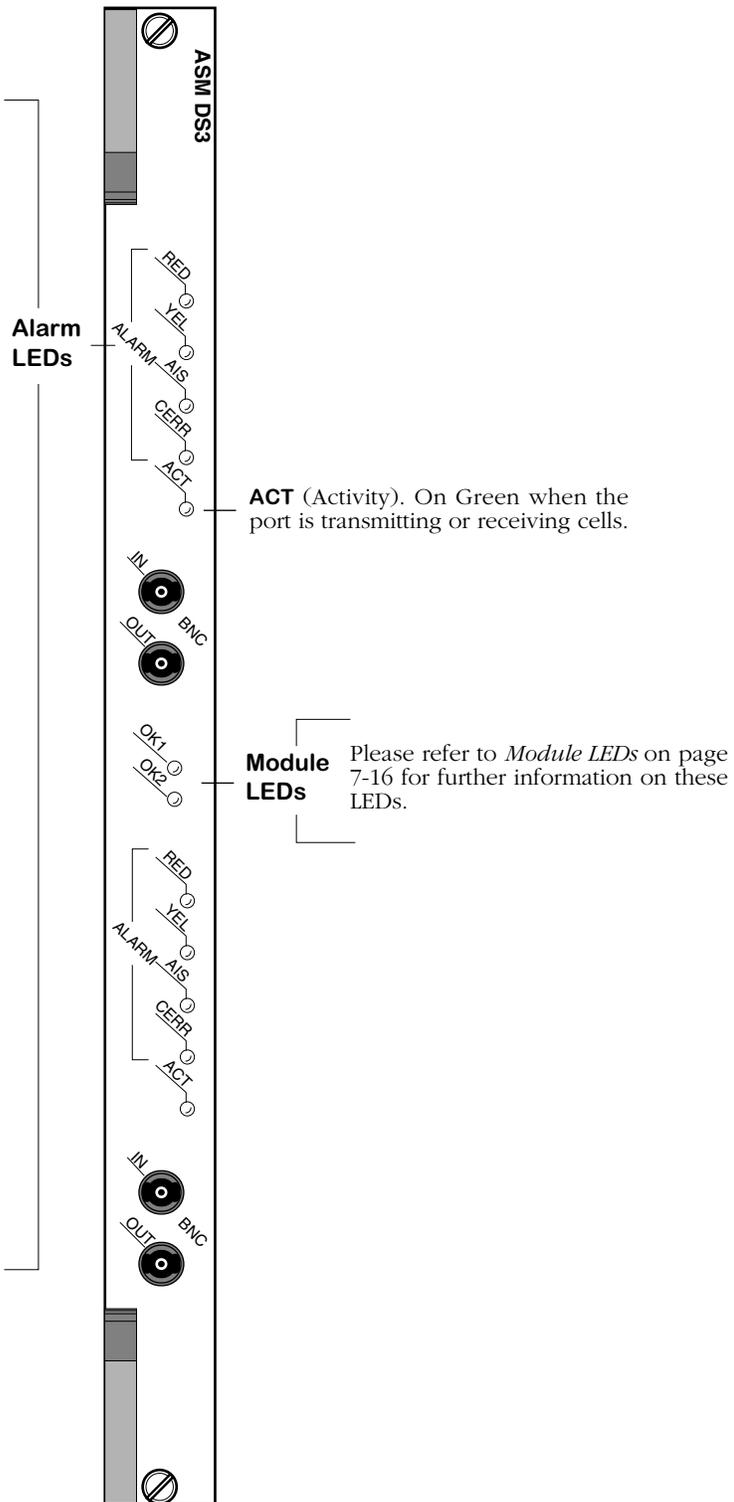
AIS (Alarm Indication Signal). On when a maintenance signal is sent to the ASM by the network. If this LED is on, then there has been a change in the Alarm Indication Signal (AIS).

CERR (Cell Loss Error). Interpretation of the CERR LED depends on the mapping protocol used on this ATM port. The mapping may be ATM Direct Mapped (ADM) or Physical Layer Convergence Protocol (PLCP) and is configured through the **map** command.

If ADM is used, then the CERR LED goes on after seven consecutive cells with errors are received. It turns back off again when six consecutive cells are received without errors.

If PLCP is used, then this LED goes on when PLCP frames are out of frame for 1 ms. It turns back off again when no out-of-frame errors have occurred for 12 ms. In PLCP framing, ATM cells are prepended with three framing octets and a path overhead octet. A PLCP frame is considered out-of-frame when errors are detected in the first two framing octets, or in the third frame octet and the path overhead octet.

In addition, the CERR LED will be on when the receive cable is not inserted.



ATM 2-Port DS-3 Module

ASM-E3 (Discontinued)

The ASM-E3 switching module can contain one or two BNC ports that support E3 connections. Each port connection provides 34.368 Mbps of bandwidth and connects to coaxial (RG-59) cable. ASM-E3 ports are suited for connections to ATM carrier services offered by International Telcos. The ASM-E3 port is a physical DTE (Data Termination Equipment) device that connects to a physical DCE (Data Communication Equipment) device, such as a DSU (Data Service Unit).

E3 is a designation used by Telcos to indicate the capacity of a digital service. E3 actually multiplexes two smaller types of digital service lines (E1 and E2) to reach its channel capacity. E1 is a carrier designation for a digital service with a data rate of 2.048 Mbps. E2 is a carrier designation for a digital services with a data rate of 8.448 Mbps. E3, which interleaves four E2 channels, has a data rate of 34.368.

By default the ASM-E3 uses HDB3 line encoding. Three different mapping protocols are used to transmit ATM cells over an E3 line: Physical Layer Convergence Protocol (PLCP) and two ATM Direct Mapped (ADM) Systems. The PLCP is G.751, and the ADM protocols are G.751 and G.832. The three protocols are not compatible. Many existing E3 implementations use PLCP as defined in ANSI T1.624-1993, but many new implementations of Digital Signaling use ADM. The ASM-E3 module supports all three physical layer protocols.

The ASM-E3 is actually a sub-module, or daughtercard, that attaches to a High-Speed Module (HSM). The HSM contains memory and processing power for switching modules that operate at speeds greater than 10 Mbps. You plug your cable directly into the ASM-E3 sub-module, but it is the HSM module that connects to the switch backplane.

◆ **Note** ◆

The ASM-E3 is supported, but it has been discontinued. For E3 ATM access, the ASM2-DS3 (see *ASM2-E3* on page 7-71) is recommended.

ASM-E3 Technical Specifications	
Number of ports	1 or 2
Connector Type	BNC
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/2.0 MPOA Client ANSI T1.624-1993 (PLCP Mapping)
Data Rate	34.368 Mbps
ATM Adaption Layers	AAL5
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Max. No. of VCs Supported	1,024
Connections Supported	E3 connections to ATM carrier service.
Cable Distance	185 m
Cable Supported	Coaxial RG-59 (75 ohm)

This module includes one set of LEDs for each port. The LEDs for a given port display above the port. If the ASM module includes two ports, then the module contains two sets of LEDs. The second set of LEDs displays above the second port.

RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when the receive cable is not inserted. This LED will be on when the ASM module is plugged in, but no cable has been connected.

YEL (Yellow Alarm). On Amber when a far end receive failure occurs. The Far End Receive Failure (FERF) is defined as FERF for ADM G.832 mapping protocols, and defined as Remote Alarm Indication (RAI) for PLCP and ADM G.751 mapping protocols. The recipient of cells from this ASM is not receiving those cells. This error may be due to a transmission error by the ASM or a receive error on the other end of the link.

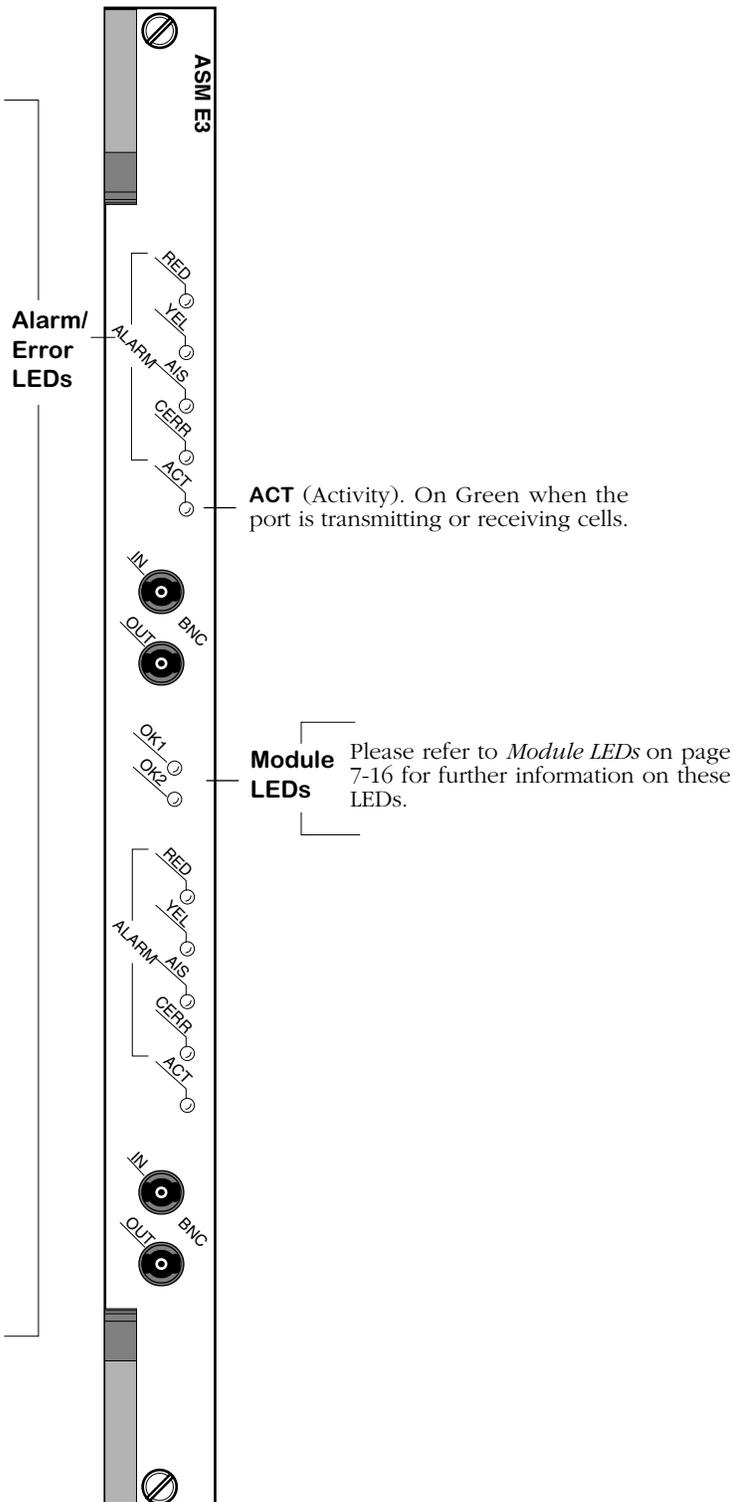
AIS (Alarm Indication Signal). On while the Alarm Indication Signal (AIS) maintenance signal is received in the frame payload of the ASM.

CERR (Cell Loss Error). Interpretation of the CERR LED depends on the mapping protocol used on this ATM port. The mapping may be ATM Direct Mapped (ADM) or Physical Layer Convergence Protocol (PLCP) and is configured through the **map** command.

If ADM is used, then the CERR LED goes on after seven consecutive cells with errors are received. It turns back off again when six consecutive cells are received without errors.

If PLCP is used, then this LED goes on when PLCP frames are out of frame for 1.2 ms. It turns back off again when no out-of-frame errors have occurred for 10 ms. In PLCP framing, ATM cells are prepended with three framing octets and a path overhead octet. A PLCP frame is considered out-of-frame when errors are detected in the first two framing octets, or in the third frame octet and the path overhead octet.

In addition, the CERR LED will be on when the receive cable is not inserted.



ATM 2-Port E3 Module

ASM-CE (Discontinued)

The ASM-CE converts traditional circuit emulation traffic from T1, E1, or serial ports to ATM cells for transport over an ATM network. This module is best employed as a means of connecting legacy Time Division Multiplexing (TDM) and synchronous serial traffic to an enterprise ATM network. It contains one ATM uplink port, two T1 or E1 ports, and two serial ports. The ATM uplink port may be factory-configured as OC-3, DS-3, or E3.

You can configure several circuit emulation parameters through switch software commands. Configurable options include service mode (structured or unstructured), clocking mode, cell delay variation, and ATM reassembly buffer size. Configuration options specifically for T1 and E1 ports include frame format, facility datalink, and line coding. In addition, the switch can store up to 24 hours of local and remote statistics for T1 and E1 ports.

ASM-CE Technical Specifications	
Number of ports	5 total 1 ATM Uplink port (OC-3, DS-3, or E3) 2 T1 or E1 ports 2 Universal Serial ports
Connector Types	ATM Uplink OC-3: SC fiber (single or multimode) DS-3 and E3: BNC T1/E1 RJ-48C
Standards Supported	RFCs 1406, 1213, 1659 ATM Forum CES-IS, version 2 ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/2.0 MPOA Client ANSI T1.624-1993 (PLCP Mapping)
Frame Formats	T1: Superframe, Extended Superframe, Unframed E1: E1, E1-CRC, E1-MF, E1-CRC-MF, Unframed
Line Coding	T1: B8ZS or AMI E1: HDB3 or AMI
Data Rates Supported	ATM Uplink OC-3: 155 Mbps DS-3: 44.736 Mbps E3: 34.368 Mbps T1: 1.544 Mbps E1: 2.048 Mbps Serial: 56, 64, 128, 256, 384, 512, 768, 1024, 1536, 1544, 2048 Kbps

continued on next page...

ASM-CE Technical Specifications (Cont.)	
Facility Datalink Protocol	ANSI T1.403 and AT&T 54016
Data Transfer Services	Structured or Unstructured
Clocking	Synchronous, SRTS, Adaptive
Virtual Circuits Supported	Permanent Virtual Circuits (PVCs) for CE traffic PVCs or (SVCs) for LAN traffic.
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Max. No. of VCs Supported	1,024
Connections Supported	Physical Data Terminal Equipment (DTE) or Data Communication Equipment (DCE)
Optical output power (fiber ports)	Multimode: -19 to -14 dBm Single mode (intermediate reach): -14 to -8 dBm
Optical receiver sensitivity (fiber ports)	Multimode: -30 to -14 dBm Single mode (intermediate reach): -31 to -8 dBm
Power Budget (fiber ports)	Multimode: 11 dB Single mode (intermediate reach): 16 dB
Cable Distance	T1/E1 (short haul): 200 meters T1/E1 (long haul): 1829 meters Multimode: 4.2 km Single mode (intermediate reach): 24 km
Cable Supported	Serial Ports: DTE or DCE in the following types: R2-232, V.35, X.21, RS-530, RS-449 Fiber ports: Multimode: 62.5 micron multimode fiber Single mode (intermediate reach): single mode fiber

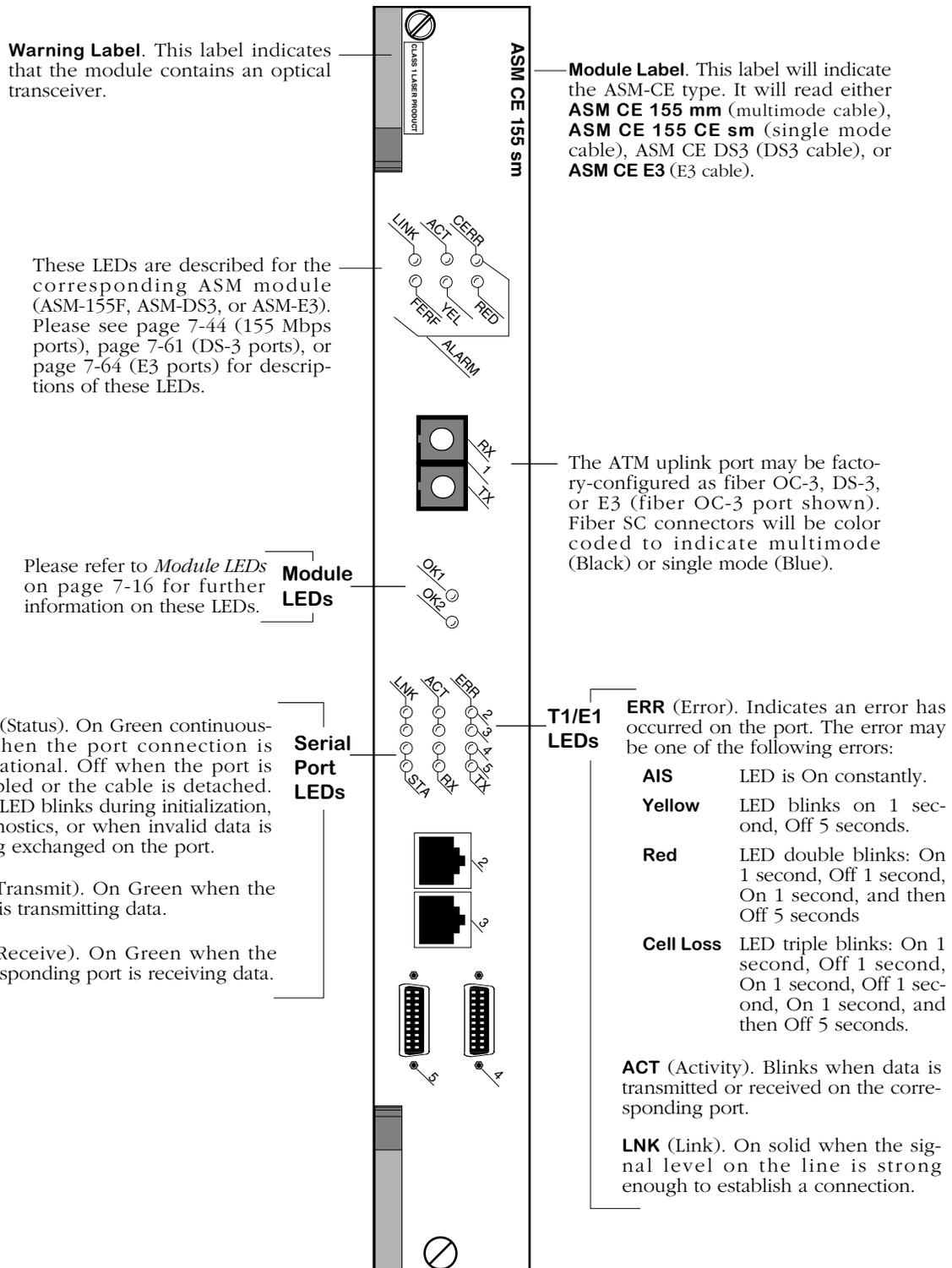
◆ Special Note ◆

The single mode version of this module is:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

This module includes three sets of LEDs. The cluster of six LEDs for the ATM uplink port are located above that port. LEDs for the T1/E1 ports and the serial ports are clustered together above those ports; the first two rows of LEDs in this cluster describe activity on the T1/E1 ports, and the second two rows describe activity on the serial ports. Each port and its corresponding LEDs are labelled.



ATM Circuit Emulation Module With OC-3 Uplink

ASM2-DS3

The ASM2-DS3 switching module contains one or two BNC ports that support DS-3 connections. The port connection provides 44.736 Mbps of bandwidth and connects to coaxial (RG-59) cable. ASM2-DS3 ports are suited for connections to ATM carrier services offered by North American Telcos. The ASM2-DS3 port is a physical DTE (Data Termination Equipment) device that connects to a physical DCE (Data Communication Equipment) device, such as a DSU (Data Service Unit). The one-port version is called the ASM2-DS3-1W; the two-port version is called the ASM2-DS3-2W. See *ASM2-DS3 Technical Specifications* on page 7-69 for more information.

DS-3 is a Digital Signal (DS) interface used to implement wide area, public connectivity for ATM networks. There is a hierarchy of DS services based on channel capacity. DS-0, the lowest bandwidth DS channel, provides 64 Kbps of throughput. Twenty-four (24) DS-0 channels combine to form a DS-1 (1.544 Mbps of throughput). Four DS-1 channels combine to form a DS-2 (6.312 Mbps of throughput). And seven DS-2 channels combine to form a DS-3 (44.736 Mbps of throughput).

By default the ASM2-DS3 uses B3ZS line encoding. Using the **dsmmod** command, you can configure the module to use C-bit parity or M23 parity and configure it for loopback controls. You should configure the ASM2-DS3 module to use the same parity as the ATM service provider.

Two different mapping protocols are used to transmit ATM cells over DS-3: PLCP (Physical Layer Convergence Protocol) and ATM Direct Mapped (ADM) System. The two protocols are not compatible. Many existing DS-3 implementations use PLCP as defined in ANSI T1.624-1993, but many new implementations of DS-3 use ADM. The ASM2-DS3 module supports both physical layer protocols.

The ASM2-DS3 is actually a submodule, or daughtercard, that attaches to a High-Speed Module (HSM). You plug your cable directly into the ASM2-DS3 submodule, but it is the HSM module that connects to the switch backplane.

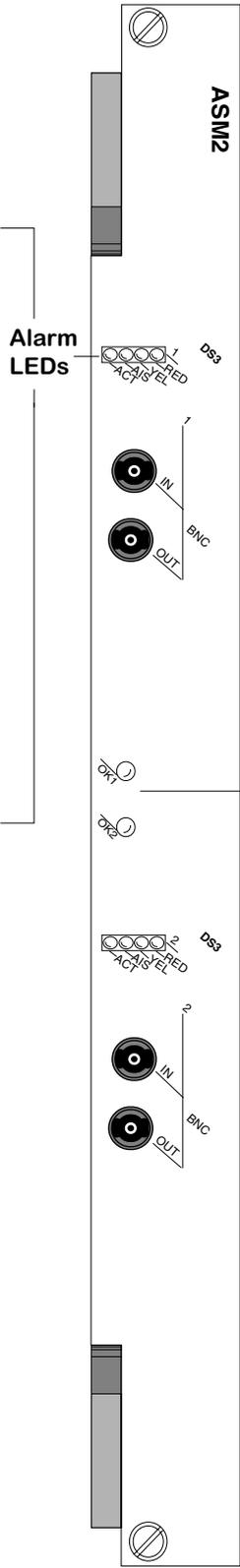
ASM2-DS3 Technical Specifications	
Number of ports	1 or 2
Connector Type	BNC
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/V2.0 ANSI T1.624-1993 (PLCP Mapping) MPOA Client
Data Rate	44.736 Mbps
ATM Adaption Layers	AAL5
MAC Addresses Supported	4096
Max. No. of VCs Supported	1,024
Connections Supported	DS-3 connections to ATM carrier service.
Cable Supported	Coaxial RG-59 (75 ohm)
Cable Distance	185 m
Current Draw	1-port: 4.0 amps 2-port: 5.5 amps

RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the ASM module is plugged in, but no cable has been connected.

YEL (Yellow Alarm). On Amber when a far end receive failure occurs. The recipient of cells from this ASM is not receiving those cells. This error may be due to a transmission error by the ASM or a receive error on the other end of the link.

AIS (Alarm Indication Signal). On when a maintenance signal is sent to the ASM by the network. If this LED is on, then there has been a change in the Alarm Indication Signal (AIS).

ACT (Activity). On Green when the port is transmitting or receiving cells.



Alarm LEDs

Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

ATM DS-3 Uplink Module

ASM2-E3

The ASM2-E3 switching module contains one or two BNC ports that support E3 connections. Each port connection provides 34.368 Mbps of bandwidth and connects to coaxial (RG-59) cable. ASM2-E3 ports are suited for connections to ATM carrier services offered by International Telcos. The ASM2-E3 port is a physical DTE (Data Termination Equipment) device that connects to a physical DCE (Data Communication Equipment) device, such as a DSU (Data Service Unit). The one-port version is called the ASM2-DS3-1W; the two-port version is called the ASM2-DS3-2W. See *ASM2-E3 Technical Specifications* on page 7-72 for more information.

E3 is a designation used by Telcos to indicate the capacity of a digital service. E3 actually multiplexes two smaller types of digital service lines (E1 and E2) to reach its channel capacity. E1 is a carrier designation for a digital service with a data rate of 2.048 Mbps. E2 is a carrier designation for a digital services with a data rate of 8.448 Mbps. E3, which interleaves four E2 channels, has a data rate of 34.368.

By default the ASM2-E3 uses HDB3 line encoding. Three different mapping protocols are used to transmit ATM cells over an E3 line: Physical Layer Convergence Protocol (PLCP) and two ATM Direct Mapped (ADM) Systems. The PLCP is G.751, and the ADM protocols are G.751 and G.832. The three protocols are not compatible. Many existing E3 implementations use PLCP as defined in ANSI T1.624-1993, but many new implementations of Digital Signaling use ADM. The ASM2-E3 module supports all three physical layer protocols. To configure E3 parameters, use the **dsmod** command.

The ASM2-E3 is actually a submodule, or daughtercard, that attaches to an High-Speed Module (HSM). You plug your cable directly into the ASM2-E3 submodule, but it is the HSM module that connects to the switch backplane

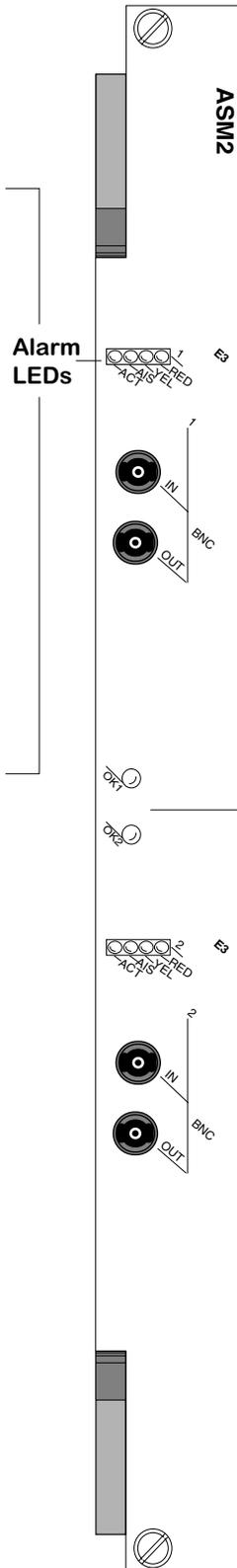
ASM2-E3 Technical Specifications	
Number of ports	1 or 2
Connector Type	BNC
Standards Supported	ATM Forum User-to-Network Interface 3.1 and 3.0 ISO Q.2931 IAB RFC 1483 (Multiprotocol Point-to-Point Encapsulation over ATM) IAB RFC 1577 (Classical IP over ATM) IAB RFC 1755 (Signaling guidelines for Classical IP) ATM LAN Emulation Client V1.0/V2.0 ANSI T1.624-1993 (PLCP Mapping) MPOA Client)
Data Rate	34.368 Mbps
ATM Adaption Layers	AAL5
MAC Addresses Supported	4096
Max. No. of VCs Supported	1,024
Connections Supported	E3 connections to ATM carrier service.
Cable Supported	Coaxial RG-59 (75 ohm)
Cable Distance	185 m
Current Draw	1-port: 4.0 amps 2-port: 5.5 amps

RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the ASM module is plugged in, but no cable has been connected.

YEL (Yellow Alarm). On Amber when a far end receive failure occurs. The recipient of cells from this ASM is not receiving those cells. This error may be due to a transmission error by the ASM or a receive error on the other end of the link.

AIS (Alarm Indication Signal). On when a maintenance signal is sent to the ASM by the network. If this LED is on, then there has been a change in the Alarm Indication Signal (AIS).

ACT (Activity). On Green when the port is transmitting or receiving cells.



Alarm LEDs

Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

ATM E3 Uplink Module

Token Ring Modules

The Token Ring modules support Station, Lobe, Ring Out Only, and Ring In/Ring Out configurations. Module ports can connect existing Token Ring MAUs, hubs, and devices. In addition, the Token Ring fiber module supports specialized hub connections—Ring Out Only and Ring In/Ring Out—to Synoptics (Bay), IBM, ODS, and Bytex hubs. The Token Ring modules are as follows:

- TSM-C-6 Six port UTP or STP Station connections. **(Discontinued)**
- TSM-F-6 Six-port fiber that supports Station, Lobe, Ring Out, Ring In/Ring Out connections.
- TSM-CD-6 Six-port UTP or STP that supports Station or Lobe connections. **(Discontinued)**
- TSM-CD-16W Sixteen-port UTP or STP that supports Station or Lobe connections.

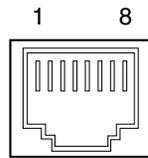
The TSM-C-6 allows you to connect existing Token Ring MAUs and hubs to your OmniSwitch network and extend Token Ring devices over Fast Ethernet, or ATM backbones.

The TSM-F-6 allows you to configure all ports in the module s Station or Lobe connections. The TSM-CD-6 and TSM-CD-16W allow you to configure individual ports as Station or Lobe connections. As a Station port, you can connect existing Token Ring MAUs and hubs to your OmniSwitch network and extend Token Ring devices over Fast Ethernet, or ATM backbones. As a Lobe port, you can connect high-traffic Token Ring workstations or servers directly to an OmniSwitch and provide the full 4 or 16 Mbps of bandwidth to that single device. In addition, the TSM-F-6 allows you to connect in Ring Out Only mode or Ring In/Ring Out mode to Synoptics, IBM, ODS, and Bytex hubs.

Token Ring ports are configurable through software. You can set the ring speed (4 or 16 Mbps), active monitor participation, and frame copied bit variables for all ports. In addition, a variety of error and configuration statistics are available through software commands. See Chapter 21, “Managing Token Ring Modules,” for further information on software configuration and monitoring commands.

Token Ring Pinouts

The figure and table below illustrate the pinouts for a Token Ring RJ-45 port.



Token Ring RJ-45 Specifications	
Pin Number	Standard Signal Name
1	Not used
2	Not used
3	TX -
4	RX +
5	RX -
6	TX +
7	Not used
8	Not used

TSM-C-6 (Discontinued)

The TSM-C-6 contains six active ports that may support either unshielded twisted pair (UTP) or shielded twisted pair (STP) connections. Each active port connects to a Lobe port on an MAU, so the TSM port acts as a Token Ring station. The ports each support a fully switched connection at either 4 or 16 Mbps. The Ring Speed is configurable through software.

The TSM-C-6 is actually a sub-module, or daughtercard, that attaches to a High-Speed Module (HSM). The HSM contains memory and processing power for switching modules that operate at speeds greater than 10 Mbps. You plug your cable directly into the TSM-C-6 sub-module, but it is the HSM module that connects to the switch backplane.

Note

The TSM-C-6 is supported, but it has been discontinued. For copper-based Token Ring switching, the TSM-CD-16W module (see *TSM-CD-16W* on page 7-85) is recommended.

TSM-C-6 Technical Specifications	
Number of ports	6 Station Ports
Connector Type	Shielded RJ-45 (UTP or STP)
Standards Supported	IEEE 802.5 IAB RFC 1231
Data Rate	4 or 16 Mbps
Maximum Frame Size	4,472 bytes
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	Lobe port on MAU or hub acting as device
Cable Supported	Shielded twisted pair (STP) <ul style="list-style-type: none">• IBM Type 1 Unshielded twisted pair (UTP) <ul style="list-style-type: none">• IBM Type 3• ANSI category 3, 4, or 5
Cable Distance	100 m

This module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number. The TSM module includes a total of six ports with one set of LEDs for the top three ports and a second set of LEDs for the bottom set of ports.

BCN (Beacon Detect). On Yellow when this port is inoperable because of a hard error and the beacon recovery process is in effect.

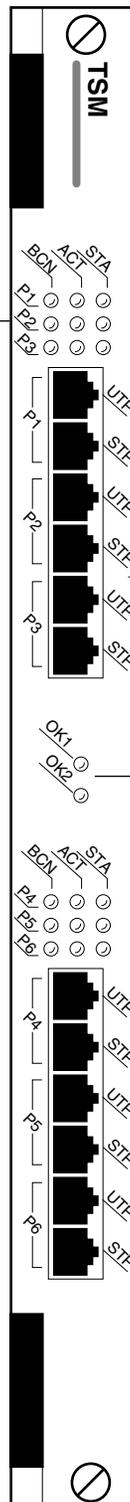
ACT (Activity). On Green when the port is transmitting or receiving frames on the ring.

STA (Link Status/Disabled). On Green when attached to a working network. Off when not attached to a network. Flashing Green when the port is initializing.

Port LEDs

Each port contains an unshielded twisted pair (UTP) and a shielded twisted pair (STP) connector. You can use the UTP or STP connector on each port, but not both.

Module LEDs Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.



Token Ring Single Mode 6-Port Module

TSM-F-6

The TSM-F-6 contains six multimode fiber ports that may be configured to operate as Station, Lobe, Ring Out Only, or Ring In/Ring Out ports. Ports are configured through software, but all ports on a module are set to the same interface type. The ports each support a fully switched connection at either 4 or 16 Mbps. The Ring Speed is individually configurable through software. See Chapter 21, “Managing Token Ring Modules,” for information on software commands.

The TSM-F-6 is actually a sub-module, or daughtercard, that attaches to a High-Speed Module (HSM). The HSM contains memory and processing power for switching modules that operate at speeds greater than 10 Mbps. You plug your cable directly into the TSM-F-6 sub-module, but it is the HSM module that connects to the switch backplane.

TSM-F-6 Technical Specifications	
Number of ports	6 Lobe or Station Ports
Connector Type	ST
Standards Supported	IEEE 802.5j IAB RFC 1231
Data Rate	4 or 16 Mbps
Maximum Frame Size	4,472 bytes
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	Lobe port, station port, Ring Out Only, or Ring In/Ring Out (RI/RO) port
Optical output power	-19 to -12 dBm
Optical receiver sensitivity	-31 to -11 dBm
Power Budget	13 dB
Cable Supported	62.5/125 micron multimode fiber cable 50/100 micron multimode fiber cable
Cable Distance	2 km

This module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number. The TSM module includes a total of six ports with one set of LEDs for the top three ports and a second set of LEDs for the bottom set of ports. (Ring In/Ring Out configurations use only the top three rows of LEDs because only three logical ports exist.)

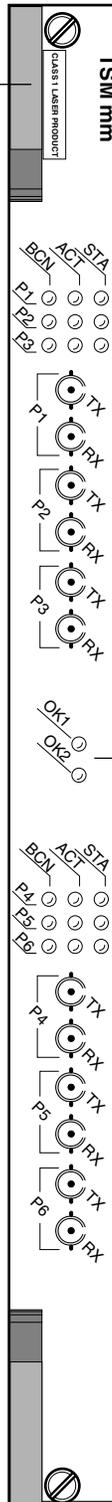
Warning Label. This label indicates that the module contains an optical transceiver.

BCN (Beacon Detect). On Yellow when this port is inoperable because of a hard error and the beacon recovery process is in effect.

ACT (Activity). On Green when the port is transmitting or receiving frames on the ring.

STA (Link Status/Disabled). On Green when attached to a working network. Off when not attached to a network. Flashing Green when the port is initializing.

Port LEDs



Module LEDs Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

Token Ring 6-Port Fiber Module

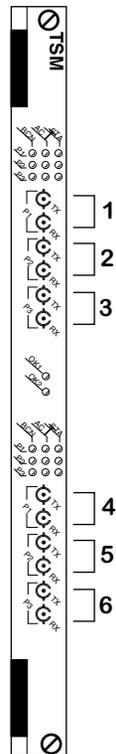
TSM-F-6 Port Configurations

The TSM-F-6 ports may be configured as a Station, Lobe, Ring Out Only, or Ring In/Ring Out ports. The Ring Out Only and Ring In/Ring Out configurations each contain options for IBM, Synoptics (Bay Networks) and Bytex hubs. You configure these ports through the Token Ring Interface menu, which is described in Chapter 21, "Managing Token Ring Modules." The following sections show how ports are handled in each configuration option.

◆ Note ◆

If TSMF-6 ports are configured to support either Source Routing (SR) or Source Route Transparent (SRT) operation, then these ports should be connection an IBM Ring In *or* Ring Out on the concentrator, but not to both.

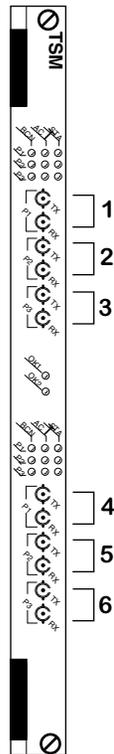
Station or Lobe Ports



When ports are used in a Station or Lobe interface, each port operates independently. In total, there are 6 ports with the assignments shown in the figure to the left. There are two configuration options that can be chosen through software:

- Station 802.5j Interface
- Lobe 802.5j Interface

Ring Out Only



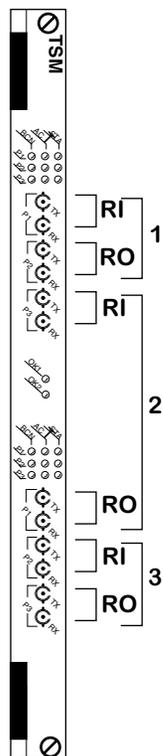
When ports are used in a Ring Out Only interface, each port operates as a Ring Out Port. In total, there are 6 Ring Out ports with the assignments shown in the figure to the left.

There are three configuration options that can be chosen through software for the Ring Out (RO) interface:

- IBM RO Ports Interface
- Synoptics RO Ports Interface
- Bytex RO Ports Interface

In the Ring Out Only configuration, the TX port on the TSM-F-6 should connect directly to the Ring In (RI) port on a Bytex or Synoptics (Bay) hub. The Ring Out (RO) ports on the hub should not be connected.

Ring In/Ring Out



When ports are used in a Ring In/Ring Out (RI/RO) interface, two fiber ports act as a RI/RO port pair. In total, the module provides three RI/RO port pairs and each pair operates as a single switch port. Only the top three rows of LEDs are used in this configuration.

There are three configuration options that can be chosen through software for the RI/RO interface:

- IBM RI/RO Ports Interface
- Synoptics RI/RO Ports Interface
- Bytex RI/RO Ports Interface

The following list describes the RI/RO function and port number for each port labelled on the TSM-F-6:

<u>Port Number</u>	<u>Function</u>	<u>Logical Port</u>	<u>To Hub</u>
P1	RI	1	RO
P2	RO	1	RI
P3	RI	2	RO
P4	RO	2	RI
P5	RI	3	RO
P6	RO	3	RI

TSM-CD-6 (Discontinued)

The TSM-CD-6 contains six shielded ports that each may be separately configured as a Station or Lobe port. As a Station port, the TSM-CD-6 port plugs directly into a MAU; as a Lobe port, the port acts as an MAU port and a Token Ring station plugs directly into the module. You configure the ports as Station or Lobe through the **tsc** command. By default, ports are configured as Lobe ports. See Chapter 21, “Managing Token Ring Modules,” for more information.

Each port can support either unshielded twisted pair (UTP) or shielded twisted pair (STP) connections. No configuration is necessary to set up a port for UTP or STP.

Each port supports a fully switched connection at either 4 or 16 Mbps. Ring Speed is configurable through the **tpcfg** command. By default, ports are configured at 16 Mbps.

◆ Warning ◆

If a TSM-CD-6 is hot swapped, it will restart itself every time IPX is started.

Automatic Speed Detection. Switch software will automatically modify the Ring Speed if there is a discrepancy with the ring to which the port is connected. A TSM-CD-6 port detects this difference in Ring Speed as it is inserted into the ring, then it resets itself and comes up in the new Ring Speed. (The new Ring Speed, however, is not saved in the system configuration file, **mpm.cfg**.) Once the port inserts into the ring, automatic Ring Speed detection is disabled (i.e., thereafter the port will not change speed automatically). Both Station and Lobe ports handle automatic speed detection this way.

If a TSM-CD-6 port is the first device on the ring, then the Ring Speed is automatically set to the port’s configured speed. The port does not reset to match the Ring Speed—its speed becomes the Ring Speed. If the port is not the first device, then it will auto-detect the ring speed and match that speed as described in the preceding paragraph.

The TSM-CD-6 is actually a sub-module, or daughtercard, that attaches to a High-Speed Module (HSM). The HSM contains memory and processing power for switching modules that operate at speeds greater than 10 Mbps. You plug your cable directly into the TSM-CD-6 sub-module, but it is the HSM module that connects to the switch backplane.

◆ Note ◆

The TSM-CD-6 is supported, but it has been discontinued. For copper-based Token Ring switching, the TSM-CD-16W module (see *TSM-CD-16W* on page 7-85) is recommended.

TSM-CD-6 Technical Specifications	
Number of ports	6 Station or Lobe Ports
Connector Type	Shielded RJ-45 (UTP or STP)
Standards Supported	IEEE 802.5 IAB RFC 1231
Data Rate	4 or 16 Mbps
Maximum Frame Size	4,472 bytes
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	Station or Lobe port
Cable Supported	Shielded twisted pair (STP)—100 or 150 ohm. Unshielded twisted pair (UTP)—100 ohm.
Cable Distance	100 m

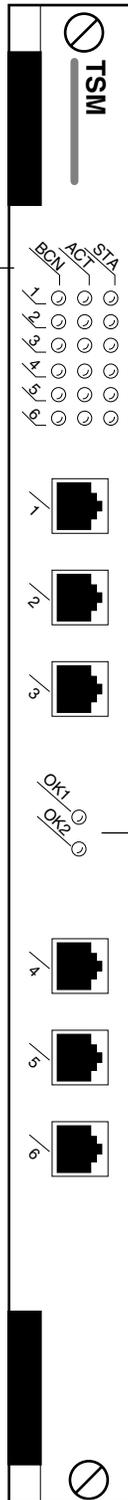
The module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number.

BCN (Beacon Detect). On Yellow when this port is inoperable because of a hard error and the beacon recovery process is in effect.

ACT (Activity). On Green when the port is transmitting or receiving frames on the ring.

STA (Link Status/Disabled). On Green when attached to a working network. Off when not attached to a network. Flashing Green when the port is initializing.

Port LEDs



Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

Token Ring Dual Mode 6-Port Module

TSM-CD-16W

The TSM-CD-16W contains sixteen (16) auto-sensing ports, each supporting a fully-switched 4 or 16 Mbps connection in either full- or half-duplex mode.

The TSM-CD-16W also allows you to configure individual ports as either Station or Lobe connections. As a Station connection, a port can be used to connect existing Token Ring MAUs and hubs to your OmniSwitch network. As a Lobe connection, a port can be used to connect OmniSwitches to high-traffic Token Ring workstations or servers.

◆ Important Note ◆

Although the TSM-CD-16W offers similar functionality to the Omni Switch/Router TSX-CD-16W module, the TSM-CD-16W is compatible *only* with the OmniSwitch chassis. (Note that OmniSwitch modules are distinguished by the letter **M** in the module name on the front panel, whereas Omni Switch/Router modules are distinguished by the letter **X**.)

In addition, the TSM-CD-16W is intended for use *only* with MPM-1G or MPM-III management processor modules.

Each port in the TSM-CD-16W is auto-sensing [i.e., each port can automatically detect Ring Speed (4 or 16 Mbps), Port Mode (Station or Lobe), and Duplex Mode (half or full) and then reconfigure itself to match the ring's parameters]. You can enable or disable auto-sensing via the **tpcfg** command.

If a TSM-CD-16W port is the first device inserted into the ring and auto-sensing has been enabled, it will auto-sense the ring speed every 18 seconds, or until another device is inserted into the ring. However, if the port is *not* the first device in the ring (and auto-sensing has been enabled), it will auto-detect the existing ring speed and reconfigure itself to conform to that speed. (Note that the new ring speed is *not* saved in the system configuration file, **mpm.cfg**.)

Once a port has been inserted into the ring, automatic ring speed detection will become disabled (i.e., the port will no longer reset its speed automatically).

◆ Note ◆

The automatic speed detection information described above applies to both Station and Lobe connections.

If auto-sensing has been disabled, you can manually configure an individual port's parameters via the **tpcfg** command [These parameters include Ring Speed (4 or 16 Mbps), Port Mode (Station or Lobe), and Duplex Mode (half or full)].

For more information on the **tpcfg** command, see Chapter 21, "Managing Token Ring Modules."

TSM-CD-16W Technical Specifications	
Ports	16
Connector Type	RJ-45
Standards Supported	IEEE 802.5r, IAB RFC 1231
Data Rate	4 or 16 Mbps (full- or half duplex)
Maximum Frame Size	8,144 bytes
MAC Addresses Supported	4,096
Connections Supported	Station or Lobe connections
Cables Supported	Unshielded twisted pair (UTP)—100 ohm Shielded twisted pair (STP)—100 or 150 ohm
Current Draw	8.0 amps
Cable Distance	100 m

OK1 LED (Hardware Status). This dual-state LED displays Green when the switch has passed hardware diagnostic tests that are initiated at boot-up.

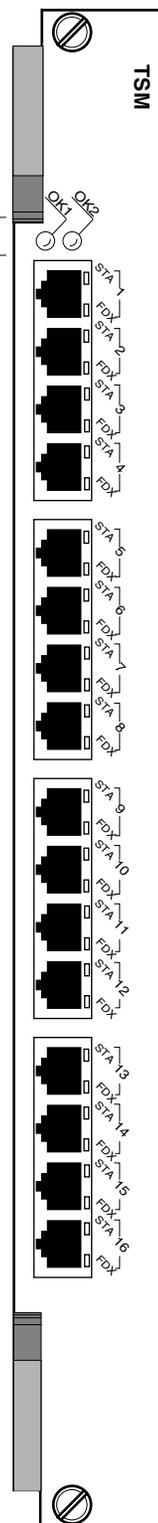
The **OK1** LED displays Amber when the hardware has failed diagnostic tests.

OK2 LED (Software Status). This dual-state LED displays Green when software has loaded successfully and the module is ready to execute commands.

The **OK2** LED blinks Amber when the switch is in a transitional state, such as when it first boots up. [If the **OK2** LED blinks Amber for an extended period of time (i.e., more than a minute), you should reboot the switch.]

The **OK2** LED displays solid Amber when software was not loaded successfully.

Module LEDs



Port LEDs

Port LEDs (Port Connection Status). There are two (2) port LEDs located directly above each port. Definitions for these LEDs are given below.

STA (Link Status). Displays Green when the corresponding port has a valid physical link and a signal is present. Under normal conditions, this LED should always display Green whenever a cable is connected.

FDX (Full-Duplex Status). Displays Green when the corresponding port is operating in full-duplex mode.

16-Port Token Ring Switching Module

Original 10 Mbps Ethernet Modules

The 10 Mbps Ethernet switching modules provide a variety of connection options. Each switch port supports one Ethernet segment. You can choose from modules with copper, fiber, or Telco connectors. Port densities range from six (6) to 12 ports per module. The six-port option allows you to mix and match Ethernet connector types (AUI, RJ-45, fiber ST, and BNC).

◆ **Note** ◆

See *High-Density, 10/100, and Gigabit Ethernet Modules* on page 7-17 for high-density, 10/100, and Gigabit Ethernet modules.

You can connect a hub or a single device to an Ethernet switching module port. If you connect a hub, you can gradually decrease the number of devices connecting to that switch port as bandwidth requirements increase. High-traffic network devices, such as network servers, can connect directly into a single dedicated switch port using the full 10 Mbps of bandwidth available. The switch will automatically sense if only one device is attached to a port and optimize it to receive only traffic destined for the address of that device.

Ethernet modules include the following:

- ESM-C-12 Twelve 10BASE-T connections using RJ-45 ports. (**Discontinued**)
- ESM-C-8 Eight 10BASE-T connections using RJ-45 ports. (**Discontinued**)
- ESM-F-8 Eight 10BASE-FL connections using fiber (ST) ports. (**Discontinued**)
- ESM-T-12 One Telco connector supporting 12 ports. (**Discontinued**)
- ESM-U-6 Universal Ethernet module supporting six connections that may be a combination of AUI (full- or half-duplex), RJ-45, fiber, or BNC ports.

Each of these modules is illustrated and described in this section.

◆ **Note** ◆

See *Ethernet Pinouts* on page 7-17 for information on Ethernet RJ-45 pinouts.

ESM-C-12 (Discontinued)

The ESM-C-12 Ethernet switching module contains 12 10BASE-T ports. Each port connection supports one switched Ethernet segment at the full 10 Mbps of bandwidth. The 12 RJ-45 ports may connect to unshielded twisted pair (UTP) or shielded twisted pair (STP) cable. Each port may connect to a single high-traffic device, such as a mail or file server, or a hub serving multiple devices. In a fully populated 5-slot switch, you could have up to 48 switched Ethernet connections, and in a fully populated 9-slot switch you could have up to 96 switched connections.

ESM-C-12 Technical Specifications	
Number of ports	12
Connector Type	RJ-45 (MDD)
Standards Supported	IEEE 802.3, 802.3i; IAB RFCs 826, 894, 1398
Data Rate	10 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	10BASE-T hub or device
Cable Supported	Unshielded twisted-pair (UTP) Shielded twisted-pair (STP)—100 ohm
Cable Distance	100 m

This ESM module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number.

STA (Status). On Green continuously when a good cable connection exists, per the 10BASE-T specification, to a 10BASE-T device. Off when a good connection does not exist. Flashes Green slowly when the port has been disabled.

ACT (Activity). On Green when data is transmitted or received on the corresponding port.

COL (Collision). Flashes amber when a collision has been detected on the port.

Port LEDs

Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.



Ethernet 12-Port UTP/STP Module

ESM-C-8 (Discontinued)

The ESM-C-8 Ethernet switching module contains eight 10BASE-T ports. Each port connection supports one switched Ethernet segment at the full 10 Mbps of bandwidth. The eight RJ-45 ports may connect to unshielded twisted pair (UTP) or shielded twisted pair (STP) cable. Each port may connect to a single high-traffic device, such as a mail or file server, or a hub serving multiple devices. In a fully populated 5-slot switch, you could have up to 32 switched Ethernet connections, and in a fully populated 9-slot switch you could have up to 64 switched connections.

Note

The ESM-C-8 is supported, but it has been discontinued. For 10BASE-T switching, the ESM-C-16 or ESM-C-32 modules are recommended.

ESM-C-8 Technical Specifications	
Number of ports	8
Connector Type	RJ-45 (MDI)
Standards Supported	IEEE 802.3, 802.3i; IAB RFCs 826, 894, 1398
Data Rate	10 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	10BASE-T hub or device; half-duplex Ethernet-to-Ethernet
Cable Supported	Unshielded twisted-pair (UTP) Shielded twisted-pair (STP)—100 ohm
Cable Distance	100 m

This ESM module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number.

STA (Status). On Green continuously when a good cable connection exists, per the 10BASE-T specification, to a 10BASE-T device. Off when a good connection does not exist. Flashes Green slowly when the port has been disabled.

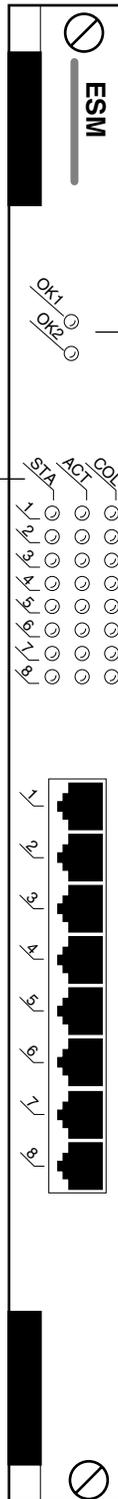
ACT (Activity). On Green when data is transmitted or received on the corresponding port.

COL (Collision). Flashes amber when a collision has been detected on the port.

Port LEDs

Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.



Ethernet 8-Port Module (Discontinued)

ESM-F-8

The ESM-F-8 Ethernet switching module contains eight 10BASE-FL ports. Each port connection supports one switched Ethernet segment at the full 10 Mbps of bandwidth. The eight dual ST connector ports connect to multimode fiber optic cable. Each port may connect to a single high-traffic device, such as a mail or file server, or a hub serving multiple devices. In a fully populated 5-slot switch, you could have up to 32 switched Ethernet connections, and in a fully populated 9-slot switch you could have up to 64 switched connections.

ESM-F-8 Technical Specifications	
Number of ports	8
Connector Type	ST
Standards Supported	IEEE 802.3, 802.3i; IAB RFCs 826, 894, 1398
Data Rate	10 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	10BASE-FL hub or device; half-duplex Ethernet-to-Ethernet
Optical output power	-20 to -12 dBm
Optical receiver sensitivity	-32.5 to -12 dBm
Power Budget	12.5 dB
Cable Supported	62.5 micron multimode fiber (13 dBm)
Cable Distance	2 km

Warning Label. This label indicates that the module contains an optical transceiver.

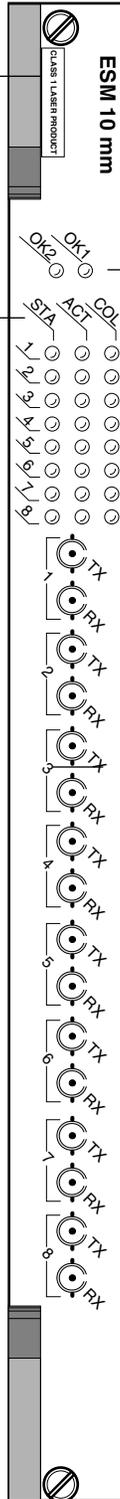
This ESM module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number.

STA (Status). On Green continuously when a good cable connection exists, per the 10BASE-FL specification, to a 10BASE-FL device. Off when a good connection does not exist. Flashes Green slowly when the port has been disabled.

ACT (Activity). On Green when data is transmitted or received on the corresponding port.

COL (Collision). Flashes amber when a collision has been detected on the port.

Port LEDs



Module Label. This label will indicate the ESM-F-8 type. It will read either **ESM 10 mm** (multimode cable), or **ESM 10 sm** (single mode cable).

Module LEDs Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

Ethernet 8-Port Fiber Module

ESM-T-12 (Discontinued)

The ESM-T-12 Ethernet switching module contains one 50-pin connector that supports 12 switched Ethernet ports. Each of the 12 ports uses the full 10 Mbps of dedicated bandwidth. The 50-pin RJ-21 connector provides a convenient cabling solution for networks with existing punch down blocks and patch panels. Each port may connect to a single high-traffic device, such as a mail or file server, or a hub serving multiple devices. In a fully populated 5-slot switch, you could have up to 48 switched Ethernet connections, and in a fully populated 9-slot switch you could have up to 96 switched connections.

ESM-T-12 Technical Specifications	
Number of ports	One Telco supporting 12 end devices
Connector Type	Telco 50-pin (RJ-21)
Standards Supported	IEEE 802.3, 802.3i; IAB RFCs 826, 894, 1398
Data Rate	10 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	Telco patch panel or punch down block
Cable Supported	Unshielded twisted pair (UTP) Shielded twisted pair (STP)—100 ohm
Cable Distance	100 m

This ESM module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number.

STA (Status). On Green continuously when a good cable connection exists, per the 10BASE-T specification, to a 10BASE-T device. Off when a good connection does not exist. Flashes Green slowly when the port has been disabled.

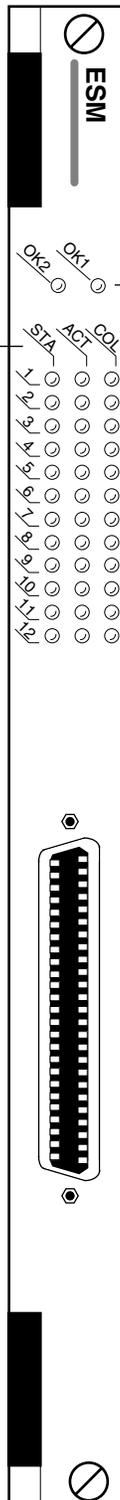
ACT (Activity). On Green when data is transmitted or received on the corresponding port.

COL (Collision). Flashes amber when a collision has been detected on the port.

Port LEDs

Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.



Ethernet 12-Port Telco Module

ESM-U-6

The Ethernet Universal switching module has six positions in which you can mix and match different Ethernet media. The media options are as follows:

- 10BaseFL fiber optic ST (single mode or multimode)
- 10Base2 thin coax BNC
- 10BaseT UTP RJ-45
- Combined 10Base5 thick coax AUI and 10BaseT UTP RJ-45 (occupies two positions)
- 10Base5 thick coax AUI (full-duplex)

Each port connection supports one switched Ethernet segment at the full 10 Mbps of bandwidth. Depending on the connector types with which the ESM-U is configured, each port connector may connect to the following cable types: multimode fiber optic, single mode fiber optic, thin coaxial, unshielded twisted pair (UTP), or thick coaxial. Each port may connect to a single high-traffic device, such as a mail or file server, or a hub serving multiple devices.

ESM-U Technical Specifications	
Number of ports	6
Connector Type	Combinations of dual-fiber (ST), BNC, RJ-45 and AUI
Standards Supported	IEEE 802.3, 802.3i; IAB RFCs 826, 894, 1398
Data Rate	10 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	10BASE-FL, 10BASE-2, AUI-based transceiver, or 10BASE-T hubs or device; Half-duplex Ethernet-to-Ethernet with full-duplex support for AUI connections.
Cable Supported	62.5 micron multimode fiber optic 9 micron single mode fiber optic Thin coaxial Thick coaxial Unshielded twisted pair (UTP)
Cable Distance	Multimode Fiber: 2 kilometers Single Mode Fiber: 5.7 kilometers Long-Reach Single Mode Fiber: 28.0 kilometers ThinNet: 185 meters over RG58 cable ThickNet: 50 meters UTP: 100 meters over 100 ohm Category 3

◆ Special Note ◆

The single mode fiber adapter used with the ESM-U-6 has been deemed:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

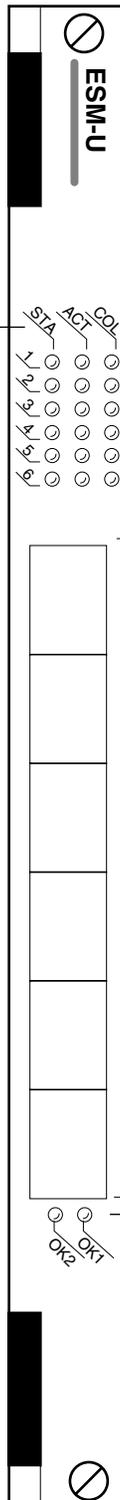
This ESM module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number.

STA (Status). On Green continuously when a good cable connection exists to a network device. Off when a good connection does not exist. Flashes Green slowly when the port has been disabled.

ACT (Activity). On Green when data is transmitted or received on the corresponding port.

COL (Collision). Flashes amber when a collision has been detected on the port.

Port LEDs



Connector Slots

Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

Ethernet 6-Port Universal Switching Module

Original Fast Ethernet (100 Mbps) Modules (Discontinued)

Fast Ethernet switching modules provide a variety of connection options. You can choose from copper or fiber (SC) connectors running at full or half-duplex. Ethernet 100 Mbps modules can each support two fully switched ports. The copper UTP option allows you to divide a switched port into a single collision domain of four ports that share the 100 Mbps of bandwidth.

◆ Note ◆

The modules described in this section are still supported but they have been discontinued. See *High-Density, 10/100, and Gigabit Ethernet Modules* on page 7-17 for current high-density, 10/100, and Gigabit Ethernet modules.

You can connect a hub, single device, or backbone to an Ethernet switching module port. If you connect a hub, you can gradually decrease the number of devices connecting to that switch port as bandwidth requirements increase. High-traffic network devices, such as network servers, can connect directly into a single dedicated switch port using the full 100 Mbps of bandwidth available. The switch will automatically sense if only one device is attached to a port and optimize it to receive only traffic destined for the address of that device. Fiber-port modules are suited for backbone connections in networks where Fast Ethernet is used as the backbone media.

Fast Ethernet modules include the following:

- ESM-100C Four or eight 100BASE-Tx connections using RJ-45 ports. **(Discontinued)**
- ESM-100C-FD One or two full-duplex 100BASE-Tx connections using RJ-45 ports. **(Discontinued)**
- ESM-100F x -FD One or two full-duplex 100BASE-Fx fiber connections (single mode or multimode) using SC connectors. **(Discontinued)**
- ESM-100C-5 Five 100BASE-Tx connections using RJ-45 ports. One of the five ports supports full-duplex operation; the other four ports share a 100Base-Tx connection.
- ESM-100CF x -5 One fiber 100BASE-Fx connection and four shared 100Base-Tx connections. The fiber port supports full-duplex operation and can be configured with single mode or multimode connectors. **(Discontinued)**

Each of these modules is illustrated and described in this section.

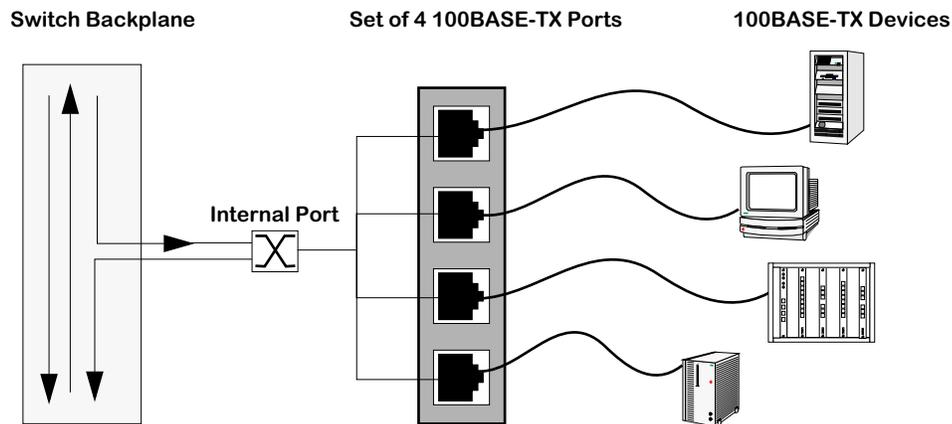
◆ Note ◆

See *Ethernet Pinouts* on page 7-17 for information on Ethernet RJ-45 pinouts.

ESM-100C (Discontinued)

The ESM-100C can be configured with four or eight ports that connect to 100Base-Tx devices. Each set of four ports is one collision domain that connects to a fifth internal port. This internal port connects directly to the switch backplane and has a unique MAC address.

Each front panel port on the ESM-100C is capable of using the full 100 Mbps of dedicated bandwidth. However, when more than one connection is made to each set of four ports, those connections must share the 100 Mbps of bandwidth. Front panel ports receive data from attached 100BaseTx devices and from the fifth internal port (which connects to the switch backplane). In addition, data received on any front panel port is automatically passed on to the other three ports that share its collision domain and to the internal port.



The internal switch port receives data from the switch backplane and the 100Base-Tx front panel ports. This port passes data destined for the front panel ports (from other switch ports) in one direction, and passes data destined for other switch ports (from the front panel ports) in the other direction. This internal port has its own set of LEDs, separate from the front panel port LEDs.

ESM-100C Technical Specifications	
Number of ports	4 or 8
Connector Type	RJ-45
Standards Supported	IEEE 802.3u (100Base-Tx)
Data Rate	100 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	100Base-Tx hub or device
Cable Supported	Unshielded twisted-pair (UTP), Category 5 EIA/TIA 568
Cable Distance	100 m

There are two versions of the ESM-100C front panel design. The difference between the two is in how LEDs are organized. Internal port LEDs are separated from front panel port LEDs. Both versions of the front panel are shown on the following pages.

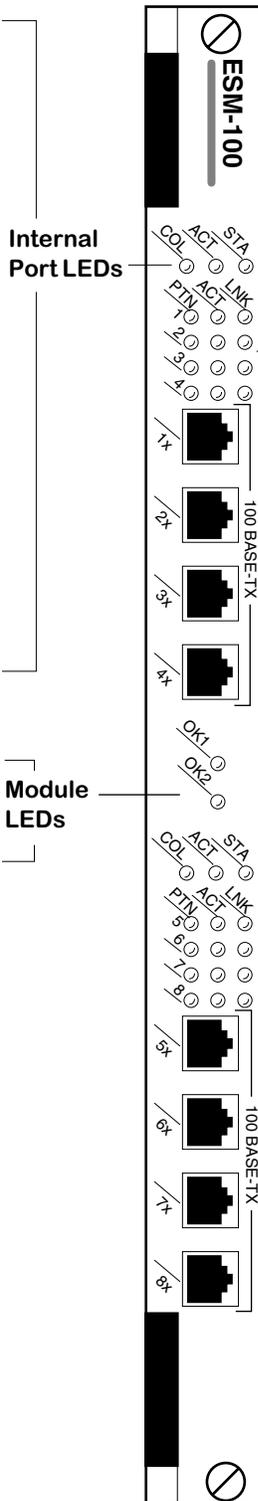
The module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number. If the ESM module includes a total of eight ports, then the module contains two sets of five rows of LEDs. The second set of LEDs displays above the second set of ports.

COL. Flashes amber when a collision has been detected on the internal port. A collision here is defined as two or more ports receiving data at the same time. The ports included in this collision domain include the four front panel ports plus the internal port connected to the switch backplane. A collision may occur when data is received simultaneously on two front panel ports or when data is received on a front panel port and the internal port attached to the switch backplane simultaneously.

ACT. On Green when data is received from the switch backplane that is destined for one of the front panel ports.

STA. On Green when the internal port has a valid connection to the switch backplane and has been initialized. This connection can be disabled via software.

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.



PTN. On amber when excessive collisions have forced the port to be partitioned. A port will partition after 64 collisions have occurred. Partitioning the port allows the other three ports to receive data again. Only one of the four front panel ports can receive data at one time. Therefore, partitioning a port that is creating a bottleneck with excessive collisions clears the data path so that the other three ports can receive data.

ACT. On Green when data is received on the corresponding port. After receiving data, the receiving port automatically transmits the data to the other three front panel ports.

LNK. On Green continuously when a good cable connection to a 100Base-Tx device exists. Off when a good connection does not exist. Flashes Green when the port has been disabled.

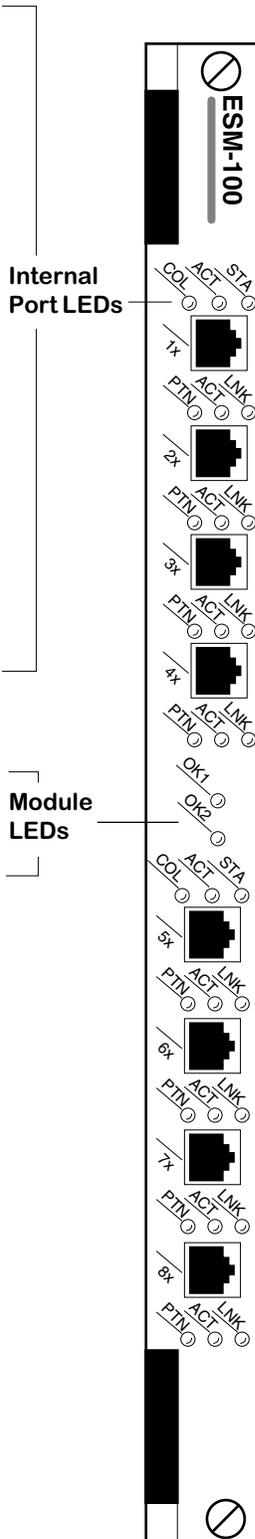
ESM-100C 8-Port Module

COL. Flashes amber when a collision has been detected on the internal port. A collision here is defined as two or more ports receiving data at the same time. The ports included in this collision domain include the four front panel ports plus the internal port connected to the switch backplane. A collision may occur when data is received simultaneously on two front panel ports or when data is received on a front panel port and the internal port attached to the switch backplane simultaneously.

ACT. On Green when data is received from the switch backplane that is destined for one of the front panel ports.

STA. On Green when the internal port has a valid connection to the switch backplane and has been initialized. This connection can be disabled via software.

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.



The ESM module includes one row of LEDs for each port. The LEDs for a given port display below that port.

PTN. On amber when excessive collisions have forced the port to be partitioned. A port will partition after 64 consecutive collisions have occurred. Partitioning the port allows the other three ports to receive data again. Only one of the four front panel ports can receive data at one time. Therefore, partitioning a port that is creating a bottleneck with excessive collisions clears the data path so that the other three ports can receive data.

ACT. On Green when data is received on the corresponding port. After receiving data, the receiving port automatically transmits the data to the other three front panel ports and to the internal port.

LNK. On Green continuously when a good cable connection to a 100Base-Tx device exists. Off when a good connection does not exist. Flashes Green when the port has been disabled.

ESM-100C (Older Front Panel Design)

ESM-100C-FD (Discontinued)

The ESM-100C-FD Ethernet switching module contains one or two RJ-45 connectors that support one or two fully switched, full-duplex, 100Base-Tx ports. Each port uses the full 100 Mbps of bandwidth in each direction. Each port supports either half- or full-duplex operation. You configure whether you want a half- or full-duplex connection through the **eth100cfg** command. By default, ESM-100C-FD ports support full-duplex connections.

The ESM-100C-FD is best used as a high-speed connection to a server. If the server supports full-duplex communication, then throughput is doubled from a standard half-duplex connection. If connection to a Fast Ethernet backbone is desired, then the fiber variation of this module, the ESM-100F-FD, is a more suitable choice. See *ESM-100Fx-FD (Discontinued)* on page 7-107 for information on the ESM-100F-FD.

The ESM-100C-FD is actually a sub-module, or daughtercard, that attaches to a High-Speed Module (HSM). The HSM contains memory and processing power for switching modules that operate at speeds greater than 10 Mbps. You plug your Ethernet cable directly into the ESM-100C-FD sub-module, but it is the HSM module that connects to the switch backplane.

ESM-100C-FD Technical Specifications	
Number of ports	One or two
Connector Type	RJ-45
Standards Supported	IEEE 100Base-Tx
Data Rate	100 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	Full duplex: 100Base-Tx device or bridge port Half-duplex: 100Base-Tx device, hub or bridge port
Cable Supported	Unshielded twisted-pair (UTP)—100 ohm Shielded twisted-pair (STP)—100 ohm
Cable Distance	100 m

Original Fast Ethernet (100 Mbps) Modules (Discontinued)

The ESM-100C-FD module includes one set of LEDs for each 100Base-Tx port. The LEDs for a given port display above the port. If the ESM module includes two ports, then the module contains two sets of LEDs. The second set of LEDs displays above the second 100Base-Tx port.

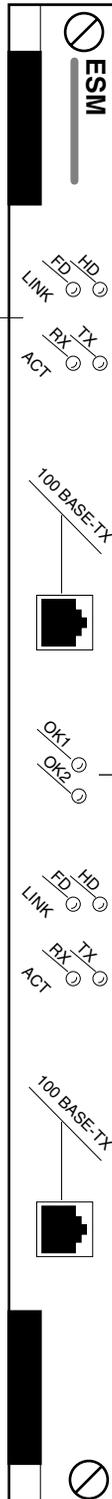
FD and HD. These two LEDs indicate the current operational mode and the link status of the connection for this ESM-100 port. When the **HD** LED is On, then the port has a good connection and is operating in half-duplex mode; the port and the device to which it is connected do not transmit at the same time. When the **FD** LED is On, the port has a good connection and is operating in full-duplex mode; the port and the device to which it is connected can transmit simultaneously. You can configure whether the port operates in half- or full-duplex mode with the **eth100cfg** command. By default, the port operates in full-duplex mode.

RX and TX. These two LEDs indicate transmit and receive activity on this port. The RX LED is On when data is received on the port. The TX LED is On when data is transmitted from the port.

Port LEDs

Module LEDs

Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.



Ethernet 100Base-Tx Full-Duplex Switching Module

ESM-100Fx-FD (Discontinued)

The ESM-100Fx-FD Ethernet switching module contains one or two fiber SC connectors that support one or two fully switched 100Base-Fx ports. Each port uses the full 100 Mbps of bandwidth in each direction. The ESM-100Fx-FD can be factory configured with single mode or multimode fiber ports. The single mode version is referred to as the ESM-100FS-FD; the multimode version is referred to as the ESM-100FM-FD. The ports are color coded to differentiate the mode: single mode connectors are blue and multimode connectors are black.

The fiber port supports either half- or full-duplex operation. You configure whether you want a half- or full-duplex connection through the **eth100cfg** command. By default, ESM-100Fx-FD ports support full-duplex connections.

The ESM-100Fx-FD is best used as a backbone connection in networks where Fast Ethernet is used as the backbone media. Its support for full-duplex operation allows you to exceed the distance available through half-duplex connections. Each 100BaseFx port may also connect to a single high-traffic device, such as a mail or file server.

The ESM-100Fx-FD is actually a sub-module, or daughtercard, that attaches to a High-Speed Module (HSM). The HSM contains memory and processing power for switching modules that operate at speeds greater than 10 Mbps. You plug your Ethernet cable directly into the ESM-100F-FD sub-module, but it is the HSM module that connects to the switch backplane.

ESM-100Fx-FD Technical Specifications	
Number of ports	One or two
Connector Type	SC
Standards Supported	IEEE 100Base-Fx
Data Rate	100 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	Full duplex: 100Base-Fx device or bridge port Half-duplex: 100Base-Fx device, hub or bridge port
Cable Supported	Single mode or multimode fiber
Optical output power	Multimode: -19 to -14 dBm Single mode (category 1): -20 to -14 dBm
Optical receiver sensitivity	Multimode: -31 to -14 dBm Single mode (category 1): -31 to -8 dBm
Cable Distance	Multimode (12dB) fiber: approximately 4.5 km Single mode (11 dB) fiber: approximately 16.5 km

◆ Special Note ◆

The single mode version of this module has been deemed:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

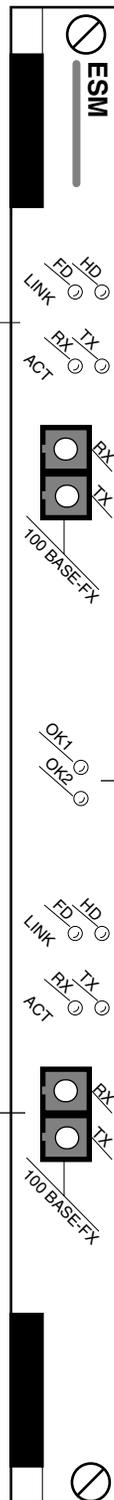
Original Fast Ethernet (100 Mbps) Modules (Discontinued)

The ESM-100Fx-FD module includes one set of LEDs for each 100Base-Fx port. The LEDs for a given port display above the port. If the ESM module includes two ports, then the module contains two sets of LEDs. The second set of LEDs displays above the second 100Base-Fx port.

FD and **HD**. These two LEDs indicate the current operational mode and the link status of the connection for this ESM-100 port. When the **HD** LED is On, then the port has a good connection and is operating in half-duplex mode; the port and the device to which it is connected do not transmit at the same time. When the **FD** LED is On, the port has a good connection and is operating in full-duplex mode; the port and the device to which it is connected can transmit simultaneously. You can configure whether the port operates in half- or full-duplex mode with the `eth100cfg` command. By default, the port operates in full-duplex mode.

RX and **TX**. These two LEDs indicate transmit and receive activity on this port. The RX LED is On when data is received on the port. The TX LED is On when data is transmitted from the port.

SC connectors are color coded to indicate multimode (Black) or single mode (Blue).



Module LEDs Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

Ethernet 100Base-Fx Full-Duplex Switching Module (Single or Multimode)

ESM-100C-5 (Discontinued)

The ESM-100C-5 Ethernet switching module contains five 100Base-Tx ports using RJ-45 connectors. The single top port is a full-duplex port that supports 100 Mbps of bandwidth in each direction over one dedicated Ethernet segment. The bottom set of four ports are one shared collision domain that switches between the top port or any other network segment.

Full-Duplex Port

The single top port is a fully switched, full-duplex 100Base-Tx port that uses the full 100 Mbps of bandwidth in each direction. It supports either half- or full-duplex operation. You configure whether you want a half- or full-duplex connection through the **eth100cfg** command, but by default the ports support full-duplex connections. This port is best used as a high-speed connection to a server. If the server supports full-duplex communication, then throughput is doubled from a standard half-duplex connection.

Four-Port Shared Collision Domain

The bottom four ports connect to 100Base-Tx devices. The set of ports connects to a fifth, internal port. This internal port connects directly to the switch backplane and has a unique MAC address. Each of the bottom four front panel ports are capable of using the full 100 Mbps of dedicated bandwidth. However, when more than one connection is made to each set of four ports, those connections share the 100 Mbps of bandwidth.

Front panel ports receive data from attached 100BaseTx devices and from the fifth internal port (which connects to the switch backplane). In addition, data received on any front panel port is automatically passed on to the other three ports that share its collision domain and to the internal port.

The internal switch port receives data from the switch backplane and the 100Base-Tx front panel ports. This port passes data destined for the front panel ports (from other switch ports) in one direction, and passes data destined for other switch ports (from the front panel ports) in the other direction. This internal port has its own set of LEDs, which is located above the front panel port LEDs.

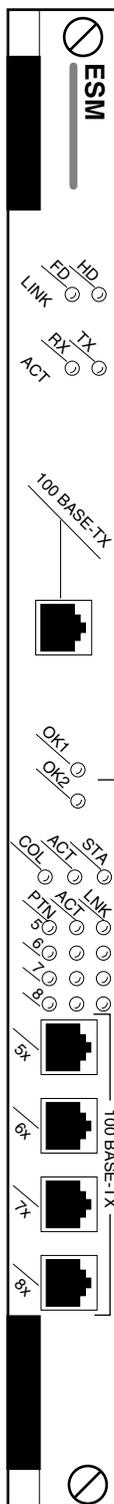
The ESM-100C-5 is actually two sub-modules, or daughtercards, that attach to a High-Speed Module (HSM). The HSM contains memory and processing power for switching modules that operate at speeds greater than 10 Mbps. You plug your Ethernet cable directly into the ESM-100C-5 sub-module, but it is the HSM module that connects to the switch backplane.

ESM-100C-5 Technical Specifications	
Number of ports	5
Connector Type	RJ-45
Standards Supported	IEEE 100Base-Tx
Data Rate	100 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	Full duplex: 100Base-Tx device or bridge port Half-duplex: 100Base-Tx device, hub or bridge port
Cable Supported	Unshielded twisted-pair (UTP)—100 ohm Shielded twisted-pair (STP)—100 ohm
Cable Distance	100 m

This module includes one set of LEDs for the full-duplex connection and one set of LEDs for the four shared-domain ports. The LEDs for the full-duplex connection display above the top switch port. The LEDs for the four shared domain ports display above the set of ports.

Full-Duplex Port LEDs. These LEDs are described for the ESM-100C-FD module. See *ESM-100C-FD (Discontinued)* on page 7-105 for a description of these LEDs.

Shared Domain LEDs. These LEDs are described for the ESM-100C module. See *ESM-100C (Discontinued)* on page 7-101 for a description of these LEDs.



Module LEDs Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

Ethernet 100Base-Tx 5-Port Switching Module

ESM-100CFx-5 (Discontinued)

The ESM-100CFx-5 Ethernet switching module contains one fiber SC connector and four RJ-45 connectors that support one fully switched 100Base-Fx port and four shared 100Base-Tx ports, respectively. The fiber port is a full-duplex port that supports 100 Mbps of bandwidth in each direction. The set of four ports is one shared collision domain that switches between the 100Base-Fx port or any other segment in the network.

Full-Duplex Fiber Port

The fiber port is a fully switched, full-duplex 100Base-Fx port that uses the full 100 Mbps of bandwidth in each direction. The ESM-100CFx-5 can be factory configured with single mode or multimode fiber ports. The single mode version is referred to as the ESM-100CFS-5; the multimode version is referred to as the ESM-100CFM-5. The port is color coded to differentiate the mode: a single mode connector is blue and a multimode connector is black.

The fiber port supports either half- or full-duplex operation. You configure whether you want a half- or full-duplex connection through the **eth100cfg** command. By default, the port supports full-duplex connections.

This port is best used as a backbone connection in networks where Fast Ethernet is used as the backbone media. Its support for full-duplex operation allows you to exceed the distance available through half-duplex connections. In addition to its use as a backbone connection, this port may connect to a single high-traffic device, such as a mail or file server.

Four-Port Shared Collision Domain

The bottom four ports connect to 100Base-Tx devices. The set of ports connects to a fifth, internal port. This internal port connects directly to the switch backplane and has a unique MAC address. Each of the four front panel ports are capable of using the full 100 Mbps of dedicated bandwidth. However, when more than one connection is made to each set of four ports, those connections must share the 100 Mbps of bandwidth.

Front panel ports receive data from attached 100BaseTx devices and from the fifth internal port (which connects to the switch backplane). In addition, data received on any front panel port is automatically passed on to the other three ports that share its collision domain and to the internal port.

The internal switch port receives data from the switch backplane and the 100Base-Tx front panel ports. This port passes data destined for the front panel ports (from other switch ports) in one direction, and passes data destined for other switch ports (from the front panel ports) in the other direction. This internal port has its own set of LEDs, which is located above the front panel port LEDs.

The ESM-100CFx-5 is actually two sub-modules, or daughtercards, that attach to a High-Speed Module (HSM). The HSM contains memory and processing power for switching modules that operate at speeds greater than 10 Mbps. You plug your Ethernet cable directly into the ESM-100CF-5 sub-module, but it is the HSM module that connects to the switch backplane.

ESM-100CFx-5 Technical Specifications	
Number of ports	5
Connector Type	SC and RJ-45
Standards Supported	IEEE 100Base-Fx and 100Base-Tx
Data Rate	100 Mbps
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	Full duplex: 100Base-Fx device or bridge port Half-duplex: 100Base-Fx/Tx device, hub or bridge port
Cable Supported	Fiber Port Single mode or multimode fiber Shared Port Unshielded twisted-pair (UTP)—100 ohm Shielded twisted-pair (STP)—100 ohm
Optical output power	Multimode fiber: -19 to -14 dBm Single mode (category 1) fiber: -20 to -14 dBm
Optical receiver sensitivity	Multimode fiber: -31 to -14 dBm Single mode (category 1) fiber: -31 to -8 dBm
Cable Distance	RJ-45 Port: 100 m Fiber Full-Duplex Port: Multimode (12dB) fiber: approximately 4.5 km Single mode (11 dB) fiber: approximately 16.5 km

◆ **Special Note** ◆

The single mode fiber version of this module has been deemed:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

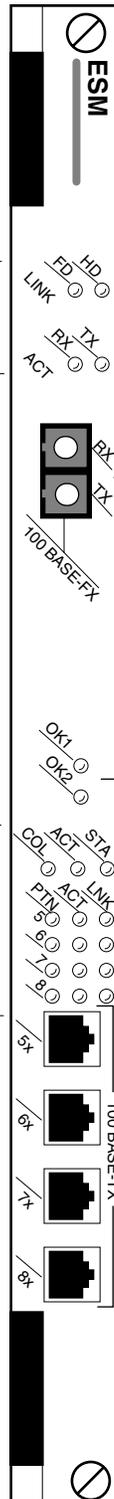
to IEC 825:1984/CENELEC HD 482 S1.

Original Fast Ethernet (100 Mbps) Modules (Discontinued)

This module includes one set of LEDs for the fiber connection and one set of LEDs for the four shared-domain ports. The LEDs for the fiber connection display above the top switch port. The LEDs for the four shared domain ports display above the set of ports.

Full-Duplex Port LEDs. These LEDs are described for the ESM-100F-FD module. See *ESM-100Fx-FD (Discontinued)* on page 7-107 for a description of these LEDs.

Shared Domain LEDs. These LEDs are described for the ESM-100C module. See *ESM-100C (Discontinued)* on page 7-101 for a description of these LEDs.



SC connector is color coded to indicate multimode (Black) or single mode (Blue).

Module LEDs Please refer to *Module LEDs* on page 7-16 for further information on these LEDs.

Ethernet 100Base-Fx/100Base-Tx 5-Port Switching Module

8 The User Interface

In order to configure parameters and statistics on the switch, you may connect it to a terminal, such as a PC or UNIX workstation, using terminal emulation software. The command interfaces used on the switch are part of the MPM executable image. When a switch boots up, the boot monitor handles the loading of this executable image and system startup. Once the image is loaded and initialized, the CLI starts.

You access the command interfaces through a connection with the switch. This connection can be made directly to the serial port, through a modem, or over a network via Telnet. You can have up to four simultaneous connections to an OmniSwitch or an Omni Switch/Router. (Please see Multiple User Sessions on page 8-37 for further details.) For Telnet access, you must first set up an IP address for the switch. See the *Getting Started Guide* that came with your switch for information on setting up an IP address and logging in.

Overview of Command Interfaces

The Alcatel OmniSwitch and Omni Switch/Router have two different command interfaces available for configuring parameters and viewing statistics. They are the User Interface (UI) and the Command Line Interface (CLI). Prior to software Release 4.4, the switch automatically booted up in the UI mode. In Release 4.4 and later, both the OmniSwitch and the Omni Switch/Router are factory-configured to boot up in the CLI mode.

◆ Terminology Notes◆

Command interface generically refers to any mechanism resident in the software that allows a user to change switch configurations or to display statistics.

The *UI* is the original command interface used exclusively on all Alcatel OmniSwitch products. The UI has its commands grouped into functional menus. Prior to software Release 4.1, the UI was the only command interface supported on the OmniSwitch products.

The *CLI* is Alcatel's text-based configuration interface that allows you to configure OmniSwitch products using single-line text commands. The CLI was implemented in software Release 4.1 and higher.

Changing Between the CLI and UI Modes

Once you log on to the switch, the following screen displays. You must press the **<Enter>** key to start the command interface.

```
*****  
Alcatel OmniSwitch  
Copyright (c), 1994-2001 Alcatel Internetworking, Inc. All rights reserved.  
OmniSwitch is a trademark of Alcatel Internetworking, Incorporated,  
registered in the United States Patent and Trademark Office.  
Press ENTER to start  
->
```

Overview of Command Interfaces

After you press **<Enter>**, the CLI starts automatically and the following text displays.

```
Entering command line interface.  
->
```

At this point, you are in the CLI mode and may configure the switch or display statistics using the commands described in the *Text-Based Configuration CLI Reference Guide*. If you want to use the UI command interface, type **ui** and press **<Enter>**. This causes the switch to leave the CLI mode and enter the UI mode, provided you are using a login with Read/Write privileges. You can verify that you are in the UI mode by typing **?** to display the top-level menu for the UI as shown below.

/%? Command	Main Menu
File	Manage system files
Summary	Display summary info for VLANs, bridge, interfaces, etc.
VLAN	VLAN management
Networking	Configure/view network parameters such as routing, etc.
Interface	View or configure the physical interface parameters
Security	Configure system security parameters
System	View/set system-specific parameters1
Services	View/set service parameters
Switch	Enter Any to Any Switching menu
Help	Help on specific commands
Diag	Display diagnostic level commands
Quit/Logout	Log out of this session
?	Display the current menu contents

To change from the UI mode back to the CLI mode, type **cli** and press **<Enter>**.

◆ Note ◆

Note the default command prompt for the UI is **/%**. The default command prompt for the CLI is **->**. You can change the UI system prompt by using the **uic** command.

Exit the Command Interface

To exit your current session with the switch from the CLI or the UI mode, type either **quit** or **logout** at the prompt, then press **<Enter>**. Your session is immediately terminated.

◆ Note ◆

If you forget which command interface mode you are in, type the **?** character. If you are in the UI mode, the Main Menu will display as shown above. If you are in the CLI mode, the switch will show the following display.

```
^NO, SHOW, VOICE, SYSTEM, ACCOUNTING, . . .  
->
```

UI to CLI Command Cross Reference

The chapters in this Users Guide are organized around the UI commands as they are grouped into menus and sub-menus. Even though the OmniSwitch software has been changed to boot up in the CLI mode, the Users Guide conforms to its original design. The CLI commands are fully documented in the *Text-Based Configuration CLI Reference Guide*.

This section presents the key UI commands that are explained in this User's Manual along with their CLI equivalents. Where the CLI commands support partition management, these tables also list the partition management family to which the commands belong.

Hardware Commands

The hardware section of this manual set consists of chapters 1 through 7. There are relatively few UI commands in this section because these chapters cover the hardware elements of the switch. The commands defined in these chapters are listed in the Hardware Table beginning on page 8-3.

Hardware Table

Chapter	UI Command	Equivalent CLI Commands	PM Family
1, "OSR Chassis/Power Supplies"	No UI commands are defined in this chapter.	N/A	N/A
2, "MPX"	ethernetc	ethernet management port view ethernet manage port	GF-interface
3, "OSR Switching Modules"	10/100cfg 10/100vc tpcfg	ethernet view interface fastethernet token ring	GF-interface
4, "Chassis"	No UI commands are defined in this chapter.	N/A	N/A
5, "Power Supplies"	No UI commands are defined in this chapter.	N/A	N/A
6, "MPM"	ethernetc ls rm ser	ethernet management port ls rm Unsupported	GF-interface GF-ls GF-rm
7, "Omni Switch Switching Modules"	100/100cfg 10/100vc camstat ethernetc map reset swap	ethernet view interface fastethernet status cam ethernet management port group authentication atm port, csm port, reset swap	GF-interface

Basic Switch Management Commands

The table beginning on page 8-4 summarizes the features supported in the UI and the CLI for Chapters 8 through 15.

Basic Switch Management Table

Chapter	UI Command	Equivalent CLI Commands	PM Family
8, "The User Interface"	alert, echo, history, kill, ping, pwd, timeout, who lookup, save, summary, uic, write	alert, echo, history, kill, ping, password, timeout, who Unsupported	No PM Support
9, "Installing Switch Software"	ftp load primary, secondary	ftp load primary, secondary	GF-Ftp GF-File
10, "Configuring Management Processor Modules"	configsnc ethernetc imgsync mpm mpmget mpmload mpmreplace mpmrm mpmstore renounce secreset slipc sls swap syncctl takeover	configuration copy ethernet management port image copy view mpm command load primary mpm file load secondary mpm file replace secondary mpm file remove secondary mpm file store secondary mpm file takeover reload secondary mpm slip view secondary mpm file swap configuration auto-copy takeover	GF-File
11, "Managing Files"	cd cp load newfs ftp ls pwd rm imgcl	cd copy load newfs ftp ls password rm imgcl	GF-CD GF-System GF-System GF-System GF-FTP GF-LS 18-User GF-RM GF-System
12, "Switch Security"	pw reboot useradd userdel usermod userview asacfg secdefine secapply layer2auth, privs, secapply, secdefine, seclog, security	password reboot now user no user user view user ldap server secure access filter secure access no filter view secure access filter security security custom security no custom Unsupported	18-User GF-Reboot 18-User 18-User 18-User 18-User 1-Configuration GF-System GF-System GF-System GF-System GF-System GF-System No PM Support

continued on next page...

Basic Switch Management Table (continued)

Chapter	UI Command	Equivalent CLI Commands	PM Family
13, "Switch-Wide Parameters"	cacheconfig camstat dt hrexassign hrexdisplay hrexhashopt hrexutil info memstat modvp newfs saveconfig slot syscfg systat camcfg, fsck, sc, si, ss, taskstat	configuration cache camstat dt hrexassign hrexdisplay hrexhashopt hrexutil info memstat modvp newfs configuration cache save slot syscfg systat Unsupported	No PM Support
14, "Switch Logging"	secdefine secapply caplog, cmdlog, syslog, conlog, debuglog, swlogc	secure access filter secure access no filter view secure access filter security security custom security no custom Unsupported	GF-System
15, "Health Statistics"	hdcfg health hmstat hpstat hreset	health threshold view health statistics view health statistics view health statistics health statistics reset	GF-System

Network Management Commands

The table on page 8-5 summarizes the commands supported in the UI and the CLI for Chapters 16 through 18.

Network Management Table

Chapter	UI Command	Equivalent CLI Commands	PM Family
16, "Network Time Protocol"	ntconfig, ntstats, ntadmin, ntaccess	Unsupported	No PM Support
17, "Configuring SNMP"	snmpc snmps	view snmp set snmp	6-SNMP
18, "RMON and DNS Resolver"	res probes events names chngmac	res view rmon probes view rmon events view dns Unsupported	GF-System

Layer II Switching Commands

The table on page 8-6 summarizes the features supported in the UI and the CLI for Chapters 19 through 23.

Layer II Switching Table

Chapter	UI Commands	Equivalent CLI Commands	PM Family
19, "Managing Ethernet Modules"	addprtchl chnlinfo crechnl delchnl delprtchl eth10/100vc eth10/100cfg	static agg view statis linkagg number static linkagg number type no static linkgg number static agg no view interface fastethernet interface ethernet	GF-Interface
20, "Managing 802.1Q Groups"	cas, das, mas, vas	All commands used to create, delete, modify and view a service, plus the message command are supported.	GF-System
21, "Managing Token Ring Modules"	br, src, tpcfg, trsw, dtmap, tsmcf, tpvc, tsmvc, vtmap crtmap, tok, tperrs, tprs, tpvc, trportsw, tsc, srs,	Supported Unsupported	No PM Support
22, "Configuring Bridging Parameters"	fddi, fsmt, fsid, fsmtc, fsstatus, fmac, fmaddr, fmstats, fmctrs, fport, fportstatus, fportctrs, fportc, macstat, slipc maccirstat, selgp, srsf, srtbcfg, srtbclrrif, srtbrif	Supported Unsupported	5-Bridge
23, "Configuring Frame Translations"	actfstps, bps, dbrmap, fc, flc, fls, fs, fstps, fwt, macinfo, modvp, rts, srtbrif, stc, sts, stpc, stps, swchmac autoencaps, ethdef, facdef, propipx, swchmac, trdef	Supported Unsupported	5-Bridge

Groups, VLANs, Policies Commands

The table beginning on page 8-7 summarizes the features supported in the UI and the CLI for Chapters 24 through 29.

Groups, VLANs, Policies Table

Chapter	UI Command	Equivalent CLI Commands	PM Family
24, "Managing Groups and Ports"	swch vi autoencaps, ethdef, facdef, propipx, swchmac, trdef	port encapsulation view group rules Unsupported	2-Group
25, "Group and VLAN Policies"	addqgp addvp cas cats crgp dats delqgp gmcfg gmstat gp modvl pmapcr pmapdel pmapmod pmapv pmcfg pmon pmstat pmp prty_mod prty_disp rmgp rmvp vats ve vi viqgp vs via vpl at, br, pmd, prty_mod, vlan, vigl, viqgp	group num 802.1q group num interface fddi svc, group 802.1q atm service group elan group group num no 802.1q group no elan group mobility group mobility view group group router, vlan router port mapping ingress no port mapping port mapping view port mapping port monitor configuration port monitor view port monitor resume port monitor group priority num view group priority no group group no interface view group auto view group virtual errors view group rules view ethernet view group virtual statistics view group virtual (ports) view group mobility Unsupported	2-Group
26, "InterSwitch Protocols"	atvl fwttl modatvl vap viatrl vivl vlap	view vlan rules view group mac group mac, vlanmac, vlan user, vlan port, vlan chcp port, vlan dhcp mac, vlan protocol, vlan binding ip, vlan binding vap port vlan ip, vlan ipx view vlan rules view vlan rules vlap	6-Group GF-System GF-System

continued on next page...

Group, VLANs, Policies Table (continued)

Chapter	UI Commands	Equivalent CLI Commands	PM Family
27, "Managing AutoTracker VLANs"	gmap, gmapst gmappgptime gmapholdtime gmapuptime xmapst xmapls xmapcmntime xmapdisctime	gmap gmap gap time gmap hold time gmap up time xmap, view xmap status view xmap, view xmap xmap common time xmap discovery time	6-Group
28, "Multicast VLANs"	cats cratvl crmcvl defvl fwtvl gmcfg gmstat mag mcvl modatvl rmatvl vag vats viatrl vimcvl vivil vpl atvl, vigl, xip	group elan vlan, vlan router ip, vlan router ipx, vlan mac, vlan user, vlan dhcp port vlan dhcp nac, vlan protocol, vlan binding ip, vlan binding mac, vlan binding port vlan ip, vlan ipx multicast vlan, multicast vlan port multicast vlan mac, vlan protocol vlan binding ip, vlan binding mac vlan binding port, multicast vlan descr vlan default view group mac view group authenticated group mobility group authentication, group authentication protocol view multicast vlan group mac, group mac range, group user, group port, group dhcp port, group dhcp mac, group dhcp range group protocol, group binding ip, group protocol mac, group binding port, group ip, group ipx, vlan mac, vlan user, vlan port, vlan dhcp port, vlan dhcp mac, vlan protocol, vlan binding protocol, vlan binding mac, vlan binding port, vlan ip, vlan ipx no vlan view group authenticated view group auto view vlan rules view multicast vlan ports view group ports, view group vports view group mobility	6-Group
29, "AutoTracker VLAN Examples"	crmcvl, modmcvl rmmcvl vimcrl vimcvl	multicast vlan no multicast vlan view multicast vlan rules view multicast vlan	GF-System

Routing Commands

The table beginning on page 8-9 summarizes the features supported in the UI and the CLI for Chapters 30 through 32.

Routing Table

Chapter	UI Command	Equivalent CLI Commands	PM Family
30, "IP Routing"	All IP Routing commands are supported in the CLI.	All IP Routing commands are supported in the CLI.	3-IP Routing GF-System
31, "UDP Forwarding"	aisr events icmps ipfilter ipmac ipr ips names ping probes ripflush rips risr snmpc snmps telnet tcpc tcps traceroute udpl udps xlat chnghmac, flush, flconfig, ipclass, ipdirbrcast, names, probes	iproute view rmon events view icmp rip filter view mac view ip route view ip traffic ip [no] domain-lookup ping view rmon probes ripflush rips no ip route snmp config, snmp communi- ty, snmp trap, broadcast, snmp trap unicast snmp station view snmp telnet ip-address view tcp users view tcp trace view udp users view ucp arp, clear arp-cache, view arp Unsupported	3-IP Routing
32, "IPX Routing"	relayc relays avlbootmode, edit	ip helper view ip helper stats Unsupported	No PM Support

ATM Access Commands

The table beginning on page 8-10 summarizes the features supported in the UI and the CLI for Chapters 33 through 39.

ATM Access Table

Chapter	UI Command	Equivalent CLI Commands	PM Family
33, "Managing ATM Access Modules"	cva cvc dva dvc map mbwg mva mvc vap vbwg vcrs, vcs, vcts vnac, vnapc	atm address atm connection no atm address no atm connection atm port atm bandwidth atm address atm connection view atm port view bandwidth view atm Unsupported	9-ATM Service No PM Support
34, "Managing Circuit Emulation Modules"	ceadd cecls cedele cemodify cestatus	atm-ce connection atm-ce connection clear statistics no atm-ce connection atm-ce connection atm-ce connection view	9-ATM Service
35, "LANE Server Config,"	lsmcfg lsib velan vlb vlbc vlbx vlec vlecs vlecsc vmac vpolicy vrđ	lsm les-bus view les-bus view elan view les bus station view les bus configuration view les bus statistics view les bus clients view lec status view lec statistics view lec configuration view les bus registered mac view elan policy view les bus registered route descriptor	9-ATM Service

continued on next page...

ATM Access Table (continued)

Chapter	UI Commands	Equivalent CLI Commands	PM Family
36 "Configuring ATM Services"	aat cas das mas vas vat vlat vss vgptovc	atm arp static atm service no atm service atm service bandwidth atm service member atm service description atm service explorer frame exclude atm service selector atm service no scaling map view atm service view atm cip arp view atm lane arp view atm service statistics Unsupported	9-ATM Service
37 "MPOA"	mpccfg vmcpc vmcpc, vmcpcs, vmcpcst vmcpci	mpos service, view mpos view mpos status view mpos statistics view mpos ingress cache	15-MPOA
38, "Frame Relay/ATM Internet- working"	fratm, frmodify, frscvc, frsdvc, frsmc, frsmvc, frsvc, frsvs, loadfrlmi	Unsupported	No PM
39, "SONET Error Statistics"	secs, ses, sess, sedm, seds, smon	Unsupported	

ATM Cell Switching (X-Cell) Commands

The table beginning on page 8-12 summarizes the features supported in the UI and the CLI for Chapters 40 through 45.

ATM Cell Switching (X-Cell) Table

Chapter	UI Command	Equivalent CLI Commands	PM Family
40, CSM	swap	swap on, swap off	GF-Swap
41, "Managing CSMs"	map cvc mvc vcts vvc imce, imcr, imci, imcd, masrt, mclk, mcst, vcac, vnac, vclk, vclka	atm port atm connection atm connection best effort atm connection pcr atm connection maximum atm connection description view atm tx view atm connection Unsupported	11-CSM
42, "Advanced CSM Management"	lvpt mvpt scvc svvc vcrs, vcs, vlrs imce, imcd, imci, masrt	view csm tunnel csm tunnel csm spvc view csm spvc view atm Unsupported	11-CSM
43, "IMA"	igpa, igpmem igpa, igpmem, igpd igpm igptestb, igptest igprst igps, igpsts icpls ilkm ilks, ilksts ilksts	interface atm ima-group csm port description status ima version active-links-minimum differential-delay-maximum invalid-icp-before-hunt errored-icp-before-hunt valid-icp-before-sync clock source framing cablelength loopback frame-length test restart view clear statistics ima-link, description, status view clear statistics	No PM Support
44, "ATM Accounting"	Not Supported	CLI Commands only.	13-ATM Accounting
45, "Clocking ATM Networks"	mclk vclk, vclka, mclka	csm clock Not supported in CLI.	No PM Support

PNNI/IISP Commands

The table beginning on page 8-13 summarizes the features supported in the UI and the CLI for Chapters 46 and 47.

PNNI/ISP Table

Chapter	UI Command	Equivalent CLI Commands	PM Family
46, "Configuring and Monitoring PNNI"	pestats pgcfg pncfg ppcfg pninfo ptinfo pnbrs plink pptse, ppadj, psmap, pmap, pnmap, pcalls, pdtl, pgstats, ppstats phalt, prestart, preset, prcft, ptst	view pnni port error statistics pnni status pnni node, pnni timer pnni port config view pnni node view pnni timer view pnni neighbors view pnni link view pnni Unsupported	12-PNNI
47, "PNNI Static Routes/IISP"	map pradd prdel prp prt prpadd prpdel proutea, prouten	atm port pnni route no pnni route view pnni route property view pnni route prefix pnni route property no pnni route property Unsupported	12-PNNI

WAN Access Table (continued)

Chapter	UI Command	Equivalent CLI Commands	PM Family
56, "Channelized DS3"	m013 ds3mod ds3dlts ds3dlcs ds3dlis ds3clis ds3dcs ds3scs ds1mod ds1dlts ds1dlcs ds1dlis ds1clis ds1dcs lpadd lpmod lpdel lpview lpcls lppmod lppview lppcls lpfradd lpfrdel riadd rimod ridel riview ricls m013cas m013das m013vas m013mas m013cfgdel	Unsupported m013 ds3 view m013 ds3 statistics view m013 ds3 statistics current view m013 ds3 statistics interval m013 ds3 clear interval statistics view m013 ds3 m013 ds3 ds1 statistics m013 ds1 view m013 ds1 statistics view m013 ds1 statistics current view m013 ds1 statistics interval m013 ds1 clear interval statistics view m013 ds1 m013 logical encapsulation ds0 channels m013 logical description no m013 logical view m013 logical m013 logical clear statistics m013 ppp view m013 logical protocol m013 clear protocol statistics m013 frvc dlci status no m013 frvc m013 ip router mask status m013 ip router mask status no m013 ip router view m013 ip router m013 ip router clear statistics m013 service description type no m013 service description view m013 service description m013 service description status no m013 configuration	No PM Support

Troubleshooting Diagnostics Commands

The table beginning on page 8-17 summarizes the features supported in the UI and the CLI for Chapters 57 and 58 and Appendices A and B.

Troubleshooting/Diagnostics Table

Chapter/ Appendices	UI Command	Equivalent CLI Commands	PM Family
57, "Troubleshoot- ing"	uic	Unsupported	No PM Support
58, "Running Hardware Diagnostics"	diag	Unsupported	No PM Support
A, "Boot Line Prompt"	ethernetc	ethernet manager port	No PM Support
B, "Custom Cables"	No UI commands in this Appendix.	No CLI commands in this Appendix	No PM Support

User Interface Menu

This menu provides a top-level view of all UI menus. The commands are grouped together in the form of sub-menus. Within each sub-menu there is a set of commands and/or another sub-menu.

Alcatel OmniSwitch
Copyright (c), 1994-2001 Alcatel Internetworking, Inc. All rights reserved.
OmniSwitch is a trademark of Alcatel Internetworking, Inc.
registered in the United States Patent and Trademark Office.

System Name: no_name

Command	Main Menu
File	Manage system files
Summary	Display summary info for VLANs, bridge, interfaces, etc.
VLAN	VLAN management
Networking	Configure/view network parameters such as routing, etc.
Interface	View or configure the physical interface parameters
Security	Configure system security parameters
System	View/set system-specific parameters1
Services	View/set service parameters
Switch	Enter Any to Any Switching menu
Help	Help on specific commands
Diag	Display diagnostic level commands
Quit/Logout	Log out of this session
?	Display the current menu contents

◆ Note ◆

Although the commands are grouped in a sub-menu structure, any command may be entered from any sub-menu. You are not restricted to the commands listed in the current sub-menu.

Main Menu Summary

These menus, their sub-menus, and sub-options are described in this manual. The following provides a brief overview of each item on this main menu.

File. Contains options for downloading system software, listing software files, copying files, editing files, and deleting files. This menu is fully described in Chapter 11, “Managing Files.”

Summary. Provides very basic information on the physical switch, such as its name, MAC address, and resets. It also provides options for viewing the virtual interface and information on the MIB. This menu is described in Chapter 13, “Switch-Wide Parameters.”

VLAN. The main menu for configuring Groups, virtual ports, and AutoTracker VLANs. This menu also contains a sub-menu for configuring bridging parameters, such as Spanning Tree and Source Routing. Groups and ports are described in Chapter 24, “Managing Groups and Ports.” VLANs are described in Chapter 27, “Managing AutoTracker VLANs” and Chapter 28, “Multicast VLANs.” Bridging parameters are described in Chapter 23, “Configuring Bridging Parameters,” and Source Routing is described in Chapter 21, “Managing Token Ring Modules.”

Networking. Contains menu options for managing internetworking protocols, such as SNMP and RMON (described in Chapters 17 and 18, respectively), IP (described in Chapter 30, “IP Routing”) and IPX (described in Chapter 32, “IPX Routing”).

Interface. The main menu for configuring parameters and viewing statistics for switching modules. This menu has sub-menus for managing ATM, FDDI, Token Ring, Frame Relay, and Fast Ethernet switching modules. In addition it includes a sub-option for configuring SLIP. These sub-menus are described in Chapters 19 through 21 and Chapter 49. The ATM sub-menu option is described in Chapter 41, “Managing Cell Switching Modules (CSMs),” and Chapter 33, “Managing ATM Access Modules.”

Security. This menu contains options for changing a password and rebooting the system. It is described in Chapter 12, “Switch Security.”

System. Contains a wide array of options for configuring and viewing information on a variety of switch functions. Options include displays of switch slot contents, configuring serial ports, and viewing CAM information. Commands used to configure User Interface display options are described in User Interface Display Options on page 8-34. Other System menu commands are described in Chapter 13, “Configuring Switch-Wide Parameters.” The System menu also includes a sub-menu option that provides additional commands for configuring the MPM module. This sub-menu is described in Chapter 10, “Configuring Management Processor Modules.”

Services. Provides options for creating, modifying, viewing, and deleting ATM, FDDI, and Frame Relay services. ATM services include PTOP bridging and LAN Emulation. FDDI services include Trunking and 802.10 Trunking. Frame Relay services include bridging, routing, and trunking. ATM services are described in Chapter 36, “Configuring ATM Services.” Frame Relay services are described in Chapter 49, “Managing Frame Relay.”

Switch. Provides options to precisely define frame translations. A MAC-layer type (Ethernet, Token Ring, etc.) may have more than one type of frame format, such as Ethernet or 802.3. But, by default, each MAC-layer type defaults to certain frame format upon translation. This menu allows you to define translations for each frame format. This menu is described in Chapter 23, “Configuring Frame Translations.”

Help. Provides textual help on how to use the UI and on each menu or sub-menu. For the item of interest, enter

help <sub-menu name>

Diag. This menu, fully available to the **diag** login account, contains commands to run diagnostic tests. It is described in Chapter 58, “Running Hardware Diagnostics.”

Quit. Logs you out of the UI. You can also enter **logout** to exit.

? Displays the options for current menu.

General User Interface Guidelines

You can monitor and configure your switch in the following various ways:

- The User Interface (UI): The UI is the original method of switch configuration. It is a text-based and menu-driven interface to which you can connect through the serial port, through a modem, or over a network via Telnet. You can have up to four simultaneous UI connections to an OmniSwitch. For Release 4.4 and later, the default for switch monitoring is the CLI mode. If you are using a login account with permission to use the UI command, you can enter the UI mode by entering the **ui** command at the CLI system prompt.
- X-Vision: This purchasable network management software program consists of several powerful sub-applications that help you manage and monitor your network. X-Vision allows you to connect and configure multiple switches simultaneously. For more information, refer to X-Vision’s on-line help.
- The Command Line Interface (CLI): The CLI is a new feature included with Release 4.1 that allows you to configure OmniSwitches using single-line text-based commands that are entered through the local console. Improved readability, easy text editing of the configuration files, and simple cloning of switch configurations are among some of the advantages of the CLI. For more information, refer to the *Text-Based Configuration CLI Reference Guide*.

Entering Command Names

The UI is not case sensitive for commands, meaning that you may enter upper or lower case as you desire. However, command line assignments, configuration input, and logins *are* case sensitive.

Except for the **logout** and **quit** commands, you only need to enter as much of the command that is unique. For example, if you want to execute the **switch** command you need only enter **swi**. If you enter only **sw**, the system will respond with a choice of the following:

switch	swch	swchmac	swap
---------------	-------------	----------------	-------------

If you set the switch to the verbose mode you will see additional information on the screen (see Setting Verbose/Terse Mode for the User Interface on page 8-26).

Non-unique command match, possible commands:

switch	Enter Any to Any Switching Menu
swch	Configure Any To Any Switching Port Translations
swchmac	View Per Mac Translation Options
swap	Change swap status of chassis
swlogc	Configure Switch Logging source/destination mapping and priority levels

◆ Note ◆

If you cannot see a UI command confirmation prompt or if you do not get the command prompt after the completion of a command, press the **<Enter>** key to regain the prompt.

Quitting a Command

Many of the commands give you a list of parameters to change. With most commands you can enter in **quit** if you want to exit the command without making changes. If the **quit** parameter is not available, press **Ctrl-d** to abort the command without making changes.

Scrolling

If the screen scrolls up too far to read you can stop the incoming data by pressing **Ctrl-s**. The screen will stop and allow you to read the data. Press **Ctrl-q** to continue the data transmission.

The UI Configuration Menu

The User Interface (UI) Configuration menu consolidates the following UI commands into a single, easy-to-use menu:

- **chpr**
- **more**
- **ver**
- **ter**
- **timeout**

◆ Note ◆

The switch's *prompt*, *more*, *verbose/terse*, and *timeout* functions remain fully supported. However, if you enter any of the commands listed above, you will be redirected to the UI Configuration menu.

To access the UI Configuration menu, type

uic

at the system prompt and press **<Enter>**. The following screen will be displayed:

UI Configuration

```
1) Prompt : '$Menu-Path%'
2) More   : on
  21) Lines : 22 lines
3) Verbose : off
4) Timeout : 5 minutes
```

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Refer to the following sections for information on using the UI Configuration menu.

Configuring the System Prompt

The **uic** submenu is listed under the system menu. The **uic** submenu allows you to change the system prompt. The prompt can be made up of literal information, system variable information, or a combination of the two.

Literal information means that the prompt will reflect exactly what you type at the **uic** submenu. For example, **Marketing 1** or **Enter command:**.

System variable information means that the prompt will reflect the switch's variable information, such as the current menu-path or the system name. Use **\$Menu-Path** (case sensitive) to have the system prompt display the current menu-path name. Use **\$SysName** to have the system prompt display the system name.

You can also mix variables and literals such as **\$Menu-Path ->** or **\$SysName Enter command:**.

◆ Note ◆

The default system prompt is **->**.

To change the system prompt, type **uic** at the user prompt and press **<Enter>**.

A screen similar to the following will be displayed.

UI Configuration

```
1) Prompt : '$Menu-Path%'
2) More   : on
  21) Lines : 22 lines
3) Verbose : off
4) Timeout : 5 minutes
```

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Next, type **1=**, followed by the desired prompt information, and press **<Enter>**. For example:

```
1=$SysName ->
```

After you press **<Enter>**, the screen will be redrawn. Note that the prompt information at line 1 of the **uic** submenu has been changed.

UI Configuration

```
1) Prompt : '$SysName ->'
2) More   : on
  21) Lines : 22 lines
3) Verbose : off
4) Timeout : 5 minutes
```

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Type **save** at the submenu prompt and press **<Enter>**. The system prompt has been successfully changed.

Configuring More Mode for the User Interface

Enabling More Mode

The more mode allows you to specify the maximum number of lines that will be scrolled to your workstation's display. However, before you can specify the maximum number of lines that can be displayed, you must first verify that the more mode is enabled. To enable the more mode, type **uic** at the user prompt and press **<Enter>**. A screen similar to the following will be displayed.

UI Configuration

```
1) Prompt : '$Menu-Path%'
2) More   : off
  21) Lines : 22 lines
3) Verbose : off
4) Timeout : 5 minutes
```

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Next, type **2=on** at the submenu prompt and press **<Enter>**. The screen will be redrawn. Note that more mode is now set to **on**.

UI Configuration

```
1) Prompt : '$Menu-Path%'
2) More   : on
  21) Lines : 22 lines
3) Verbose : off
4) Timeout : 5 minutes
```

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

The switch's default output display is 22 lines. If you want to change this value, type **21=**, followed by the maximum number of lines to be displayed, and press **<Enter>**. For example:

21=50.

After you press **<Enter>**, the screen will be redrawn. Note that the output display value at line 21 of the **uic** submenu has been changed.

UI Configuration

```
1) Prompt : '$Menu-Path%'
2) More   : on
  21) Lines : 50 lines
3) Verbose : off
4) Timeout : 5 minutes
```

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Be sure to type **save** at the submenu prompt and press **<Enter>**. More mode is now enabled.

Changing the More Mode Line Value

If the switch's more mode has already been enabled and you want to change the maximum number of lines to be displayed on your workstation, type **uic** at the user prompt and press **<Enter>**.

A screen similar to the following will be displayed.

UI Configuration

- 1) Prompt : '\$Menu-Path%'
- 2) More : on
- 21) Lines : 22 lines
- 3) Verbose : off
- 4) Timeout : 5 minutes

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Type **21=**, followed by the maximum number of lines to be displayed, and press **<Enter>**. (The value may range from 0 to 2147483647.) For example:

21=2000.

After you press **<Enter>**, the screen will be redrawn. Note that the output display value at line 21 of the **uic** submenu has been changed.

UI Configuration

- 1) Prompt : '\$Menu-Path%'
- 2) More : on
- 21) Lines : 2000 lines
- 3) Verbose : off
- 4) Timeout : 5 minutes

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Type **save** at the submenu prompt and press **<Enter>**. The more mode line value has been successfully changed.

Disabling More Mode

To disable more mode, type **uic** at the user prompt and press **<Enter>**.

A screen similar to the following will be displayed.

UI Configuration

```
1) Prompt : '$Menu-Path% '
2) More   : on
  21) Lines : 22 lines
3) Verbose : off
4) Timeout : 5 minutes
```

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Next, type **2=off** at the submenu prompt and press **<Enter>**. The screen will be redrawn. Note that more mode is now set to **off**.

UI Configuration

```
1) Prompt : '$Menu-Path% '
2) More   : off
  21) Lines : 22 lines
3) Verbose : off
4) Timeout : 5 minutes
```

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Type **save** at the submenu prompt and press **<Enter>**. More mode is now disabled.

◆ Reminder ◆

The switch's table filtering feature *cannot* be used when the **more** mode is disabled. For more information on UI table filtering, refer to UI Table Filtering (Using Search and Filter Commands) on page 8-42.

Setting Verbose/Terse Mode for the User Interface

Enabling Verbose Mode

When verbose mode is enabled, you are not required to enter a question mark in order to view the switch's configuration menus. Instead, menus are displayed automatically. For example, if verbose mode is enabled and you enter

summary

at the user prompt, the Summary menu will be displayed automatically, as shown below:

<u>Command</u>	<u>Summary Menu</u>
ss	Display MIB-II System group variables
sc	OmniSwitch chassis summary
si	Current interface status

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

The switch's default verbose mode setting is **off**, or disabled. To enable verbose mode, type **uic** at the user prompt and press **<Enter>**.

A screen similar to the following will be displayed.

UI Configuration

- 1) Prompt : '\$Menu-Path% '
- 2) More : on
 - 21) Lines : 22 lines
- 3) Verbose : off
- 4) Timeout : 5 minutes

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Next, type **3=on** at the submenu prompt and press **<Enter>**. The screen will be redrawn. Note that verbose mode is now set to **on**.

UI Configuration

- 1) Prompt : '\$Menu-Path% '
- 2) More : on
 - 21) Lines : 22 lines
- 3) Verbose : on
- 4) Timeout : 5 minutes

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Type **save** at the submenu prompt and press **<Enter>**. You will be returned to the user prompt. Verbose mode is now enabled.

Disabling Verbose Mode

Although the **terse** command is no longer supported as of Release 4.1, disabling verbose mode via the **uic** submenu is the command equivalent. When verbose mode is disabled, configuration menus *will not* be displayed automatically. To display a current menu when verbose mode is disabled, you must type a question mark (?) and then press **<Enter>**.

To disable verbose mode, type **uic** at the user prompt and press **<Enter>**.

A screen similar to the following will be displayed.

UI Configuration

- 1) Prompt : '\$Menu-Path% '
- 2) More : on
 - 21) Lines : 22 lines
- 3) Verbose : on
- 4) Timeout : 5 minutes

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Next, type **3=off** at the submenu prompt and press **<Enter>**. The screen will be redrawn. Note that verbose mode is now set to **off**.

UI Configuration

- 1) Prompt : '\$Menu-Path% '
- 2) More : on
 - 21) Lines : 22 lines
- 3) Verbose : off
- 4) Timeout : 5 minutes

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Type **save** at the submenu prompt and press **<Enter>**. Verbose mode is now disabled.

Configuring the Auto Logout Time

When the switch detects no user activity on the UI for a certain period of time, it automatically logs the user out of the system. By default, this automatic logout occurs after 4 minutes of console inactivity. You can configure the automatic logout to range from 1 minute to 35,791,394 minutes.

To set a new automatic logout time, type **uic** at the user prompt and press **<Enter>**.

A screen similar to the following will be displayed.

UI Configuration

```
1) Prompt : '$Menu-Path% '
2) More   : off
  21) Lines : 22 lines
3) Verbose : off
4) Timeout : 5 minutes
```

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Next, type **4=on**, followed by the desired automatic logout time, and press **<Enter>**. For example:

```
4=15.
```

After you press **<Enter>**, the screen will be redrawn. Note that the automatic logout time at line 4 of the **uic** submenu has been changed.

UI Configuration

```
1) Prompt : '$Menu-Path% '
2) More   : on
  21) Lines : 22 lines
3) Verbose : off
4) Timeout : 15 minutes
```

Command {Item=Value/?/Help?Quit?Redraw?Save} (Redraw) :

Be sure to type **save** at the submenu prompt and press **<Enter>**. The automatic logout time has been successfully changed.

◆ Note ◆

The automatic logout value you enter takes effect immediately; you do not have to reboot the switch. In addition, the timeout parameter you enter is saved. Later sessions using this account will have the same automatic logout parameter until you change it.

Viewing Commands

If at any time you are not sure of the commands available, enter **?** and you will be given a list of the commands in the current sub-menu. Following each list of commands is a list of sub-menus. You can go directly to any sub-menu in the list.

You can specify whether the full menu will be displayed when you enter a command for a menu or sub-menu and the amount of information you receive when you run the help command. (Refer to Setting Verbose/Terse Mode for the User Interface on page 8-26 for more information.) Additionally, there is a lookup facility to assist with administrative tasks. You can look up any command name or prefix as follows:

lookup vlans

or to see all commands starting with **v** use:

lookup v*

To see all commands available, enter:

lookup *

Changing Passwords

The **pw** command is used to change passwords and is described in Chapter 12, “Switch Security.”

Command History and Re-Executing Commands

The **history** command displays up to 50 commands numbered in order with the most recently executed command listed last. The following is a typical example of the **history** command.

```
1: view mpm.cmd
2: vlan
3: at
4: atvl
5: vimcvi
6: mcvi
7: vivi
8: fwtvl
9: xlat
10: history
```

In the example above, the **history** command is listed last because it is the one that was executed most recently. If you want to re-execute the last command, enter two exclamation points (!!). In the example above, you could re-execute the **history** command by entering

```
!!
```

at the system prompt.

You can also display a specific number of commands by entering **history** followed by a number less than or equal to the number of commands in the history buffer. For example, if you entered

```
history 5
```

in the example above you would see the following:

```
7: vivi
8: fwtvl
9: xlat
10: history
11: history 5
```

The UI also provides several other ways to re-execute earlier commands. For example, you can re-execute a specific command shown in the **history** list by entering an exclamation point (!) followed by the number to the left of that command shown in the **history** list. In the example at the beginning of this section, entering

```
!2
```

would re-execute the **vlan** command.

You can also re-execute a command a set number of commands back by entering an exclamation point and a minus sign (!-) followed by that set number of commands back. In the example at the beginning of this section, entering

```
!-3
```

would re-execute the **fwtvl** command.

In addition, you can re-execute a command by entering an exclamation point (!) followed by the first character(s) of the most recently executed command. In the example at the beginning of this section, entering

!vim

would re-execute the **vimcvl** command. Entering

!vi

however, would re-execute the **vi** command because it is the most recently executed command beginning with **vi**.

You can also re-execute the most recently executed command containing a string of characters by entering an exclamation point and a question mark (!?), followed by the string of characters, and an optional question mark (?) which acts as a “wild card.” In the example at the beginning of this section, entering

!?!an?

at the system prompt would re-execute the **vlan** command. Entering

!?!a?

however, would re-execute the **xlat** command because it is the most recently executed command containing **la**.

Commands in the history buffer can be modified by adding a parameter, when it is applicable. For example, if you entered

!7 3/1

in the example at the beginning of this section you would execute the command **vim 3/1**.

Abbreviating IP Addresses

The OmniSwitch software provides the user with a more concise way to enter the dotted decimal format of a 32-bit IP address. The new syntax conforms to the traditional Internet interpretation. Several examples of abbreviated IP addresses are shown in the table below. The first column of the table lists examples of abbreviated IP addresses, and the second column shows how the system interprets the abbreviated address.

Abbreviated IP Address Formats

Sample User Entry	IP Address
198	0.0.0.198
198.	198.0.0.0
198..	198.0.0.0
198...	198.0.0.0
198.206	198.0.0.206
198..206	198.0.0.206
198..206.	198.0.206.0
198...206	198.0.0.206
198.206.	198.206.0.0
198.206..	198.206.0.0
198.206.182	198.206.0.182
198..206.182	198.0.206.182
198.206..182	198.206.0.182
198.206.182.	198.206.182.0
198.206.182.158	198.206.182.158

As shown in the table above, the system performs two important steps to ensure that the IP address is valid. First, it puts zeroes when you do not specify the number. Second, the system will insert as many zeroes as needed to the right of a period.

This abbreviated IP address format can be used with the **ftp**, **telnet**, **crpg**, **modvl**, **ping**, **snmpc**, and **xlat** commands. For example, to ping the IP address 198.0.0.2, you can abbreviate this IP address by entering

```
ping 198.2
```

at the system prompt. After you answer a few prompts (see Chapter 30, “IP Routing” for more information on the **ping** command), something similar to the following will be displayed.

```
Ping starting, hit <Enter> to stop  
PING 198.0.0.2: 64 data bytes
```

```
[0 ] T
```

```
----198.0.0.2 PING Statistics----
```

```
1 packets transmitted, 0 packets received, 100% packet loss
```

In addition, the IP subnet mask 255.255.0.0 can be abbreviated in the following ways:

- 255.255.
- 255.255..

User Interface Display Options

The System menu several commands to configure help information, character display, and the system prompt for the UI. Enter

system

at the system prompt to enter the System menu. Press the question mark (?) to see the System menu commands, as shown below.

<u>Command</u>	<u>System Menu</u>
info	Basic info on this system
dt	Set system date and time
ser	View or configure the DTE or DCE port
mpm	Configure a Management Processor Module
slot	View Slot Table information
systat	View system stats related to system, power and environment
taskstat	View task utilization stats
memstat	View memory use statistics
fsck	Perform a file system check on the flash file system
newfs	Erase all files from /flash & create a new file system
syscfg	View/Configure info related to this system
uic	UI configuration; change - prompt, timeout, more, verbose.
camstat	View CAM info and usage
camcfg	Configure CAM info and usage
hrex	Enter HRE-X management command sub-menu
ver/ter	Enables/disables automatic display of menus on entry (obsolete, use 'uic' command)
echo/noecho	Enable/disable character echo
chpr	Change the prompt for the system (obsolete, use 'uic' command)
logging	View system logs.
health	Set health parameters or view health statistics
cli/exit	Enter command line interface
saveconfig	Dump the cache configuration content to the mpm.cfg file.
cacheconfig	Set the flag to use cache configuration only.

Main File Summary VLAN Networking
Interface Security System Services Help

For information on the **info**, **dt**, **ser**, **slot**, **systat**, **taskstat**, **memstat**, **fsck**, **newfs**, **syscfg**, **camstat**, **camcfg**, and **hrex** commands, refer to Chapter 13, “Switch-Wide Parameters.” The **mpm** command is described in Chapter 10, “Configuring Management Processor Modules.” The **ver/ter** and **chpr** commands are described earlier in Setting Verbose/Terse Mode for the User Interface on page 8-26. The **echo/noecho** command is described in the following section. The **cli** command is described earlier in Changing Between the CLI and UI Modes on page 8-1. The **logging** command is described in Chapter 14, “Switch Logging.”

◆ **Note** ◆

The **ver/ter**, and **chpr** commands now appear as items in the UI Configuration menu (displayed through the **uic** command). If you enter the **ver/ter** and **chpr** commands, a message will advise you to use the **uic** command, and the UI Configuration menu will automatically display. For more information on the UI Configuration menu, refer to The UI Configuration Menu on page 8-21.

Setting Echo/NoEcho for User Entry

You can determine whether your entries will appear by enabling the echo for user entries. The default is to echo all characters.

To enable the echo, enter

```
echo
```

at the system prompt. Everything you enter will be displayed. For example, if you enter

```
history
```

at the system prompt, it will be displayed on your terminal, as shown in the example below.

```
/%history
```

If your terminal echoes characters locally it is a good idea to set the UI to **noecho** to avoid repeated characters. To disable the echo, enter

```
noecho
```

at the system prompt. For example, if your terminal echoes characters locally, you would see something like the following if you entered **history**.

```
/%history
```

If your terminal does not echo characters locally, nothing you enter will be displayed. For example, if you enter

```
history
```

at the system prompt, it will *not* be displayed on your terminal, as shown in the example below.

```
/%
```

Setting the Login Banner

The login banner feature allows you to change the banner that displays whenever someone logs into the UI. This feature can be used to display messages about user authorization and security. You can display the same message for all login sessions or you can display different messages for login sessions initiated by the console, ftp or Telnet access. The default login message looks like this:

```
This product includes software developed by the University of California  
Berkeley and its contributors.
```

```
Welcome to the Alcatel Omni Switch/Router ! Version 4.4
```

```
login:
```

Here is an example of a banner that has been changed:

```
This product includes software developed by the University of California  
Berkeley and its contributors.
```

```
*** LOGIN ALERT ***
```

```
This is a secure device. Unauthorized use of this switch will result  
in criminal prosecution.
```

```
login:
```

Creating a new Banner

Three steps are required to change the login banner. They are listed here.

- Create a text file containing the new banner in the switch's flash directory.
- Add the **UI_add_do_alert()** command syntax to the switch's `mpm.cmd` file.
- Enable the feature by executing the **alert {console | telnet | ftp}** command.

To create the text file containing your banner you may use the **create file** command in the UI's edit buffer sub-menu. This method allows you to create the file in the flash directory without leaving the UI console session. You can also create the text file in an external editor (such as MS Wordpad) and ftp the file to the switch's flash directory. In either case, be sure to remember the name of your file.

To add the **ui_add_do_alert()** command syntax to the switch's `mpm.cmd` file, use the edit command of the UI's **file** sub-menu. (For information on using the file sub-menu, refer to Chapter 11, "Managing Files").

To enable the new login banner, add the **alert {console |telnet | ftp}** syntax to the `mpm.cmd` file, using the **edit** command of the UI's **file** sub-menu. This command will cause the banner message to display at each login until the switch is rebooted. After a reboot, the switch will not display the banner unless the **alert** command is executed again.

Permanent Banner

If you want the banner message to display after the system has been rebooted, you must add additional lines to the `mpm.cmd` file. The following example lists the commands you must add to the `mpm.cmd` file. This example uses a banner text file with the name "**banner.txt**".

```
cmDoDump=1
cmlnit
ui_add_do_alert()
change_prompt_file("console", "banner.txt")
change_prompt_file("telnet", "banner.txt")
```

◆ Note ◆

Any commands added to the `mpm.cmd` file must be added after the lines **cmDoDump=1** and **cmlnit**. If the commands in the `mpm.cmd` file are not in the proper order the switch may not boot properly.

Banners for Different Access Methods

You may use different banners for sessions accessed by console, Telnet or ftp methods. To do this, create different text files for each banner with unique filenames. When you add the commands to the `mpm.cmd` file, use the filenames to associate the banner with the session access methods. Here is an example:

```
cmDoDump=1
cmlnit
ui_add_do_alert()
change_prompt_file("console", "console_banner.txt")
change_prompt_file("telnet", "telnet_banner.txt")
change_prompt_file("ftp", "telnet_banner.txt")
```

Login Accounts

The UI provides three default login accounts—Administrator, User and Diagnostics. The Administrator login provides full access to all functions. The initial login name for an Administrator account is **admin**. The Diagnostics login also has full access to all switch functions plus a special sub-menu with a set of switching module tests. The initial login name for Diagnostics is **diag**. The User login has read-only privileges to the switch. The initial login name for a User account is **user**. The password for each of these default login accounts is **switch**.

◆ **Note** ◆

In software release 4.3, the **user** login account with read-only privileges is not included automatically.

◆ **Note** ◆

You can configure new and delete existing login accounts with the **useradd** UI command, that is described in Chapter 12, “Switch Security.”

Multiple User Sessions

You can have up to four simultaneous connections to an OmniSwitch or an Omni Switch/Router, and up to three simultaneous connections to an OmniStack. One connection can be made to the console port, two can be made through Telnet, and one connection can be made to the modem port if you are connecting to an OmniSwitch or an Omni Switch/Router.

◆ **Note** ◆

For software Releases 4.4 and later, more than one login account with write privileges *can be* active at the same time.

For software Release 4.3 and earlier, only one login account with write privileges was allowed on the switch at the same time. In this case, the first switch user who logged on as either **admin** or **diag** would be the only user with the write privilege. Subsequent users who logged on as either **admin** or **diag** would not have the write privilege and would be unable to perform any functions that change switch parameters. These users would also see a message that informs them they do not have the write privilege when they log on. For example, a user who logs on as **admin** when another user already has the write privilege will see the following message:

You are logged in as 'admin' without the WRITE privilege.

The WRITE privilege is currently in use by another user.

However, users who log on as either **admin** or **diag** without the write privilege can “kill” the session of the user with the write privilege and gain that privilege for themselves. This is described in Deleting Other Sessions on page 8-39.

If you try to log on when the limit of user has been reached (e.g., you attempt a Telnet connection when there are two users currently connected through Telnet), you will see the following message:

Sorry, reached maximum number of sessions.

Listing Other Users

To display all the users currently logged on to the switch, type

```
who
```

at the system prompt. The following is an example of the display shown where two Telnet sessions are logged in, one as **admin** and the other as **user**.

SESSION	USER	READ	PRIVILEGES WRITE	GLOBAL	TTY
3	admin (123.456.78.910)	000000008007ffffd	000000008007ffffd	0000000007fffff	/pty/telnetA
4	rrtest1 (123.456.78.910)	000000008007ffffd	000000008007ffffd	0000000000000000	/pty/telnetB

You can also display information about just your session by typing

```
who am i
```

at the system prompt. The following is a typical example of the output.

SESSION	USER	READ	PRIVILEGES WRITE	GLOBAL	TTY
3	admin (123.456.78.910)	000000008007ffffd	000000008007ffffd	0000000007fffff	/pty/telnetA

The following sections describe the parameters shown by the **who** command.

SESSION. The session number of the user. A **0** indicates that the user is connected through the console port, a **1** indicates that the user is connected through the modem port, and a **2** or **3** indicates that the user is connected through Telnet. The session number is used with the **write** and **kill** commands described in Communicating with Other Users on page 8-39 and Deleting Other Sessions on page 8-39, respectively.

USER. The administrative level of the user. This will be **admin**, **user** or **diag**.

PRIVILEGES. The privilege level of the user. The **READ**, **WRITE** and **GLOBAL** privileges are indicated in hexadecimal numbers.

TTY. Type of connection. This shows whether the user is connected by Telnet, the modem port, or the console port. If the connection is via Telnet, the IP address of the connecting workstation is also shown.

Communicating with Other Users

If you want to send a message to another user, enter **write** followed by the user's session number. If you wanted to send a message to a user connected on the console port (session 0), you would enter

```
write 0
```

at the system prompt. The switch would then display

```
Enter message. (End with CTRL-D or 'exit')
```

Everything you type now will be sent to the user connected on the console port until you press **CTRL-D** or enter **exit** on a line by itself. Here is an example of the **write** command:

```
write 0
I need the write privilege
exit
```

The user receiving the message would see the following:

```
Message from user 'admin' on session 3.
I need the write privilege
End of message.
```

If you enter an invalid session number, the switch will display an error message. For example, if you entered

```
write 1
```

at the system prompt and no user was connected through the modem port (session 1), the switch would display

```
ERROR: Session 1 is an invalid session number.
```

Note

After you have received a message or after you have written a message you must press the **<Enter>** key to regain the system prompt.

Deleting Other Sessions

If you are logged on as **admin** or **diag**, you can kill the session of another user. For example, if you want the write privilege and you are logged on as **diag** or **admin**, you must end the session of the user who currently has the write privilege with the **kill** command. The syntax for the **kill** command is as follows:

```
kill [-t <timeout>] -f <session_number>
```

The **session_number** is assigned by the switch and can be displayed with the **who** command, which is described in Listing Other Users on page 8-38. If you do not use the **-f** option, then the system will wait until the other user presses **<Enter>** or finishes his current command. If you do use this option, then the other user's session will be terminated immediately.

The **-t** option can be used with the **-f** option to set the amount of time before the other user's session is terminated. See Advanced Kill Command Options on page 8-41 for descriptions of the **-f** and **-t** options.

Multiple User Sessions

For example, to end the session of the user connected to the console port (session 0) and let him finish his current command, you would enter

kill 0

at the system prompt. The system would then display something similar to the following:

Press <Enter> to cancel.

Trying.....

The user losing the write privilege would see something similar to the following:

**Your session will be killed by user 'admin' on session 3
as soon as you finish this command or press return.**

After the user with the session being killed has finished his work, he will be logged off. If the user who was logged off had the write privilege, you will gain the write privilege and a message similar to the following will be displayed.

Done.

You have gained the WRITE privilege

You can use the **who** command to confirm that you now have the write privilege.

In addition, the session number used in the **kill** command must be valid. If, for example, you entered

kill 1

and no user was connected to the modem port (session 1), the system would display the following:

ERROR: Session 1 is an invalid session number.

Also, you cannot use the **kill** command to end your own session. For example, if your session number is **3** and you entered

kill 3

the system would display the following:

ERROR: You cannot kill your own session.

Instead, use the **quit** or **logout** command if you want to log out.

Advanced Kill Command Options

You can also kill the session of a user immediately by adding the parameter **-f** followed by the session number of the user. This option will kill the user's session before he can finish his current command. In addition, this option will end the user's sessions without waiting for him to press **<Enter>**. This option can be used to log off a user with the write privilege who forgot to log out and then gain the write privilege for yourself.

If you wanted to kill the session of the user with a session number of 2 immediately, you would enter

```
kill -f 2
```

at the system prompt.

The default timeout for the **kill** command is 2 seconds. You can modify the duration of the timeout by using **-t** option in conjunction with the **-f** option. To use the timeout option, enter **kill**, followed by **-t**, the number of seconds for the timeout, **-f**, and the session number of the user. For example, if you wanted to kill the session of the user with a session number of 2 in 15 seconds, you would enter

```
kill -t15 -f 2
```

at the system prompt. The valid range for the timeout is 1 to 240 seconds.

◆ Note ◆

You *cannot* use the timeout option (**-t**) unless you also use the **-f** option.

UI Table Filtering (Using Search and Filter Commands)

The amount of information displayed in UI tables can be extensive, especially with larger networks. Common UI commands, such as **ipr**, **vipl**, **macinfo**, and **fwl**, often return multi-page tables. The user can locate specific information in these large tables through the **More?** UI prompt.

The **More?** prompt appears whenever the maximum number of table entries designated by the **more** command has been reached (the **more** command's default is 22 lines). Note that if a table exceeds 22 lines, and the **more** mode has been configured to display *more than* 100 lines, the following message appears:

Screen Size larger than 100 Lines, Displaying with 22 Lines (Press Any Key)

After pressing any key, only the page of the table is displayed, followed by the **More?** prompt.

◆ Important Note ◆

The switch's **more** mode is active by default. If the **more** mode is turned off, the Search and Filter commands cannot be used. For more information on the **more** command, see The UI Configuration Menu on page 8-21.

A typical **More?** UI prompt will look like this:

```
1 4/6 Brg/ 1/ na 0020da:030995 Tns DFLT Enabl Inactv Disabl AutoSw
1 4/7 Brg/ 1/ na 0020da:030996 Tns DFLT Enabl Inactv Disabl AutoSw
1 4/8 Brg/ 1/ na 0020da:030997 Tns DFLT Enabl Inactv Disabl AutoSw
1 5/1 Brg/ 1/ na 0020da:954050 Tns DFLT Enabl Inactv Disabl AutoSw
More? [<SP>,<CR>,/,F,N,Q,?]
```

At the **More?** prompt, the user is given a list of options, which includes the Search (**I**) and Filter (**F**) commands:

- <SP>** Press **<SP>** (space bar) to display the next page of information.
- <CR>** Press **<CR>** (character return) to display the next line of information.
- I** Press **I** to enter the Search mode.
- F** Press **F** to enter the Filter mode.
- N** Press **N** to renew the search, starting from the next line in the UI table.
- Q** Press **Q** to exit the **More?** prompt.
- ?** Press **?** to enter the **More?** command Help Menu.

These commands are available for **admin** and **diag** login sessions. Please refer to the following sections for more information on the Search and Filter commands, as well as renewing a search, combining Search and Filter commands, and using wildcards.

The Search Command

Starting from the page being displayed, the Search command (*/*) searches all lines of a UI table for a specified text pattern (up to 80 characters). The first line containing the pattern is brought to the top of the page, followed by any remaining lines in the table.

Searches *cannot* be limited to a specific column or heading.

To use the Search command, type */* at the **More?** prompt, followed by the text pattern you are looking for, then press **<Enter>**.

◆ Important Note ◆

The Search command is case sensitive. When using this command, be sure to type the text pattern exactly as it would appear in the UI table.

Real World Example

The following example uses the Search command to locate a specific MAC address in the **macinfo** table. (Before using this example, be sure that the **more** mode is enabled and the default is set at 22 lines. For more information, refer to page 8-42.)

1. Type **macinfo** and press **<Enter>**. The following screen will be displayed:

Enter MAC address ([XXYYZZ:AABBCC] or return for none) :

Press **<Enter>** again. A screen similar to the following will be displayed:

Enter Slot Number (1-5) :

Type the slot number for the module containing the relevant MAC address information (e.g. **3**), then press **<Enter>**. A table similar to the following will be displayed:

Total number of MAC addresses learned for this slot: 58

Sl/ If/ Service/ In	MAC Address	Non-Canonical MAC Address	T	Group ID	CAM Indx	S	Last Seen	Exp Timer
3/ 1/ Brg/ 1	00A0C9:064D04	000593:60B220	E	1	7024	T	134	300
3/ 1/ Brg/ 1	006008:C1D7C2	000610:83EB43	E	1	7030	T	115	300
3/ 1/ Brg/ 1	0020DA:88F110	00045B:118F08	E	1	70E6	T	46	300
3/ 1/ Brg/ 1	0020DA:B6FF12	00045B:6DFF48	E	1	7094	T	66	300
3/ 1/ Brg/ 1	0020DA:8A7DC0	00045B:51BE03	E	1	705A	T	83	300
3/ 1/ Brg/ 1	0020DA:A67FA2	00045B:65FE45	E	1	7120	T	27	300
3/ 1/ Brg/ 1	0020DA:024F75	00045B:40F2AE	E	1	710C	T	34	300
3/ 1/ Brg/ 1	0020DA:9B88E4	00045B:D91127	E	1	70EE	T	45	300
3/ 1/ Brg/ 1	0020DA:9C062B	00045B:3960D4	E	1	7074	T	76	300
3/ 1/ Brg/ 1	0020DA:79F062	00045B:9E0F46	E	1	70D2	T	52	300
3/ 1/ Brg/ 1	006008:991CA7	000610:9938E5	E	1	701C	T	117	300
3/ 1/ Brg/ 1	0020DA:936A8F	00045B:C956F1	E	1	712A	T	23	300
3/ 1/ Brg/ 1	0020DA:9CEAC5	00045B:3957A3	E	1	70CC	T	53	300
3/ 1/ Brg/ 1	0020DA:9B9B54	00045B:D9D92A	E	1	70D6	T	50	300
3/ 1/ Brg/ 1	0020DA:7AAE24	00045B:5E7524	E	1	70B8	T	58	300
3/ 1/ Brg/ 1	0020DA:A9EEB3	00045B:9577CD	E	1	710A	T	34	300
3/ 1/ Brg/ 1	0020DA:8DB20B	00045B:B14DD0	E	1	7080	T	72	300
3/ 1/ Brg/ 1	0020DA:9F6B82	00045B:F9D641	E	1	70F4	T	42	300
3/ 1/ Brg/ 1	0020DA:8762A3	00045B:E146C5	E	1	7126	T	24	300
3/ 1/ Brg/ 1	006008:C1D7C2	000610:83EB43	E	1	7030	T	115	300

More? [**<SP>**,**<CR>**,**/**,**F**,**N**,**Q**,**?**]

Note that, because the information in the table exceeds the **more** command's default page size of 22 lines, the **More?** prompt appears at the bottom of the screen.

UI Table Filtering (Using Search and Filter Commands)

2. Type `/` at the **More?** prompt. The Search prompt (`/`) will appear automatically. At the Search prompt, enter the text pattern for the desired MAC address. For example:

```
/0020DA:9E479D
```

Press `<Enter>`. A screen similar to the following will be displayed:

```
Searching .....
```

```
3/ 1/ Brg/ 1 0020DA:9E479D 00045B:79E2B9 E 1 702C T 138 300
3/ 1/ Brg/ 1 0020DA:9D0D1B 00045B:B9B0D8 E 1 7030 T 67 300
3/ 1/ Brg/ 1 0020DA:97CDE0 00045B:E9B307 E 1 70E6 T 122 300
3/ 1/ Brg/ 1 00A0C9:8DED5B 000593:B1B7DA E 1 7094 T 114 300
3/ 1/ Brg/ 1 0020DA:92A152 00045B:49854A E 1 705A T 97 300
3/ 1/ Brg/ 1 0020DA:8528D5 00045B:A114AB E 1 7120 T 102 300
3/ 1/ Brg/ 1 0020DA:93BF73 00045B:C9FDCE E 1 710C T 130 300
3/ 1/ Brg/ 1 0020DA:B956B5 00045B:9D6AAD E 1 70EE T 56 300
3/ 1/ Brg/ 1 0020DA:730F03 00045B:CEF0C0 E 1 7074 T 68 300
3/ 1/ Brg/ 1 0020DA:8BA710 00045B:D1E508 E 1 70D2 T 99 300
```

Note that the line containing information for the specified MAC address (**0020DA:9E479D**) now appears at the top of the screen, followed by any remaining lines in the UI table. (In this case, the last line of the **macinfo** UI table contains MAC address **0020DA:8BA710**, as shown).

Renewing a Search

If you execute the Search command and the resulting page still exceeds the maximum number of table entries designated by the **more** command, you can renew the Search. Do this by typing `n` at the **More?** prompt. The Search command will scan the remainder of the table and display the next line containing the desired text pattern at the top of the screen.

The Filter Command

The Filter command filters unwanted information from a UI table by displaying only those lines containing a specified text pattern (up to 80 characters). Once the Filter command has been executed, the Filter mode remains active until the end of the UI table has been reached, or until the user exits the current UI table.

Like the Search command, the Filter command *cannot* be limited to a specific column or heading.

To use the Filter command, type **f** at the **More?** prompt, followed by the text pattern you want displayed in the UI table, then press **<Enter>**.

◆ Important Note ◆

The Filter command is case sensitive. When using this command, be sure to type the text pattern exactly as it would appear in the UI table.

Real World Example

The following example uses the Filter command to display only those lines containing Lane services in the **vi1** table. (Before using this example, be sure that the **more** mode is enabled and the default is set at 22 lines. For more information, refer to page 8-42.)

1. Type **vi1** and press **<Enter>**. A table similar to the following will be displayed:

Virtual Interface VLAN Membership					
Slot / Intf / Service / Instance	Group	Member of VLAN#			
1 /1 /Rtr /1	1	1			
1 /1 /Rtr /2	33	1			
1 /1 /Rtr /3	111	1			
1 /1 /Rtr /4	33	2			
1 /1 /Rtr /5	1	3			
1 /1 /Rtr /6	1	4			
1 /1 /Rtr /7	33	7			
1 /1 /Rtr /8	33	3			
1 /1 /Rtr /9	1	5			
1 /1 /Rtr /10	1	6			
1 /1 /Rtr /11	33	5			
1 /1 /Rtr /12	33	6			
1 /1 /Rtr /13	999	1			
2 /1 /Lne /1	1	1			
2 /1 /Lne /2	111	1			
3 /1 /Brg /1	33	1 4			
3 /2 /Brg /1	1	1			
3 /3 /Brg /1	1	1			
3 /4 /Brg /1	1	1			

More? [**<SP>**,**<CR>**,/,F,N,Q,?]

Note that, because the information in the table exceeds the **more** command's default of 22 lines, the **More?** prompt appears at the bottom of the screen.

UI Table Filtering (Using Search and Filter Commands)

2. Type **f** at the **More?** prompt. The Filter prompt (**f/**) will appear automatically. At the Filter prompt, enter the desired text pattern (remember to type the text pattern exactly as it would appear in the UI table):

f/Lne

Press **<Enter>**. A screen similar to the following will be displayed:

Filtering

```
2 /1 /Lne /1 1 1
2 /1 /Lne /2 111 1
/ %
```

Note that only those lines containing Lane services are now displayed on the screen. All other table entries have been filtered from the UI.

Combining Search and Filter Commands

If you receive a **More?** prompt after using the Filter command, the filtered information still exceeds the maximum number of table entries designated by the **more** command. To further refine your results, you can combine the Search and Filter commands.

To combine the Search and Filter commands, type **/** at the Filter mode's **More?** prompt, followed by a revised text pattern of up to 80 characters. Note that you can combine the Search and Filter commands only after you have executed a Filter command *and* received a **More?** prompt at the bottom of the resulting page.

◆ Reminder ◆

Both the Search and Filter commands are case sensitive. When using these commands, be sure to type the text pattern exactly as it would appear in the text UI table.

Real World Example

The following example combines the Search and Filter commands to find specific IP address information in the **ipr** table. (Before using this example, be sure that the **more** mode is enabled and the default is set at 22 lines. For more information, refer to page 8-42.)

1. Type `ipr` and press `<Enter>`. A table similar to the following will be displayed:

IP ROUTING TABLE

128 routes in routing table

Network	Mask	Gateway	Metric	Group:VLAN	
				Id	Protocol
155.5.0.0	255.255.0.0	155.5.4.33	1	1:5	DIRECT
155.6.0.0	255.255.0.0	155.6.4.33	1	1:6	DIRECT
155.155.0.0	255.255.0.0	155.155.4.33	1	1:1	DIRECT
172.17.0.0	255.255.0.0	172.17.6.122	1	999:1	DIRECT
172.31.0.0	255.255.0.0	172.31.4.33	1	33:3	DIRECT
172.32.0.0	255.255.0.0	172.32.4.33	1	33:2	DIRECT
172.33.0.0	255.255.0.0	172.33.4.33	1	33:1	DIRECT
172.35.0.0	255.255.0.0	172.35.4.33	1	33:5	DIRECT
172.36.0.0	255.255.0.0	172.36.4.33	1	33:6	DIRECT
172.37.0.0	255.255.0.0	172.37.4.33	1	33:7	DIRECT
172.111.0.0	255.255.0.0	172.111.4.33	1	111:1	DIRECT
198.168.12.0	255.255.0.0	192.168.12.1	1	1:1	DIRECT
198.168.13.0	255.255.0.0	192.168.13.1	1	1:1	DIRECT

More? [`<SP>`;`<CR>`;`!``F``N``Q``?`]

Note that, because the information in the table exceeds the `more` command's default of 22 lines, the `More?` prompt appears at the bottom of the screen.

2. Use the Filter command to display all IP network addresses within the **IP Routing** table that contain **198**. To do this, type `f` at the `More?` prompt, followed by the specified text pattern:

`f/198`

Press `<Enter>`. A screen similar to the following is displayed:

Filtering

198.168.12.0	255.255.0.0	198.168.12.1	1	1:1	DIRECT
198.168.13.0	255.255.0.0	198.168.13.1	1	1:1	DIRECT
198.168.236.0	255.255.0.0	172.16.255.254	4	1:1	DIRECT
198.168.237.0	255.255.0.0	172.16.255.254	4	1:1	DIRECT
198.168.238.0	255.255.0.0	172.16.255.254	4	1:1	DIRECT
198.168.239.0	255.255.0.0	172.16.255.254	4	1:1	DIRECT
198.168.240.0	255.255.0.0	172.16.255.254	4	1:1	DIRECT
198.168.241.0	255.255.0.0	172.16.255.254	4	1:1	DIRECT
198.168.242.0	255.255.0.0	172.16.255.254	4	1:1	DIRECT
198.206.181.0	255.255.255.0	172.16.255.254	2	1:1	DIRECT
198.206.183.0	255.255.255.0	172.16.255.254	3	1:1	DIRECT
198.206.184.0	255.255.255.0	172.16.255.254	3	1:1	DIRECT
198.206.185.0	255.255.255.0	172.16.255.254	3	1:1	DIRECT
198.206.186.0	255.255.255.0	172.16.255.254	2	1:1	DIRECT
198.206.187.0	255.255.255.0	172.16.255.254	2	1:1	DIRECT
198.206.188.0	255.255.255.0	172.16.255.254	2	1:1	DIRECT
198.206.189.0	255.255.255.0	172.16.255.254	3	1:1	DIRECT
198.206.190.0	255.255.255.0	172.16.255.254	2	1:1	DIRECT
198.206.191.0	255.255.255.0	172.16.255.254	2	1:1	DIRECT
198.206.192.0	255.255.255.0	172.16.255.254	2	1:1	DIRECT
198.206.193.0	255.255.255.0	172.16.255.254	2	1:1	DIRECT
198.206.194.0	255.255.255.0	172.16.255.254	2	1:1	DIRECT

More? [`<SP>`;`<CR>`;`!``F``N``Q``?`]

Because the filtered information in the table still exceeds the `more` command's default of 22 lines, the `More?` prompt appears at the bottom of the screen.

UI Table Filtering (Using Search and Filter Commands)

3. In order to further refine your results, you can now combine the Search and Filter commands. In this example, you will search for IP addresses beginning **198.206.2**. To do this, enter */* at the Filter mode's **More?** prompt, followed by the specified text pattern:

```
/198.206.2
```

Press **<Enter>**. A screen similar to the following is displayed:

Filtering and Searching ...

```
198.206.200.0 255.255.255.0 172.16.255.254 2 1:1 DIRECT
198.206.201.0 255.255.255.0 172.16.255.254 2 1:1 DIRECT
198.206.202.0 255.255.255.0 172.16.255.254 2 1:1 DIRECT
198.206.203.0 255.255.255.0 172.16.255.254 2 1:1 DIRECT
/Networking/IP %
```

Note that the IP address, **198.206.200.0**, now appears at the top of the screen, followed by any remaining lines in the table. (In this case, the last line of the **ipr** table contains information for IP address **198.206.203.0**, as shown).

Using Wildcards with Search and Filter Commands

Wildcards allow users to substitute symbols (***** or **?**) for text patterns while using the Search and Filter commands.

Any number of wildcards can be used within a single search string. In addition, multiple character (*****) and single character (**?**) wildcards can be combined within a single search string.

Wildcard Command Options

Multiple Characters

An asterisk (*****) is used as a wildcard for multiple characters in a text pattern. For example, the Filter pattern

```
/*.img
```

will filter out all lines from the UI table except those containing any text followed by **.img**.

This wildcard can also be used *within* a specific text pattern. For example, the Filter pattern

```
/1*6
```

will filter out all lines from the UI table except those containing **1**, followed by any number of characters, then **6**. For example:

```
1:3/6
```

or

```
33:3/1 Virtual port (#66)
```

or

```
16.
```

Single Characters

A question mark (?) is used as a wildcard for a single character in a text pattern. For example, the Search pattern

f/127?.0.1

will locate the first line in a UI table containing **127.** followed by *any single character*, and then the remaining text pattern **.0.1**. For example:

127.0.0.1.

◆ Note ◆

If you use a wildcard at the Search command and the resulting page still exceeds the maximum number of table entries designated by the **more** command, you can renew the search, starting from the next line containing the text pattern. Do this by typing **n** at the **More?** prompt. Note that you can renew a search only while in Search and Search/Filter modes.

9 Installing Switch Software

User Interface software comes pre-loaded on your MPM. You do not have to reload unless you are upgrading, backing up, or reloading due to file corruption.

There are different methods for loading software into your switch. The method you use depends on your hardware configuration and the condition of the switch. These methods are:

- FTP Server - The OmniSwitch has a built-in FTP server. If you have FTP client software, you can FTP to the switch and load new software.
- FTP Client - The OmniSwitch can also be an FTP client. You can use this by connecting a terminal to the switch and using the set of FTP commands in the User Interface. You can also do this through a telnet session.
- ZMODEM - You can load software directly through the serial port with any terminal emulator that supports the ZMODEM protocol. You can do this using the file commands in the User Interface or through the boot line prompt. Note that a ZMODEM transfer of larger files can take several minutes to complete.

Do Not Mix Software Versions

When loading software, ensure that the versions of software for all the modules are from the same release. Mixing earlier versions of software with current versions can cause the switch to reset or hang.

File Transfer/Corruption Problems

If at anytime, a file transfer fails, a fragment of the file may be left on your system. This remaining file is corrupted. You should delete the file fragment and reload the file before continuing. If the MPM image file (**mpm.img**) is corrupted, you will receive a message during the boot sequence requesting you to delete the file. You should delete the file and reload it using ZMODEM through the boot line prompt. See *Using ZMODEM With the Boot Line Prompt* on page 9-5 for information on loading through the boot prompt.

Using FTP Server

The OmniSwitch is an FTP server. Using any compatible FTP client software you can load software to and from the switch. Consult the manual that came with your FTP client software package. The following are general instructions on how to FTP to the switch.

1. You will need to configure the IP address in the switch. If you have not done this, refer to the *Getting Started Guide* that came with your switch.
2. Use your FTP client software just as you would with any FTP server. When you connect to the switch you will be able to see the files contained in the flash directory. It is the only directory in the switch.
3. Note that because of the organization of files in the switch, any time a file is deleted, the flash memory is compacted. Depending on the number of files in the switch and where they are located in memory, this compaction can take anywhere from a few seconds to a couple of minutes.
4. When you transfer a file to the switch and one of the same name exists, the old file must first be deleted. You first delete the old file, then the compaction takes place, and then you can transfer the new file. When you begin your transfer, you may not see anything happening for approximately 2 minutes due the file compaction procedure. After compaction, the file will be transferred.

Using FTP Client

The User Interface contains several FTP commands. Using these commands is similar to using FTP on a UNIX system. Follow the steps below to start the FTP Client.

1. Log on to the switch and type **ftp**. For instructions on logging into the switch see the *Getting Started Guide* that came with your switch.
2. The system will prompt for a host. It saves the last host name or IP address used. If it's the one you want, press **<Enter>** or enter the new address.
3. The system will prompt for a user name. It saves the last user name. If it's the one you want, press **<Enter>** or enter the new user name.
4. The system will prompt for a password. Enter your password.
5. After logging onto the system you will receive the **ftp>** prompt. Type a question mark (?) to review the ftp commands. These commands are described in Chapter 11, "Managing Files." The following screen displays:

Supported commands:

ascii	binary	bye	cd	delete
dir	get	help	hash	ls
put	pwd	quit	remotehelp	user
lpwd				

ascii	Set transfer type to ASCII (7-bit).
binary	Set transfer type to binary (8-bit).
bye	Close gracefully.
cd	Change to a new directory on the remote machine.
delete	Delete a file on the remote machine.
dir	Obtain a long listing on the remote machine.
get	Retrieve a file from the remote machine.
hash	Print the hash symbol (#) for every block of data transferred. This command toggles hash enabling and disabling.
ls	Summary listing of the current directory on the remote host.
put	Send a file to the remote machine.
pwd	Display the current (present) working directory on the remote host.
quit	Close gracefully.
remotehelp	List the commands that the remote FTP server supports.
user	Send new user information.
lpwd	Display the current (present) working directory on the local host.
?	Summarize this list.

If you lose communications while running ftp, you may receive the following message:

Waiting for reply (Hit ^C to abort).....

6. You may press **<ctrl-c>** to abort the ftp or wait until the communication failure is resolved and the ftp transfer will continue. Note that Sun OS systems lose echo when you use the **ctrl-c** key combination.

Using ZMODEM

Normally you use FTP to transfer files to and from the switch. It is faster than using the serial port. A ZMODEM transfer can take several minutes. There are generally two situations which would require you to use the serial port to load software:

- You do not have access to an FTP client or server program. If the switch is up and running, you can use the File commands to load software.
- You have deleted the image software files in the switch. If you are in this situation, the only way to load software is using ZMODEM with the boot line prompt.

To use ZMODEM, you must have a terminal emulator that supports the ZMODEM protocol. There are many packages on the market and they operate differently; therefore instructions on how to use them are beyond the scope of this document. Consult the user manual which came with your terminal emulation software.

Before doing a serial port transfer, you should set the baud rate to the highest possible (however, it is not recommended that you run it at 38.4 Kbps). Running at 19200 is twice as fast as 9600. To set the baud rate, use the **ser** command. For more information on the **ser** command, see Chapter 10, "Configuring Management Processor Modules."

Note

If a file you are transferring already exists in the switch's flash memory, you must remove the file before transferring the new file via ZMODEM.

Using ZMODEM with the load Command

If your switch is up and running, log on to the switch. Type **ls** to list the files in flash memory. If the file you are going to transfer exists, you must delete it first with the **rm** command.

From the File menu, type **?** to list the file commands. The command you use to start the ZMODEM process is **load**. The **load** command does not support speeds greater than 19,200 bauds.

```
/File % load
```

```
The Console (DCE) port is currently running at 19200 baud  
Type 'y' to start ZMODEM download, 'q' to quit (y) : y
```

```
Upload directory: /flash  
ZMODEM ready to receive file, please start upload (or send 5 CTRL-X's to abort).
```

```
**B0100000023be50
```

Activate the ZMODEM transfer according to the instructions that came with your terminal emulation software. When the transfer is completed use **ls** again to list the file or files you have loaded.

Using ZMODEM With the Boot Line Prompt

If you encounter the situation where you have deleted some or all of the files in your switch, you may need to load files through the boot line prompt. This load procedure is done before the switch has booted. If there is no software available in the switch, then it cannot boot until you reload the software.

Using ZMODEM with the boot prompt is similar to using it with the load command. This section covers only specific step-by-step instructions to load a file using ZMODEM at the [boot]: prompt. Before doing this you may want to familiarize yourself with the boot line commands. See Appendix A, “Boot Line Prompt,” for more information.

◆ Important Note ◆

Loading software through the boot prompt should only be done when the switch is off line and not being used for normal network traffic.

Set Up the Correct Baud Rate

1. Connect a terminal to the console port. The terminal must be set to the last values set in the switch before it was powered down. For example if you were running at 19200,8,n,1, you must set your terminal to these values.

Note

If you have deleted or lost your configuration file (**mpm.cfg**), the console port values will revert back to the factory settings which are 9600,8,n,1.

If you are not sure what baud rate your switch is running, try the last known value. If your terminal displays garbage, keep changing the baud rate on your terminal emulator until you see normal ASCII characters.

2. If the switch is on, switch it off for a few seconds, then back on. You should see the boot start up on your screen. You will see the following:

```
System Boot
Press any key to stop auto-boot...
2
```

The number 2 shown above counts down to 0. To stop the boot, you must press a key before the number counts down to 0. If you miss this, simply turn the switch off for a few seconds, then back on to restart the process. Note that if there is no software in the switch it will not be able to boot and will eventually end up at the [boot] prompt anyway.

The [boot] Prompt

The [boot] prompt has its own set of commands that are built into the switch. You do not need to have files or software loaded to use this set of commands. You can perform many of the functions that the MPM software does; however, the purpose of these commands are to reload software in order to get the switch up and running.

To see a list of the boot commands, type **?** at the [boot]: prompt. The following screen displays:

```
[Boot]: ?
?          - print this list
Q          - boot (load and go)
p          - print boot params
c          - change boot params
l          - load boot file
g adrs    - go to adrs
d adrs [,n] - display memory
m adrs    - modify memory
f adrs, nbytes, value - fill memory
t adrs, adrs, nbytes - copy memory
e          - print fatal exception
n netif   - print network interface device address
L          - list ffs files
P          - Purge system: remove ALL ffs files
R file [files] - remove ffs file(s)
S          - save boot configuration
V          - display bootstrap version
$dev(0,procnum)host:/file h=# e=# b=# g=# u=usr [pwr=passwd] f=#
            tn=targetname s=script o=other

Boot flags:
0x02 - load local system symbols
0x04 - don't autoboot
0x08 - quick autoboot (no countdown)
0x20 - disable login security
0x40 - use bootp to get boot parameters
0x80 - use tftp to get boot image
0x100 - use proxy arp
0x1000 - factory reset

available boot devices: sl ffs zm
[Boot:]
```

Note that these commands are all case sensitive.

Type **L** to lists the files in flash memory. This will help you determine what files may be missing. If the file you are going to transfer exists, you must delete it first with the **R** command.

You may want to purge memory and reload all the files. To purge the flash memory, type in the **P** command.

Warning

After using the **P** command, there will be no files in flash and you will have to reload them all with ZMODEM.

Starting a ZMODEM Transfer at the [boot] Prompt

1. Type **c** to change boot parameters. You will be changing the boot device to **zm**. This will tell the system to load files from a ZMODEM connection instead of flash memory.

```
[Boot]: c
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
Boot device : zm
```

2. Type **zm** at this prompt. You will be prompted for more parameters. Just hit **<Enter>** to accept the defaults.

```
Boot file : /flash/mpm.img
Local SLIP adr :
Startup script: /flash/mpm.cmd
Console params : 9600,n8lc
Modem params : 9600,n8l
Boot flags :0xb
Other: dvip:no_name, 198.206.183.253, 255.255.255.0, 198.206.183.255;
```

```
[Boot]:
```

3. When you complete the command, the system will return to the **[Boot]:** prompt. Type in the “at” command (**@**) to load the boot parameters.

```
[Boot]: @
```

```
Boot device : zm
Boot file : /flash/mpm.img
Startup script: /flash/mpm.cmd
Console params : 9600,n8lc
Modem params : 9600,n8l
Boot flags :0xb
Other: dvip:no_name, 198.206.183.253, 255.255.255.0, 198.206.183.255;
```

```
Attaching network interface lo0... done.
Disk load or Boot load (D/B/Q)? -> d
```

4. At the **Disk load or Boot load {D/B/Q}? ->** prompt, type in **d** to tell the system to load from a disk. The system is prepared to accept a ZMODEM transfer, and displays the following:

```
Upload directory: /flash
ZMODEM ready to receive file, please start upload (or send 5 CTRL-X's to abort).
```

```
**B0100000023be50
```

5. Activate the ZMODEM transfer according to the instructions that came with your terminal emulation software.
6. When the transfer is completed use **L** (case sensitive) to list the files you have loaded.
7. Repeat this procedure for every file that you want to load.

10 Configuring Management Processor Modules

The management processor module (MPM on the OmniSwitch and MPX on the Omni Switch/Router) coordinates control of the OmniSwitch by providing access to the User Interface (UI) software, maintaining user configuration information, downloading switching module software, managing basic bridge functions, maintaining basic routing functions, and managing the SNMP management agent. Switching modules are dependent on the MPM/MPX for downloading software and for receiving initialization and configuration information. In addition, the Network Management System (NMS) depends on the MPM/MPX to send and receive SNMP messages for managing the switch.

◆ Important Note ◆

All of the UI commands described in this chapter also work with the Omni Switch/Router MPX.

The OmniSwitch and Omni Switch/Router also support two MPMs/MPXs with one acting as the primary and with one acting as the secondary. If the primary MPM/MPX fails, the secondary MPM/MPX can take over automatically. Operating with redundant MPMs/MPXs can also help avoid network downtime.

◆ Note ◆

When you have two MPMs in one chassis, they must be installed in slots 1 and 2, and only one will be active.

The primary MPM/MPX executes all the commands and, when needed, sends requests to the secondary MPM/MPX. The secondary MPM/MPX continuously monitors the primary MPM. For more information on MPMs, see Chapter 6, “The Management Processor Module (MPM).” For more information on MPXs, see Chapter 2, “The Omni Switch/Router MPX.”

The UI provides commands to configure the serial port, to configure the Ethernet management port (on the MPX and MPM-C only), and a set of commands to monitor and configure primary and secondary MPMs/MPXs. These commands are described in the pages that follow.

Changing Serial Port Communication Parameters

The serial communications parameters for the two MPM ports are set by default to the following:

- 9600 bits per second (bps)
- 8 data bits
- 1 stop bit
- no parity

To change the serial port configuration parameters, follow the steps below:

1. Log into the switch. For instructions on logging in, see your *Getting Started Guide*.
2. At the system prompt, type **ser**.
3. You will see the following message:

Port to configure? {(C)onsole,(M)odem} (Console) :

Press **C** if you want to configure the console port (female, DCE) parameters, or type **M** to configure the modem port (male, DTE) parameters. The default is the Console Port (**C**).

4. The current port values are shown, followed by a prompt to change the speed value.

Current Console (DCE) configuration:

**9600 bps, 8 data bits, None parity, 1 stop bit, running Console (shell)
Speed (9600):**

Enter the speed (in bits per second) at which you want the port to operate, or simply press **<Enter>** to accept the default in parentheses. Valid values are 1200, 9600, 19200, and 38400 bps.

5. The following prompt displays:

Data size {7/8} bits (8) :

Enter the data size in bits (7 or 8). The default is 8. Press **<Enter>** to accept the default in parentheses.

6. The following prompt displays:

Parity { (N)one/(E)ven/(O)dd } (None) :

Enter the parity (none, even, odd) and press **<Enter>**. The default is None.

7. The following prompt displays:

Stop bits {0/1/2} (1):

Enter the number of stop bits (0, 1, or 2) and press **<Enter>**. The default is 1.

8. The following prompt displays:

Mode {(D)own,(C)onsole,(A)uxConsole,(S)LIP} (C) :

Enter the port mode and press **<Enter>**. This option defaults to console for a console connection and down for a modem connection. You can also configure the port for SLIP. If you are configuring the modem port, you should plan the mode configuration carefully. See *Configuring the Modem Port* on page 10-3 for further information.

◆ Important Note ◆

You cannot configure the console port as an auxiliary port (**AuxConsole**).

9. The following prompt displays:

Set (and save) these settings {(S)ave/(Q)uit} (Save) :

Enter **save** to accept the parameters you entered and exit, or enter **quit** to exit this command without saving your changes.

Changing Port Speed When Communication With The Switch Lost

When you cannot communicate with the switch, there is an alternative method you can use to toggle through the various serial port speed options. The port defaults to 9600 bps. But if you send a Break signal (by pressing the **BREAK** key), the port speed will change to the next higher speed. When it reaches the highest speed (38400 bps), it toggles back to the lowest speed (1200 bps). You cycle through the port speeds in the following order: 9600–19200—38400–1200.

◆ Note ◆

On the MPX, MPM-C, and MPM-III, you must remove the default baud rate shunt (E1), which fixes the baud rate at 9600 bps, before you can change the baud rate. This shunt is located near the front end of the circuit board, just to the right of the Ethernet management port.

Configuring the Modem Port

If you plan to use the modem port as your main connection to User Interface software, then you need to make sure its mode and jumper settings are configured correctly.

Modem Port Mode

The **ser** command allows you to configure an active modem port to SLIP, console, or auxiliary console mode. When using a modem, it is recommended that you configure the two ports as follows:

```
modem port mode=SLIP
console port mode=console
```

This configuration allows you to use the modem port to access User Interface software through a SLIP connection. The console port is used as an optional way to access software.

◆ Please Note ◆

You need Release 3.2 or above to use the modem and console ports simultaneously.

Another valid configuration is as follows:

```
modem port mode=console
console port mode=down
```

This configuration does not allow you to use the console port as an optional access method since it is configured down. Using a cross-over cable, you could access the modem port through an attached PC. If you could not use the modem port for some reason, you would have to reboot the switch to get back, or—if the cable connection were the problem—use a cross-over cable to connect through a PC.

A third valid configuration that keeps both ports active is:

```
modem port mode=console
console port mode=SLIP
```

This configuration allow you to use the modem port regularly and use a SLIP connection to access switch software through the console port.

A fourth valid configuration that keeps both ports active is:

```
modem port mode=auxiliary
console port mode=console
```

This configuration allow you to use the console and modem ports simultaneously to access switch software.

Configuring SLIP

Before configuring SLIP on an MPM (but not an MPX or MPM-C) you should check to see that the jumper settings are correct for the modem port (refer to Chapter 6, “The Management Processor Module (MPM)”). To configure SLIP, enter the **slipc** command. If you enter the command and SLIP is not running on any ports, the system displays the following message:

Current SLIP configuration

SLIP not running on any ports, do you want to configure it?
Yes, No {Y/N} (Y) :

Enter **y** to display current information. Enter **n** to skip the display. To configure the required SLIP parameters, complete the following steps:

1. Type **slipc** at the prompt and press **<Return>**.
2. Enter a valid IP address.
3. Enter a valid remote IP address.

You can use the **ping** command to validate the connection's integrity.

Configuring the Ethernet Management Port

To configure the Ethernet management port on an Omni Switch/Router MPX, OmniSwitch MPM-C, or OmniSwitch MPM-III, you use the **ethernetc** command. To use this command, enter

ethernetc

at the system prompt. A screen similar to the following will be displayed.

Ethernet Port Configuration

```

1) Port Admin status UP : Yes
2) IP Address           : 198.206.184.175
3) Subnet Mask         : 255.255.255.0
4) Bcast Address      : 198.206.184.255
5) Gateway Address    : 198.206.184.254
6) Remote Host Address : UNSET
7) RIP Mode           : Inactive

```

Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw) :

The question mark option (?) and the **Help** option provide reference and instructional information on using this command. The **Redraw** option refreshes the screen.

You make changes by entering the line number for the option you want to change, an equal sign (=), and then the value for the new parameter. When you are done entering all new values, type **save** at the colon prompt (:) and all new parameters will be saved. If you do not want to save the changes enter **quit** or **Ctrl-D**.

◆ Important Note ◆

On some revisions of the MPX, you *must* configure the Ethernet management port with the boot prompt before you can use the **ethernetc** command. See Appendix A, “The Boot Prompt,” for more information on configuring the Ethernet management port with the boot prompt.

The configurable options displayed by the **ethernetc** command are described below.

1) Port Admin status UP

Enter **1=Yes** (the default) to enable the Ethernet management port or **1=No** to disable it.

2) IP Address

Enter an IP address for the Ethernet management port in dotted decimal or hexadecimal notation (the default is **192.168.11.1**). For example, to change the Ethernet management port's IP address to **198.206.184.170**, enter

2=198.206.184.170

at the prompt.

◆ Note ◆

This IP address *must* not be on the same subnet as any other IP router on the switch.

3) Subnet Mask

Enter an IP subnet mask in dotted decimal or hexadecimal notation (the default is **255.255.255.0**). If no mask is provided, the switch will try to determine the mask using Internet Control Message Protocol (ICMP) requests. For example, to change the subnet mask to **255.255.255.254**, enter

3=255.255.255.254

at the prompt.

4) Bcast Address

The default broadcast address is automatically derived from the default VLAN IP address class (the default is 192.255.255.255). You can enter a new address in dotted decimal or hexadecimal notation. For example, to change the broadcast address to **198.206.184.255**, enter

4=198.206.184.255

at the prompt.

5) Gateway Address

You can enter an IP address for the first hop router to a remote host (if the host is on a different IP net) in dotted decimal or hexadecimal notation. The default is 192.168.1.1. For example, to change this address to **198.206.184.170**, enter

5=198.206.184.170

at the prompt.

6) Remote Host Address

You can enter an IP address for a a remote host (if the host is on a different IP net) in dotted decimal or hexadecimal notation. The default is 192.168.1.1. For example, to change this address to **198.206.184.170**, enter

5=198.206.184.170

at the prompt.

7) RIP Mode

This parameter is an informational field, which shows that the RIP mode is inactive. You *cannot* modify this parameter.

Ethernet Management Ports and Redundant Management Processor Modules

If redundant MPXs /MPM-Cs/MPM-IIIs both have Ethernet management ports (EMPs), both EMPs in the switch will have the same IP address if automatic file synchronization is enabled. If both EMPs are plugged into the same subnet, the UI will show that there are duplicate IP addresses on the network.

To get around this duplicate IP address problem, you must disable automatic file synchronization and then you must configure different IP addresses for the two EMPs. To do this, perform the following steps:

1. On the primary management module, enter

syncctl

at the system prompt. (See *Setting Automatic Config Synchronization* on page 10-15 for more information on the **syncctl** command.)

2. If automatic file synchronization is already disabled, simply press **<Enter>**. If it is enabled, enter **disable** at the prompt.

3. Enter

ethernetc

at the prompt. (See *Configuring the Ethernet Management Port* on page 10-5 for more information on the **ethernetc** command.)

4. Enter **2=** followed by the IP address for the EMP on the primary management module.

5. Enter

save

at the prompt to save the IP address.

6. Enter

renounce

at the prompt to make the primary management module the secondary module and the secondary module primary.

7. Log into the now primary management module.

8. On the now primary management module, enter

syncctl

at the system prompt.

9. If automatic file synchronization is already disabled, simply press **<Enter>**. If it is enabled, enter **disable** at the prompt.

10. Enter

ethernetc

at the prompt.

11. Enter **2=** followed by the IP address for the EMP on the management module.

12. Enter

save

at the prompt to save the IP address.

13. Enter

renounce

at the prompt to make the management module that was originally the primary one primary again.

The MPM Command/Menu

The **mpm** command has two functions: displaying the MPM redundancy configuration and entering the **mpm** menu. Displaying the MPM redundancy is described below and the **mpm** menu is described in *MPM Menu Commands* on page 10-9.

Displaying MPM Redundancy

You can display the number of MPMs, their location in the switch, and the MPM redundancy configuration of the switch by entering

mpm

at the system prompt. The following is a typical example of the message that displays when you enter **mpm** for a switch without a redundant MPM.

Currently this slot 1 holds the Primary MPM; there is no secondary MPM.

The following is a typical example of the message that displays when you enter **mpm** for a switch with redundant MPMs on the primary MPM.

Currently this slot 1 holds the Primary MPM and slot 2 holds the secondary.

The following is a typical example of the message that displays when you enter **mpm** for a switch with redundant MPMs on the secondary MPM.

Currently slot 1 holds the Primary MPM; this slot 2, holds the secondary MPM.

MPM Menu Commands

The **mpm** command also takes you to the **mpm** menu which contains the commands needed to configure single and redundant MPMs. With a serial or modem connection, you can communicate with either the primary or secondary MPM by connecting to the respective RS232 connectors. With a telnet connection, however, you can only communicate with the primary MPM.

Type a **?** to list the **mpm** commands. One set of commands will be displayed if you are connected to the primary MPM and another command will be displayed if you are connected to the secondary MPM. If you are connected to the primary MPM, you will see the following.

<u>Command</u>	<u>Redundancy Menu</u>
sls	List the contents of the Secondary /flash and /simm directories
mpmstore	Store file to Secondary /flash or /simm directory
mpmreplace	Replace file on Secondary /flash or /simm directory
mpmload	Load file from Secondary MPM
mpmrm	Remove file from Secondary MPM
renounce	Give up control to Secondary
nisuf	Set load suffix for NI image files
syncctl	Enable/Disable synchronization of configuration data
configsync	Synchronize configuration data
imgsync	Synchronize Image (Executable) files
secreset	Reset Secondary MPM
swap	Change swap status of chassis

All of the **mpm** menu commands, except for the **nisuf** and **swap** commands, function only if you have redundant MPMs. If you are connected to the secondary MPM, type a **?** to list the **mpm** commands shown below.

<u>Command</u>	<u>Redundancy Menu</u>
mpmget	Get file from Primary MPM
takeover	Become Primary

All of the **mpm** commands are described in the sections that follow.

Using MPM Commands with Software Release 3.2 and Later

In Release 3.2 and later, the commands in the **mpm** menu support the use of more than one flash directory. If you install a 32 or 56 Mb SIMM memory module in an MPM, for example, you will have **/flash** and **/simm** flash memory directories. Since more than one flash directory can exist, you *must* indicate which flash directory you want to use when you access a secondary MPM from a primary MPM and when you access a primary MPM from a secondary MPM. All of these commands begin with the prefix **mpm** and are listed below.

mpmstore
mpmreplace
mpmload
mpmrm
mpmget

To indicate which flash directory you want to use, enter a slash (*/*), the name of the directory, and another slash (*/*) before the file name in all commands that begin with the prefix **mpm**. For example, to transfer the **asm.img** file from the **/simm** directory on the secondary MPM to the primary MPM when you have logged into the secondary MPM, enter

```
mpmget /simm/asm.img
```

at the system prompt.

◆ Important Note ◆

In the current release, you *must* indicate the name of the flash directory in commands that begin with the prefix **mpm** even if you have just one flash directory on both MPMs.

Listing the Secondary MPM Files

The **sls** command lists the files in the secondary MPM module. This is similar to the **ls** command; however, it lists files in the secondary MPM. To list files in the secondary MPM, enter

```
sls
```

at the system prompt. The following is a typical example.

```

/flash/esm.img          27204      7/14/99   11:39
/flash/mesm.img        27561      7/14/99   11:39
/flash/mpm.img         1790889    7/14/99   11:39
/flash/rav.img         83588      7/14/9    11:39
/flash/mpm.cnf         32768      1/ 1/70   00:00
/flash/mpm.log         18072      7/30/99   13:51
/flash/mpm.cfg         32768      7/30/99   14:40
/flash/mpm.cmd          32         1/ 1/70   00:00
/flash/gated.img       547041     8/27/9    16:01

/flash has          1071449 bytes free.
/simm Not present.
```

The **sls** command lists every file in the secondary MPM's flash memory followed by its size (in bytes), creation date, and creation time. The three-letter file name suffix indicates the type of file which includes configuration (**cnf** and **cfg**), command (**cmd**), and image (**img**). The image file suffix can be changed for both the primary and secondary MPMs with the **nisuf** command, which is described in *Setting the Load Suffix* on page 10-14.

Transferring a File to the Secondary MPM

The **mpmstore** command transfers a file in the flash memory of the primary MPM to the flash memory of the secondary MPM. To use this command, enter **mpmstore**, followed by a space, a slash (*/*), the name of the flash directory, another slash (*/*), and the name of the file you want to transfer.

For example, to transfer the file **mpm.log** from the **/flash** directory on the primary MPM to the secondary MPM, for example, you would enter

```
mpmstore /flash/mpm.log
```

at the system prompt. The following will be displayed.

```
Transferring...
```

If the file already exists on the target MPM, something similar to the following message will be displayed.

```
File mpm.log exists on slot 2
```

Use the **mpmreplace** command, which is described in *Replacing a File on the Secondary MPM* on page 10-12, to replace a file that already exists.

Replacing a File on the Secondary MPM

The **mpmreplace** command replaces a file on the secondary MPM. It works like a combination of **mpmrm**, which is described in *Removing a File from the Secondary MPM* on page 10-13, and **mpmstore**, which is described in *Transferring a File to the Secondary MPM* on page 10-11. To use this command, enter **mpmreplace**, followed by a space, a slash (/), the name of the flash directory, another slash (/), and the name of the file you want to replace.

For example, to replace the file **mpm.log** on the secondary MPM with the file **mpm.log** from the **/flash** directory on the primary MPM, for example, you would enter

```
mpmreplace /flash/mpm.log
```

at the system prompt. The following will be displayed.

```
Deleting.  
Transferring
```

If the file already exists on the target MPM and it is identical to the one you are transferring, something similar to the following message.

```
File mpm.log is identical on Primary and Secondary 2
```

If the files are identical, the **mpmreplace** command will terminate and the file will not be replaced.

Loading a File from the Secondary MPM

The **mpmload** command loads a file from the flash memory of the secondary MPM into the flash memory of the primary MPM. To use this command, enter **mpmload**, followed by a space, a slash (/), the name of the flash directory, another slash (/), and the name of the file you want to load.

For example, to load the file **mpm.log** from the **/flash** directory on the secondary MPM into the primary MPM, for example, you would enter

```
mpmload /flash/mpm.log
```

at the system prompt.

Removing a File from the Secondary MPM

The **mpmrm** command removes (deletes) a file from the flash memory of the secondary MPM. To use this command, enter **mpmrm**, followed by a space, a slash (/), the name of the flash directory, another slash (/), and the name of the file you want to remove.

◆ Note ◆

You can only remove a single file with the **mpmrm** command. You *cannot* use wildcards to remove multiple files.

For example, to remove the file **mpm.log** from the **/flash** directory on the secondary MPM in slot 2, for example, you would enter

```
mpmrm /flash/mpm.log
```

at the system prompt. Something similar to the following will be displayed.

```
Checking for /flash/mpm.log on slot 2
```

After a brief moment, the file will be deleted from the secondary MPM and something similar to the following will be displayed.

```
Deleting /flash/mpm.log on slot 2 . Done.
```

◆ Warning ◆

You *cannot* recover a file once it has been deleted with the **mpmrm** command.

Giving Up Control to the Secondary MPM

The **renounce** command tells the primary MPM to give up control and become the secondary MPM. It does this by issuing a request to the secondary MPM to take control. You *must* be logged into the primary MPM to use this command. If you are logged into the secondary MPM, use the **takeover** command, which is described in *Gaining Control from the Primary MPM* on page 10-18.

◆ Warning ◆

The **renounce** command should only be used during network down times since it could cause network interruptions.

To transfer control from primary MPM to the secondary MPM, enter

```
renounce
```

at the system prompt. The following prompt will display.

```
Confirm? (n):
```

Press **y** to transfer control to the secondary MPM or press **n** to cancel the command (the default is **n**). If you enter **y**, the switch will reset after displaying the following message.

```
System going down immediately...
```

The switch will reboot and the original secondary MPM will be the primary once the switch comes back up.

Setting the Load Suffix

The **nisuf** command sets the load suffix for the switch's executable image files. (The factory default suffix is **img**.)

◆ Warning ◆

The **nisuf** command should only be used when it is necessary to have two versions of the software on the switch at the same time and the user is directly connected to the console for reboot.

You can change it by typing the **nisuf** command followed by the new suffix. For example, to change the load suffix from **img** to **bin**, enter

```
nisuf bin
```

at the system prompt. The following message will then be displayed.

```
Changing load suffix from img to bin
```

You should create or load new image files with the new suffix as soon as possible because the switch will not recognize the files with the old suffix as image files. See Chapter 9, "Installing Switch Software," and Chapter 11, "Managing Files," for information on loading and creating files.

Setting Automatic Config Synchronization

The **syncctl** command sets the automatic configuration synchronization to Enabled or Disabled. If it is Enabled, then the MPM primary/secondary pair will continue to maintain synchronization automatically. This means that when the configuration file (**mpm.cfg**) is updated in the primary MPM, it will automatically be updated in the secondary MPM, keeping the two MPMs in sync.

Enabling Automatic Config Synchronization

To enable synchronization between the primary and secondary MPMs, enter

```
syncctl
```

at the system prompt. The following prompt will then be displayed if synchronization is not enabled.

Desired state (enable):

Press **<Enter>** to enable synchronization or enter **disable** to cancel. If you enabled synchronization, the following will be displayed.

Configuration synchronization is now Enabled

Note that automatic configuration synchronization is disabled unless all image (**img**) and Programmable Gate Array (PGA) files in the switch are synchronized first. See *Synchronizing Image Files* on page 10-16 for information on the **imgsync** command, which synchronizes image and PGA files.

The interval between updates is 5 minutes. The primary MPM will copy any changes to the secondary MPM after 5 minutes have elapsed since the last update.

Disabling Automatic Config Synchronization

To disable synchronization between the primary and secondary MPMs, enter

```
syncctl
```

at the system prompt. The following prompt will then be displayed if synchronization is enabled.

Desired state (disable):

Press **<Enter>** to disable synchronization or enter **enable** to cancel. If you disabled synchronization, the following will be displayed.

Configuration synchronization is now Disabled

If automatic config synchronization is Disabled, the configuration file in the secondary MPM will be unaffected if you change the configuration file in the primary MPM.

Synchronizing Configuration Data

The **configsync** command copies the configuration files (**mpm.cnf** and **mpm.cfg**) in the primary MPM to the secondary MPM. You can run this command whether or not automatic config synchronization is on. For example, to copy the configuration file from the primary MPM to the secondary MPM, you would enter

```
configsync
```

at the system prompt. Something similar to the following will be displayed.

```
Syncing Config file  
Config files are currently synchronized.
```

See *Setting Automatic Config Synchronization* on page 10-15 for information on setting automatic config synchronization.

Synchronizing Image Files

The **imgsync** command copies all of the image (executable) files in the primary MPM to the secondary MPM. When used in conjunction with the **configsync** command, it ensures that the two MPMs are running exactly the same versions of software and are in sync (i.e., have the same configuration). To synchronize all the image files, enter

```
imgsync
```

at the system prompt. When you run **imgsync** you will be asked if you want to synchronize the **cmd** file and/or PGA files if they are found to be different.

◆ **Note** ◆

If any PGA file is being used by a Token Ring module and you choose to sync the cmd file, then the PGA file that is in use will be synced even if you do not choose to synchronize PGA files.

Something similar to the following prompt will be displayed.

```
Sync cmd file (y) :
```

Press **y** to sync the **cmd** file or press **n** to skip this file (the default is **y**). If you have any PGA files, you will be asked if you want to sync those files. In addition, if the secondary MPM has any additional image, then the following prompt will be displayed.

```
Remove Additional images from Secondary (n) :
```

Press **y** to remove any extra image on the secondary MPM or press **n** to keep these files (the default is **n**). After you answer all the prompts, something similar to the following will be displayed.

```
8 files to be synchronized  
1 file to be synchronized  
Syncing  
Deleting /flash/mpm.cmd.....  
Replacing /flash/mpm.cmd.....
```

Loading a File From the Primary MPM

The **mpmget** command loads a file from the primary MPM and copies it into the secondary MPM. This command is only available and can only be run from a secondary MPM. To use this command, enter **mpmget**, followed by a space, a slash (*/*), the name of the flash directory, another slash (*/*), and the name of the file you want to transfer.

For example, to load the file **mpm.log** from the **/flash** directory on the primary MPM to the secondary MPM you would enter

```
mpmget /flash/mpm.log
```

at the system prompt. After a brief moment, the file will be transferred into the secondary MPM. The following would then be displayed.

```
Transferring .. Complete
```

Gaining Control from the Primary MPM

The **takeover** command tells the secondary MPM to take control and become the primary MPM. It does this by issuing a request to the primary MPM to relinquish control. You *must* be logged into the secondary MPM to use this command. If you are logged into the primary MPM, use the **renounce** command, which is described in *Giving Up Control to the Secondary MPM* on page 10-14.

◆ Warning ◆

The **takeover** command should only be used during network down times since it could cause network interruptions.

To transfer control from primary MPM to the secondary MPM, enter

takeover

at the system prompt. The following prompt will display.

Confirm? (n):

Press **y** to transfer control to the secondary MPM or press **n** to cancel the command (the default is **n**). If you enter **y**, the switch will reset after displaying the messages similar to the following.

System going down immediately...

**Please standby, chassis configuration changing (Hit ^C to abort).....Taking over
as Primary**

... Alcatel SNMP Agent Operational.

The switch will reboot and the original secondary MPM will be the primary once the switch comes back up.

Resetting a Secondary MPM

The **secreset** command initiates a soft reset on the secondary MPM. Conceptually, resetting a secondary MPM with this command is similar to switching off power to the module; the MPM will be in the same state after a reset as it is after a power on.

To reset a secondary MPM, enter

```
secreset
```

at the system prompt. Messages similar to the following will display:

```
Module 1 changed while Swap OFF
```

```
Syncing configuration data with secondary 1 .. complete
```

◆ **Note** ◆

To reset a switching module, use the **reset** command, which is described in Chapter 58, “Running Hardware Diagnostics.”

Displaying and Setting the Swap State

The **swap** command displays or alters the swap state of the chassis. The swap state must be on in order to hot swap modules. If not, the system may halt or restart. While the swap state is on, performance may decrease. Therefore, the swap state should only be turned on when you want to hot swap modules. See Chapter 7, “OmniSwitch Switching Modules,” for instructions on hot swapping a switching module.

Displaying the Swap State

To display the current swap state of the chassis, enter

```
swap
```

at the system prompt. If the swap mode is **OFF** (the default for the switch), something similar to the following will be displayed.

```
Swap is OFF, timeout is 5 minutes
usage swap { ON [ minutes ] | OFF [ minutes ] }
```

If the swap mode is **ON**, something similar to the following will be displayed.

```
Swap is ON, expires in 4 minutes
usage swap { ON [ minutes ] | OFF [ minutes ] }
```

The swap mode *must* be enabled (**ON**) to hot swap a switching module. If not, the system may halt or restart. See the subsection below for instructions on enabling the swap mode.

Enabling the Swap Mode

To turn the swap mode **ON**, enter

```
swap on
```

at the system prompt. (The default for swap mode is 5 minutes). Something similar to the following will be displayed.

```
Swap is ON for 5 minutes
```

When you turn the swap state on, you set a timer which determines how long the system will remain in swap state. After the timer expires, the system will automatically turn off the swap state.

If you want to vary the amount of time that the swap mode is enabled, enter **swap on** followed by the number of minutes you want the swap mode enabled. You can set the swap state from 1 to 227,055 minutes. To set the swap mode on for 10 minutes, for example, enter

```
swap on 10
```

at the system prompt. The following will then be displayed.

```
Swap is ON for 10 minutes
Save minutes value {Y/N}? (N) :
```

Press **y** and then press **<Enter>** to save the new value. If you don't want save, just press **<Enter>** and the default value will not change. You can also turn off the swap immediately as shown in *Disabling the Swap Mode* on page 10-21.

Disabling the Swap Mode

Normally, the swap mode will timeout and no user intervention is required. However, you can manually turn the swap mode off. This function is particularly useful since the performance of the switch can be adversely affected if the swap mode is enabled. To turn the swap mode off immediately, enter

swap off

at the system prompt. The swap mode will be disabled and something similar to the following will be displayed.

Swap is OFF, timeout is 5 minutes

11 Managing Files

Depending on the model type and configuration, an Alcatel switch has anywhere from 2 to 32 MB of usable flash memory. This memory is used to store files, including executable files (used to operate switching modules), configuration files, and switch usage log files. Through the User Interface (UI), you can load, copy, and delete any of these files types. In addition, the UI has commands for displaying, creating, and editing ASCII (text-based) files.

All commands described in this chapter will work with files located in the **/flash** and **/simm** directories on either the primary or secondary MPM. However, these commands work only with the files that reside on the MPM to which you are connected. See Chapter 10, “Configuring Management Processor Modules,” for more information on commands for working with redundant MPMs.

UI commands for file maintenance are grouped into two menus: the File menu and System menu. File menu commands are listed below. For a list of System menu commands, see *System Menu* on page 11-13.

File Menu

The File menu contains commands for loading, listing, copying, and deleting individual switch files. To access the File menu, enter

file

at the UI prompt.

If verbose mode is enabled, the following list of commands will be displayed automatically.

If verbose mode is disabled, press the question mark (?) to display the following list of commands. (For information on enabling verbose mode, refer to the **uic** command description in Chapter 8, “The User Interface.”)

Command	File Menu
load	Download system software using the serial interface
ftp	Download from an FTP server
pwd	Display the current working directory
ls	List the contents of the current working directory (default working directory is /flash)
rm	Remove a file
cp	Copy a file
view	View an ASCII file
edit	Edit buffer locally
imgcl	Remove all image files

Main Interface	File Security	Summary System	VLAN Services	Networking Help
-----------------------	----------------------	-----------------------	----------------------	------------------------

All commands in the File menu, except for the **load** and **ftp** commands, are described in the following sections. For instructions on using the **ftp** and **load** commands, refer to Chapter 9, “Installing Switch Software.”

◆ Note ◆

If you want to use the **rm**, **cp**, **imgcl**, and the **edit** sub-menu commands, you must be logged in as **admin** or **diag**. See Chapter 8, “The User Interface,” for more information on login accounts.

Displaying the Current Directory

To display the switch's current directory, enter

```
pwd
```

at the system prompt. If you have not installed a SIMM module into your MPM, the working directory will be the **/flash** memory system and the corresponding directory information will be displayed:

```
/flash
```

If you have installed a SIMM module, you will also have a file system called **/simm**. However, your working directory will still be the **/flash** file system unless you execute the **cd** command (explained in the section below, *Changing Directories*).

Command and Image File Placement

If there is a SIMM module installed, be sure that the following files are loaded in the **/flash** file system: **mpm.cmd**, **mpm.img**, and **dni.img** (if applicable). *Do not* place these files in the **/simm** flash file system.

All other files can go in either the **/flash** or **/simm** flash file system.

Configuration and Log File Generation

The **mpm.cnf**, **mpm.cfg**, and **mpm.log** files are generated automatically by the switch and placed in flash memory during the boot process; you do not have to load them.

◆ Important ◆

If you remove the configuration files (**mpm.cnf** and **mpm.cfg**) from your switch, all of your switch's non-default configuration settings will be deleted at the next boot sequence. Use caution when removing configuration files and be sure to create backup copies if you want to safeguard your current configuration.

Changing Directories

You can change the working directory with the **cd** command. If you have installed a SIMM memory module into your MPM, you can switch from the **/flash** to the **/simm** memory by entering

```
cd simm
```

at the system prompt. To change the working directory back to **/flash** file system, enter

```
cd flash
```

at the system prompt.

◆ Conserving Flash File System Memory ◆

You can put many switch files on the **/simm** flash system. This will leave the **/flash** file system with additional free space for the configuration files (**mpm.cnf** and **mpm.cfg**) to grow. Refer to *Command and Image File Placement* above for more information.

Listing Switch Files

You can use the **ls** command to list the files in the primary MPM's flash memory. To use this command, enter

```
ls
```

at the system prompt. A screen similar to the following will be displayed.

```

mpm.cmd           18      05/30/98  13:04
mpm.log           18072   06/15/98  17:57
mpm.img          1573617 06/18/98  12:16
mesm.img          24289   06/18/98  12:18
tsm.img           125154  06/18/98  12:18
esm.img           26421   06/18/98  12:18
mpm.cfg           1024    01/01/70  00:00
mpm.cnf           32768   06/18/98  12:27

```

1858057 bytes free.

The **ls** command lists all the files in the current working directory of the primary MPM's flash memory, followed by its size (in bytes), creation date, and creation time. The three-letter file extension indicates the type of file. Examples include configuration (**cnf** and **cfg**), command (**cmd**), image (**img**), Programmable Gate Array (**.pga**), etc. The **ls** command also lists the total number of bytes of free memory in flash memory.

◆ Note ◆

If you are connected to the primary MPM and you want to display the files in a secondary MPM, use the **sls** command, which is further detailed in Chapter 10, "Configuring Management Processor Modules."

If you have installed a SIMM memory module, you can list the files in the **/simm** file system by entering

```
ls /simm
```

at the system prompt.

Deleting Switch Files

You can use the **rm** command to delete files in the primary MPM's flash memory. To use this command, enter **rm**, followed by the name of the file you want to delete. For example, to delete the file **mpm.log**, you would enter

```
rm mpm.log
```

at the UI prompt. The following screen will be displayed:

```
File system compaction in progress...
```

The switch will take a few seconds to delete the file and compact the flash memory.

◆ Note ◆

If you are connected to the primary MPM and you want to remove files from a secondary MPM, use the **mpmrm** command, which is described in Chapter 10, "Configuring Management Processor Modules."

Deleting Multiple Files

You can remove multiple files either by entering multiple file names in the command line or by using wildcards.

When entering multiple file names, be sure to include a space between each file name you want to delete. For example, to remove both the **mpm.cfg** and **mpm.cnf** files, you would enter the following:

```
rm mpm.cfg mpm.cnf
```

Wildcards let you substitute an asterisk (*) for file name text. You can remove all files with the same extension by entering **rm**, followed by an asterisk (*), a period (.), and the file extension. For example, if you want to delete all the files with the **log** extension, enter

```
*.old
```

at the UI prompt. The following message will be displayed:

```
Remove the following?  
  /flash/mpm.log.old  
  /flash/mpm.old  
Are you sure you want to remove this? (n)
```

Press the **y** key to delete the selected files or press **<Enter>** to cancel. If you press the **y** key, the following will be displayed:

```
...2 files removed
```

The switch will take a few seconds to delete the file and compact the flash memory.

◆ Note ◆

If you want to delete all the image files (i.e., files with the **img** extension), you can use the **imgcl** command, which is described in *Deleting All Image Files* on page 11-5.

Deleting All Image Files

You can use the **imgcl** command to delete all executable (image) files. The files deleted by the **imgcl** command include the MPM boot file (**mpm.img** on an MPM-1G, **mpx.img** on an MPX, **mpm3.img** on an MPM-III, and **mpmc.img** on an MPM-C), all executable switching module files (the factory default is all files ending with the **.img** extension), and all PGA files.

◆ Important ◆

You should only use the **imgcl** command during network down times and when you are connected to the switch through the serial port.

To use this command, enter

```
imgcl
```

at the system prompt. A screen similar to the one shown below will be displayed.

```
Remove the following?  
/flash/asm.img  
/flash/esm.img  
/flash/fsm.img  
/flash/mesm.img  
/flash/mpm.img  
/flash/tsm.img  
Are you sure you want to remove them? (n)
```

Press the **y** key to delete all the image files or press **<Enter>** to cancel. If you press the **y** key, the switch will spend several minutes deleting the image files.

◆ Note ◆

If you want to delete *all* files in flash memory, you can use the **newfs** command, which is described in *Creating a New File System* on page 11-15.

After you have deleted all the old image files, you must load new image files using FTP or ZMODEM so the switch can function. See Chapter 9, "Installing Switch Software," for instructions on using the **ftp** and **load** commands.

Copying System Files

You can use the **cp** command to copy files. This is particularly useful if you want to make backups of important files. To use this command, enter **cp**, followed by the name of the original file you want to copy, and then by the name that you wish to give the duplicate file. For example, to make a duplicate of the file **mpm.cmd** that is to be called **mpm.bak**, enter

```
cp mpm.cmd mpm.bak
```

at the system prompt. The following information will be displayed:

```
/flash/mpm.cmd -> /flash/mpm.bak : 100%
```

Displaying Text Files

You can use the **view** command to display the contents of ASCII (text-based) files. To use this command, enter **view**, followed by the name of the file you want to display. To display the **mpm.cmd** file, for example, enter

```
view mpm.cmd
```

at the system prompt. A screen similar to the one shown below will be displayed.

```
cmDoDump=1  
cmInit
```

Note that if you try to view a file with non-ASCII characters, an error message will be displayed. For example, if you use the **view** command on the file **mpm.cfg**, the following error message will appear:

```
The file mpm.cfg has non-printable characters, can't view
```

◆ Note ◆

You can edit text files with the **edit** sub-menu commands, which are described in *Editing Text Files* on page 11-7.

Editing Text Files

The commands in the Edit sub-menu (also called the Text Buffer or Edit Buffer) are used to create new text files and to modify existing text files. To enter the edit sub-menu, enter

edit

at the system prompt.

If verbose mode is enabled, the following list of commands will be displayed automatically.

If verbose mode is disabled, press the question mark (?) to display the following list of commands. (For information on enabling verbose mode, refer to the **uic** command description in Chapter 8, “The User Interface.”)

Command	Edit Menu
ab	Append line(s) to the buffer
cb	Clear the buffer
db	Delete line from the buffer
eb	Edit a buffer line
ib	Insert buffer line
lb	List contents of the buffer
nb	Name file for buffer
rb	Read file into buffer
wb	Write buffer to file

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

The Edit sub-menu commands are outlined in the following sections. You can edit up to 100 lines of text. Each line of text can be up to 97 characters long.

◆ Note ◆

When you edit text files, you will normally use several of the Edit sub-menu commands to produce the results you want. See *Real-World Example 1* on page 11-11 or *Real-World Example 2* on page 11-12 for examples of how to use multiple commands from the Edit sub-menu.

Clearing the Text Buffer

You can use the **cb** command to clear the Edit buffer’s memory so you can create a new text file. To use the **cb** command, enter

cb

at the system prompt.

Loading an ASCII File into the Text Buffer

You can use the **rb** command to load—or *read*—an existing ASCII file in flash memory to the Edit buffer's memory. To use this command, enter **rb**, followed by the file you wish to edit. For example, to edit the **mpm.cmd** file, enter

```
rb mpm.cmd
```

at the system prompt.

◆ Loading Binary Files ◆

You can load a binary file into the Edit buffer but you will not be able to edit it.

Listing the Contents of the Text Buffer

The **lb** command is used to list the contents of the Edit buffer's memory. To use this command, enter

```
lb
```

at the system prompt. If there is something in the buffer, the system will display the contents numbered from the zero. The following display is a typical example:

```
00: cmDoDump=1  
01: cmlnit
```

If there is nothing in the buffer, nothing will be displayed.

Adding Lines of Text to the Text Buffer

You can use the **ab** command to manually add lines of text to the Edit sub-menu. Note that the lines you enter are appended at the end of the buffer. For example, if there are 10 lines of text in the buffer, you will begin entering text at the 11th line. If the buffer is empty, the line of text you enter will be the first line of text in the buffer.

To add text to the buffer, enter

```
ab
```

at the system prompt. A screen similar to the one shown below will be displayed:

```
02 :
```

Enter your text and press the **<Enter>** key to add the text to the buffer. If the buffer is not full, the system will prompt you to enter another line of text. If the buffer is full (i.e., there are 100 lines in the text buffer), the following message will be displayed.

```
Buffer Full!
```

To exit the **ab** command, type a period (.) and press **<Enter>**.

Deleting a Line of Text from the Text Buffer

You can use the **db** command to delete a specific line in the text buffer. To use this command, enter **db**, followed by line number of the line of text you want delete, which is shown by the **lb** command. For example, to delete the third line of text in the text buffer, enter

```
db 3
```

at the system prompt.

Enter the **lb** command again to view the contents of the buffer. Note that the text that appeared at line 3 has been deleted.

Inserting a Line of Text into the Text Buffer

You can use the **ib** command to insert a line of text between two existing lines in the buffer. To use this command, enter **ib**, followed by the number of the line where you want the new text to appear. For example, if you want to add the text, **atm_use_mbus=3**, between lines **00** and **01** in the buffer, enter

```
ib 1
```

at the system prompt. The following screen will be displayed:

```
01:
```

Enter the line of text, **atm_use_mbus=3**.

At the system prompt, enter the **lb** command to view the contents of the buffer. If the original text buffer looked like this,

```
00: cmDoDump=1
01: cmlnit
```

the revised text buffer, with the inserted text, will now appear as follows:

```
00: cmDoDump=1
01: atm_use_mbus=3
02: cmlnit
```

Editing a Line Name of Text in the Text Buffer

You can use the **eb** command to edit an existing line of text in the buffer. To use this command, enter **eb**, followed by the line number of the text you want to edit. For example, if you want to edit the text at line 01, enter

```
eb 1
```

at the system prompt. The following screen will be displayed:

```
01:
```

Enter the text as you want it to appear and press **<Enter>**.

Enter the **lb** command again to list the contents of the text buffer. Note that the buffer now reflects the edited line of text.

Creating a File Name for the Text Buffer

If no file name has been created for the text buffer, the following message is displayed whenever the **lb** command is executed:

Work buffer is unnamed

Use the **nb** command to create a name for the text buffer. To use this command, enter **nb**, followed by the name you wish to give the text buffer. For example, if you want to name the buffer **mpm.cmd**, enter

nb mpm.cmd

at the system prompt. The following screen is displayed, showing the current working directory (**/flash**), followed by the new name for the text buffer (**/mpm.cmd**):

Work buffer name is: /flash/mpm.cmd

Creating a Text File from the Text Buffer

The **wb** command is used to create—or *write*—a text file from the text buffer. To use this command, enter **wb** followed by the name of the output file. For example, if you want to create the file **switch.txt**, enter

wb switch.txt

at the system prompt. The following screen is displayed:

Work buffer name is: /flash/switch.txt

Writing Changes to Existing Files

You can also use the **wb** command to overwrite changes to an existing file. For example, if you want to overwrite changes to the file **mpm.cmd**, enter

wb mpm.cmd

at the system prompt. The following screen is displayed:

/flash/mpm.cmd exists in /flash. Overwrite it? (y)

Press **<Enter>** to create the text file from the text buffer. The computer will take a few seconds as it overwrites the file, and the following information is displayed:

File system compaction in progress...

At the system prompt, enter the **lb** command to view the name of the buffer. Note that the work buffer is now named **/flash/mpm.cmd**.

Real-World Examples

As noted on page 10-7, when you edit text files, you will normally use several of the Edit sub-menu commands to produce the results you want. The following two examples, *Real-World Example 1* and *Real-World Example 2*, are actual multi-command procedures that you may encounter as you work with your switch.

Real-World Example 1

```
cp mpm.cmd mpm.bak
rb mpm.cmd
lb
00: cmDoDump=1
01: cmlnit
nb mpm.cmd
Work buffer name is: /flash/mpm.cmd
ab
02 :
02 : reg_port_rule=1
03 :
No line 3 inserted
lb
00: cmDoDump=1
01: cmlnit
02: reg_port_rule=1
Work buffer name is: /flash/mpm.cmd
wb
/flash/mpm.cmd exists in /flash. Overwrite it? (y)
File system compaction in progress...
view mpm.cmd
cmDoDump=1
cmlnit
reg_port_rule=1
```

Real-World Example 2

```
cp mpm.cmd mpm.bak
rb mpm.cmd
lb
00: cmDoDump=1
01: cmlnit
02: reg_port_rule=1
nb mpm.cmd
Work buffer name is: /flash/mpm.cmd
db 2
lb
00: cmDoDump=1
01: cmlnit
ib 1
01 :
01 : rifStripping=1
lb
00: cmDoDump=1
01: rifStripping=1
02: cmlnit
Work buffer name is: /flash/mpm.cmd
wb
/flash/mpm.cmd exists in /flash. Overwrite it? (y)
File system compaction in progress...
view mpm.cmd
cmDoDump=1
cmlnit
rifStripping=1
```

System Menu

The System menu contains two commands, **fsck** and **newfs**, for checking and deleting all files in the flash memory. To access the System menu, enter

system

at the UI prompt.

If verbose mode is enabled, the following list of commands will be displayed automatically.

If verbose mode is disabled, press the question mark (?) to display the following list of commands. (For information on enabling verbose mode, refer to the **uic** command description in Chapter 8, “The User Interface.”)

Command	System Menu
info	Basic info on this system
dt	Set system date and time
ser	View or configure the DTE or DCE port
mpm	Configure a Management Processor Module
slot	View Slot Table information
sysstat	View system stats related to system, power and environment
taskstat	View task utilization stats
memstat	View memory use statistics
fsck	Perform a file system check on the flash file system
newfs	Erase all file from /flash and create a new file system
syscfg	Configure info related to this system
uic	UI configuration; change - prompt, timeout, more, verbose.
camstat	View CAM info and usage
camcfg	Configure CAM info and usage
hrex	Enter HRE-X management command sub-menu
ver/ter	Enables/disables automatic display of menus on entry (obsolete)
echo/noecho	Enable/disable character echo
chpr	Change the prompt for the system (obsolete, use ‘uic’ command)
logging	View system logs.
health	Set health parameters or view health statistics
cli	Enter command line interface
saveconfig	Dump the cache configuration content to the mpm.cnf file.
cacheconfig	Set the flag to use cache configuration only.
Main Interface	File Security
	Summary System
	VLAN Services
	Networking Help

Checking the Flash File System

The **fsck** command performs a file system check of flash memory, which consists of the flash file system. All image files are stored in flash memory and loaded into system memory when the switch boots up.

The command also provides diagnostic information in the event of file corruption. To perform a file system check of flash memory, enter

```
fsck
```

at the system prompt. A screen similar to the following will be displayed:

```
Your bootroms support Flash File System Version 2 and greater.
```

```
Out of 16 file descriptors in use, 0 of these are opened on the /flash device.
```

```
Performing a file system check using manual mode. If a file is encountered  
with a potential problem, you may wish to consider preserving it for technical  
support analysis...
```

```
Flash file system check in progress...  
Checking root file system... OK  
Performing file consistency check...  
Done.
```

```
There doesn't appear to be a system problem related to the Flash File  
system or kernel file system data structures. If you are experiencing  
problems with the flash file system, perhaps try using the "info",  
"systat", or "memstat" commands. They may indicate some other condition  
(such as low memory) which could prohibit correct operation of the  
file system.
```

If the **fsck** command detects a problem with the flash file system, a message will be displayed indicating the problem, along with any steps needed to resolve it.

Each logical file system (**/flash** and **/simm**) must be checked independently. If you have installed the 32 or 56 Mb SIMM upgrade and you want to check the **/simm** memory, enter

```
cd /simm
```

at the system prompt before you execute the **fsck** command.

Creating a New File System

The **newfs** command removes a complete flash file system and all files within it, replacing it with a new empty flash file system. Use this command when you want to reload all files in the file system, or in the unlikely event that the flash file system becomes corrupted.

To create a new file system and re-initialize the flash memory, enter

```
newfs
```

at the system prompt. The following will be displayed.

```
You are about to destroy all files on file system /flash. If you  
are experiencing problems with the flash file system, you might  
want to use the "fsck" command to help determine where problems  
may exist.
```

```
Are you absolutely sure you want to strip the current file  
system and create a new one? (n)
```

Press **<Enter>** to cancel, or enter **y** to create a new file system. If you enter **y**, you will have to load new software into the switch.

◆ Warning ◆

Do not power-down the switch after running the **newfs** command until you reload your image and configuration files. Otherwise, you will have to reload the image files at the boot monitor prompt using the serial interface (e.g., ZMODEM), which can take several minutes. Also, before you execute the **newfs** command, you may also want to preserve your configuration file by saving it to another host.

You can now download new files via FTP or ZMODEM.

Creating a New File System in the SIMM Directory

If you have installed the 32 or 56 Mb SIMM upgrade and you want to create a new file system in the SIMM's memory, enter

```
cd /simm
```

at the system prompt before you execute the **newfs** command.

12 Switch Security

Commands listed in the Security menu are for configuring system security parameters such as the password and logout time. The menu also provides a command for rebooting the switch. Enter

security

at the prompt to enter the Security menu. Press ? to see the following list of commands:

<u>Command</u>	<u>Security Menu</u>
pw	Set a new password for a login account
reboot	Reboot this system (allowed if the user is "admin")
timeout	Configure Auto Logout Time (obsolete, use "uic" command)
layer2auth	Enable/Disable layer2 user authentication
seclog	Display Secure Access log file entries
secdefine	Define Secure Access filter(s)
secapply	Apply Secure Access filter(s)
useradd	Create a new user for a login account
usermod	Modify a user's privileges
userdel	Remove a user
asacfg	Configure Authenticated Switch Access
userview	View the users in the local user database
auth	Enter the Authentication menu

Main File Summary VLAN Networking
Interface Security System Services Help

The **pw**, **reboot**, **seclog**, **secdefine**, and **secapply** commands are described in this chapter. The **useradd**, **usermod**, **userview** and **userdel** commands are also described in this chapter.

For information about the **layer2auth** and **asacfg** command as well as the authentication (**auth**) submenu, see the *Switched Network Services User Manual*.

Changing Passwords

The switch provides three types of login accounts by default—Administrator, User and Diagnostics. The Administrator login provides full READ/WRITE access to all command families. The login name for the Administrator account is **admin**. The login name for the default User account is **user** and provides READ ONLY access to the switch's command families except for the global family, and NO WRITE privileges. The Diagnostics login has full READ/WRITE access to all command families plus a command for running switching module tests. The login name for Diagnostics is **diag**.

The initial password for all three accounts is **switch**. If you log in as **diag** you can change the passwords for the **diag** and **admin** login accounts. If you log in as **admin**, however, you can only change the password for the **admin** login account. To change the password, complete the following steps. Remember that the User Interface does not echo (display) the password characters.

1. From the prompt, type

pw <account-name>

The **<account-name>** is the user login name (**diag**, **admin**) for which you want to change the password. The following prompt displays:

**Changing password for account:<account-name>
Old password:**

2. Enter the old password and press **<Enter>**. If you enter the old password incorrectly, the following message displays:

Authentication failure

and the command will terminate. You will then need to start over from **Step 1** above.

If you answered the old password correctly, the following prompt displays:

New password:

3. Enter the new password (you are allowed up to 18 characters) and press **<Enter>**. The following prompt displays:

Retype new:

4. Re-enter the new password to confirm it and press **<Enter>**.

◆ Note◆

It is recommended that you change the password from the default for all login accounts.

The passwords are stored encrypted in the **mpm.cnf** file. If you forget your password, you will have to delete the **mpm.cnf** file which will cause the passwords to revert to the default.

◆ Caution ◆

Deleting the **mpm.cnf** file will also remove all of your configuration data and restore everything back to factory settings.

Rebooting the Switch

The **reboot** command should only be executed during network down time and when no data is being transmitted across the network. Also, you should ensure that all configuration information has been saved first. Note that the **reboot** command is only available to the **admin** and the **diag** logins.

◆ **Caution** ◆

Rebooting the switch will disconnect a Telnet connection to the User Interface and will interrupt the network connections on the switching modules.

To reboot the switch from the command line, enter

reboot

at the prompt and press **<Enter>**. The following prompt will display:

Confirm? (n) :

Enter **Y**. The following message displays:

```
Locking file system...locked  
System going down immediately...  
switch[489917b0]: System rebooted by admin
```

The switch will now take at least a minute to start up again. (If you are connected to the User Interface with a serial connection, the console displays start-up related information.) The login message displays when the reboot is complete:

```
Welcome to the Alcatel OmniSwitch! (Serial # xxxx)  
login :
```

Secure Switch Access

Secure Switch Access is a filtering program that prevents unauthorized access to the switch by allowing you to define a list of *filters* and *filter points*. For Secure Switch Access, filters are lists of source traffic that are allowed onto the switch. Filter points operate on IP protocols that include FTP, Telnet, SNMP, TFTP, HTTP, and a custom IP protocol. Whenever any of these filter points is enabled, all filters configured for that protocol are applied to incoming traffic using the filter point protocol.

All access violations are logged. If a filtering point is not enabled, it is accessible to all users.

Configuring the Secure Switch Access Filter Database

Use the **secdefine** command to view and configure the database of secure access filters. This database includes information on filter names, source IP addresses, source MAC addresses, and the physical ports receiving data.

The following is a sample **secdefine** display:

```

Secure Access Filter Database

List      (l) :
Create    (c) :
Delete    (d) :
Modify    (m) :
Find      (f) :
Help      (h) :
Quit      (q) :
Enter selection:

```

Select an option by entering the relevant letter at the selection prompt. To exit this menu, enter **q** (quit). Descriptions and sample displays for each of the options are as follows:

List

This is a list of all defined filters. A filter determines what traffic is allowed on the switch. The list includes information on the filter's name, IP Address, MAC Address, and physical port receiving the user's data. The following is a sample display:

Filter Name	Source IP Address	Source MAC Address	Slot #	Port #
Engineering	198.34.56.10	0:23:da:67:97:e4	4	1
Test	ANY	ANY	7	3
Accounting	172.14.25.13	0:32:e4:a3:6f:e4	2	1
HR	198.34.56.15	ANY	ANY	ANY

The value **ANY** displays if a field is left blank when configuring filter information through the **Create (c)** option. The **ANY** value signifies a "don't care" condition. When an inbound packet is checked against a Filter Name to establish authorized access, the **ANY** fields are not checked.

Create

This option allows you to create a new filter in the secure access database. The following is a sample display:

```

Create Filter
-----
Enter Filter Name:

Enter IP Address ( [a.b.c.d] ) :
Enter MAC Address ( [XXYYZZ: AABBC] ) :
Is this MAC in Canonical or Non-Canonical (C or N) [C] :
Enter Slot :
Enter Port :

```

After you have created a filter, the information is automatically saved in the secure access database, and the **secdefine** submenu re-displays. To review your new configuration, simply select the list (I) option. Descriptions of the fields are as follows:

Enter Filter Name: The name of the new filter. The name is required and must be at least one character long and no more than 25 characters.

Enter IP Address ([a.b.c.d]): The allowed IP address. The address must be in the displayed format ([a.b.c.d]). If you enter a value here, the user may access the switch only from this IP address. If you leave this field blank, a value of **ANY** will display in the secure access list, allowing access to the switch from any IP address.

Enter MAC Address (([XXYYZZ: AABBC])): The allowed MAC address. The address must be in the displayed format (([XXYYZZ: AABBC])). If you enter a value here, a user may access the switch only from this source MAC address. If you leave this field blank, a value of **ANY** will display in the secure access list, allowing this user access to the switch from any MAC address.

Is this MAC in Canonical or Noncanonical (C or N) [C] : The format of the specified MAC address. Typically, ethernet MAC addresses are in canonical format while token ring and addresses are in noncanonical format. The default is canonical (C). This parameter is not required.

Enter Slot: The module on the switch receiving data from the specified IP or MAC address. If you leave this field blank, a value of **ANY** will display in the secure access list, allowing data from the specified IP or MAC address to be sent through any module on the switch.

Enter Port: The port on the module receiving data from the specified IP or MAC address. If you enter a value here, you should also specify a slot in the above field. If you leave this field blank, a value of **ANY** will display in the secure access list, allowing data from the specified IP or MAC address to be sent through any port on the module (if one is specified) or on the switch (if no slot is specified).

Delete

This option allows you to delete a filter from the secure access list. The screen displays similar to the following:

```

Delete Filter
-----
Enter Filter Name:

```

If you enter a filter name here, that filter will be immediately deleted from the secure access database.

Modify

This option allows you to modify information about an existing secured access filter. Enter the name of the filter you wish to modify, as follows:

Modify Filter

Filter Name: Test

The filter's existing information will display. For example:

Filter Name	Source IP Address	Source MAC Address	Slot #	Port #
Test	ANY	10.2.8.13	5	2

Enter IP Address ([a.b.c.d]) :

Enter MAC Address ([XXYYZZ: AABBC]) :

Is this MAC in Canonical or Non-Canonical (C or N) [C] :

Enter Slot :

Enter Port :

To change a value, type in the new value at the prompt. If you do not wish to modify a particular field, press **Enter** and the existing user information will remain unchanged. To change a field to **ANY** privilege, enter a value of **0**, an asterisk (*), or **ANY** at the prompt. Descriptions of the fields in the above display are provided earlier under the option "List" on page 12-4.

Find

This option allows you to find information about a specified filter in the secured access database. You must know the filter's name in order to use this search feature. The following is a sample display:

Find Filter

Filter Name: Test

To find a filter in the database, enter the name of the filter at the prompt. If the filter you enter is a valid one, information on that filter will display similar to the following:

Filter Name	Source IP Address	Source MAC Address	Slot #	Port #
Test	ANY	10.2.8.13	5	2

Configuring Secure Access Filter Points

The **secapply** command allows you to view the list of secure access filter points, to enable/disable security globally or for a specific IP protocol filter point, and to define a filter list for each filter point. To use this command, enter:

```
secapply
```

A screen similar to the following displays:

```

                Secure Access Filter Points

1) FTP Security           : Enabled
   11) Filter List       : Test, Engineering
2) Telnet Security       : Disabled
   21) Filter List       : Test
3) SNMP Security         : Enabled
   31) Filter List       :
4) TFTP Security         : Enabled
   41) Filter List       : Manufacturing
5) HTTP Security         : Disabled
   51) Filter List       :
6) Custom Security       : Enabled
   61) Filter List       : HR
   62) Protocol          :
   63) Port Service      :
7) One-touch Global Security :
   71) One-touch Filter List :

Command { Item=Value/?/Help?Quit/Redraw/Save} (Redraw) :
```

◆ Note ◆

If security is enabled for a filter point and there are no names defined on its list, then the filter point is essentially inaccessible to all users. For example, in the above sample display, SNMP is not accessible to any user.

You can enter commands by entering just the first letter of the command. For example, select **Quit** by entering **q** and pressing **<Enter>**. The question mark option (?) and the **Help** option provide reference and instructional information on using this command. The **Quit** option exits this command without saving configuration changes. The **Redraw** option refreshes the screen.

When you are done entering new values, type **save** at the prompt and all new settings will be saved.

The following option is available for all filter points:

Filter List

Applies the filter name(s) defined through the **secdefine** command for this filter point.

Filter points are disabled by default. The different filter points are defined as follows:

1) FTP Security

Indicates whether or not secure access is enabled for File Transfer Protocol (FTP) on the switch. **Enabled** means secure access is enabled for FTP services, and only filters on FTP's filter list have authorization. **Disabled** indicates that secure access is not enabled for FTP services, and all users can access the switch through FTP.

2) Telnet Security

Indicates whether or not secure access is enabled for Telnet service on the switch. **Enabled** means secure access is enabled, and only filters on Telnet's filter list have authorization. **Disabled** indicates that secure access is not enabled for Telnet service, and all users can access the switch through Telnet.

3) SNMP Security

Indicates whether or not security is enabled for Simple Network Management Protocol (SNMP) on the switch. **Enabled** means security is enabled for SNMP services, and only filters on SNMP's filter list are authorized. **Disabled** indicates that secure access is not enabled for SNMP services, and all users can access the switch through SNMP.

4) TFTP Security

Indicates whether or not security is enabled for Trivial File Transfer Protocol on the switch. **Enabled** means security is enabled for TFTP services, and only users on TFTP's filter list are authorized. **Disabled** indicates that security is not enabled for TFTP services, and all users can access the switch through TFTP.

5) HTTP Security

Indicates whether or not security is enabled for HyperText Transfer Protocol (HTTP) on the switch. **Enabled** means that security is enabled for HTTP, and only filters on HTTP's filter list are authorized. **Disabled** indicates that security is not enabled for HTTP, and all users can access the switch through HTTP.

6) Custom Security

Configures whether or not security is enabled for the custom IP protocol specified in line 62. **Enabled** means that security is enabled for the custom IP protocol, and only filters on that protocol's filter list are authorized. **Disabled** indicates that security is not enabled for the custom IP protocol, allowing all users access to the switch through that protocol.

62) Protocol

(Available for Custom Security only.) The IP protocol number to be included as a secured access protocol (IP protocol field in the IP header). You may define only one custom IP protocol.

63) Port Service

(Available for Custom Security only.) The Custom IP protocol's destination port (port field in the IP header)

7) One-touch Security

Configures the same **Security** value for all secure access protocols. **Enabled** enables security for all secure access filter points. **Disabled** disables security for all secure access filter points. Any value configured for individual security parameters overrides the global setting. If you wish to set a different value for **Telnet Security**, for example, enter the line number for Telnet, followed by an equal sign (=) and the new value.

71) One-touch Filter List

Configures a single filter list for all security filter points.

Enabling/Disabling Security Parameters

To change any of the **Security** values, enter the line number for the parameter, followed by an equal sign (=), and then **enabled** or **e** for enable or **disabled** or **d** for disable at the prompt. For example, to enable security for Telnet, enter the following:

```
2=e
```

Adding Filters

To add a filter, at the command prompt, enter the line number for the parameter, followed by an equal sign (=), and then the filter's name at the prompt. For example:

```
21=Test
```

◆ Note ◆

If the filter does not exist in the secure access database, the system prompts you to create the filter. To view the list of secure access filters, use the **secdefine** command. For more information, see “Configuring the Secure Switch Access Filter Database” on page 12-4.

Enter **save** to save the new filter.

Deleting Filters

To remove an existing filter from a filter list, at the command prompt, enter the line number for the parameter, followed by an equal sign (=), a negative sign (-), and then the filter's name as follows:

```
11=-Engineering
```

To remove all filters in a list, include an asterisk after the negative sign. For example:

```
4=-*
```

Enter **save** to save the change.

Viewing Secure Access Violations Log

The **seclog** command displays a log of all secure access violations.

◆ **Note** ◆

To log access violations on the switch, use the **swlogc** command. For more information on the **swlogc** command, see Chapter 14, “Switch Logging.”

To view the secure access violations log, enter

seclog

The following is a sample display:

Secure Access Violations Log						
Time	Protocol	Source IP	Attempts	Slot/ Intf	Elapsed Time (secs)	
12:49:02	FTP	172.23.8.801	1	5/1	23	
03:15:34	Telnet	198.20.2.101	10	2/3	240	

Descriptions of the fields are as follows:

Time. The first time the access violation occurred.

Protocol. The IP protocol for which the violation occurred.

Source IP. The source IP address of the unauthorized user.

Attempts. The number of access attempts made by this user within the sample period (5 minutes).

Slot/Intf. The physical port that received the unauthorized user information.

Elapsed Time (secs). The duration (in seconds) from the first unauthorized access to the end of the sampling period. Secure access violations will take 5 minutes to display in the log file.

Managing User Login Accounts

Prior to software release 4.4, the switch provided security in the form of privilege control for individual login accounts by allocating each user accounts READ or WRITE privileges. Software release 4.4 contains a partition management feature that enhances the privilege capability with an authorization scheme based on the functional capacity assigned to each user.

The purpose of partition management is to provide a mechanism in the switch operating system for system administrators to control access while maintaining enough flexibility to use the switch's full range of services. This is normally done for security reasons. System administrators can partition access to the switch by restricting a user's ability to perform certain switch commands or to use certain command groups.

◆ Terminology Notes◆

A *user account* refers to the user's ability to log onto the switch and perform certain functions. From the user's perspective, it consists of the login name and a password.

A *privilege* refers to the user's ability or permission from the system administrator to execute a command.

Partition Management Requirements

Partition management is available *only* for user login accounts that have *no* permission to use the UI command mode. Where a user account has permission to use the UI mode, partition management is effectively destroyed for that user account. To maintain partition management capability for a user account, that account must be restricted to using the CLI mode only. Refer to "Assigning Account Privileges Using the UI Command Mode" on page 12-16 or "Assigning Account Privileges Using the CLI Command Mode" on page 12-13 for information on restricting use UI commands.

◆ Note◆

Not all UI commands have CLI equivalents. Also, not all CLI commands support partition management. For detailed information, refer to the UI to CLI Cross Reference Tables in Chapter 8 of this manual.

Default Accounts

Initially each switch is preconfigured with three default logins (**admin**, **user** and **diag**). See Chapter 8, “The User Interface,” for more information about login accounts. If you are logged into an account with the **WRITE** privilege to the **USER** command you may create or delete login accounts as described in this section. You may also create new user accounts.

◆ Note◆

At least one **user** account with **WRITE** privileges to use the **USER** family of commands is required on the switch at all times. If you attempt to remove or modify the only user account to **READ-ONLY** privilege, the switch will reject the modification command.

There are several commands available for modifying the user login accounts on the switch. To see a list of all user accounts currently available on the switch, use the **userview** command in the UI mode.

Adding a User Account Using the UI Command Mode

To add a user account you must be logged into an account with administrative privileges.

1. At the system prompt enter the **useradd** command. The following prompt displays:

Enter Username: () :

2. Enter the desired user name. The following prompt displays:

Force Password change on next login [y/n] ? (y) :

3. Press **<Enter>** to force a password change at the next login for this user, or enter **n** to keep the configured password. The following prompt displays:

Enter password: () :

4. Enter the desired password. The following prompt displays:

Enter new password again: () :

5. Enter the desired password again. In this example, the username “TechPubs1” is entered. A message similar to the following displays:

User TechPubs1 user privileges (0:0:0) :

The user login account “TechPubs1” is now active on the switch.

At this point the new account has permission to log onto and off of the switch. To add other privileges refer to “Assigning Account Privileges Using the UI Command Mode” on page 12-16 or to “Assigning Account Privileges Using the CLI Command Mode” on page 12-13.

Adding a User Account Using the CLI Command Mode

To add a user account from the CLI mode, you must be logged into an account with administrative privileges. Enter the following at the command prompt.

```
user user_name <password user_password>
```

where *user_name* is the new user login account name and *user_password* is the new user login account password. Both these values are specified by the user. For the user name “Techpubs1”, the following message is displayed:

```
User Techpubs1 created.
```

If you do not specify a password when you create the new account, **switch** becomes the default password.

◆ Note◆

It is recommended that you change the password from the default for all login accounts.

Both the user account name and the password are limited to 16 text characters. The new login account and password will take effect at the user’s next login session.

Assigning Account Privileges Using the CLI Command Mode

A user account’s READ and WRITE privileges can be assigned for all commands or for various subsets of commands. The command subsets referred to as command families are shown here:

config, vlan, iprout, ipxrout, bridge, snmp, xswitch, hrefilter, atmser, atmup, cem, csm, pnni, atmacct, voip, mpoa, and **user.**

In addition to assigning privileges according to command families, an administrator can restrict the user account’s ability to execute specific commands. Here is a list of commands that can be restricted from a user account.

system, status, slot, timeout, prompt, define, prefix, reboot, telnet, ftp, ping, swap, reset, cd, ls, rm, file, interface, ethernet, gated, and **ui.**

◆ Warning◆

If partition management is intended for a user account, that account *cannot* have permission to use the UI command or the UI mode.

User Write Privileges

To assign privileges to a user account, you must be logged into an account with WRITE privileges to the USER family of commands. Enter the following command at the system prompt.

```
user userId [write list-of-families]
```

where *userId* indicates the name assigned to the user account for which you want to assign READ and WRITE privileges. The *list-of-families* parameter indicates the switch command families and the specific commands for which the user account will receive READ and WRITE privileges. Command families must be separated by commas.

User Read Privileges

To assign READ-ONLY privileges to a user account, you must be logged into an account with WRITE privileges to the USER family of commands. Enter the following command at the system prompt.

```
user userId [read list-of-families]
```

where *userId* indicates the name assigned to the new login account for which you want to assign READ-ONLY privileges. The *list-of-families* parameter indicates the switch command families and the specific commands for which the user account will receive READ-ONLY privileges. For a list of command families and specific commands, refer to the “Assigning Account Privileges Using the UI Command Mode” section on page 12-16 or to “Adding a User Account Using the CLI Command Mode” on page 12-13.

Removing Privileges

You can remove READ and WRITE privileges from a user created login account if you are logged into an account with WRITE privileges to the USER command family. Use the following command:

```
user userId no write list-of-families
```

You can remove READ-ONLY privileges from a user created login account by using the following command:

```
user userId no read list-of-families
```

For both these commands, the *userId* parameter indicates the name assigned to the user created login account for which you want to remove privileges. The *list-of-families* parameter indicates the switch command families and the specific commands from which you want to remove READ or WRITE privileges.

Miscellaneous CLI Privileges Commands

The following is a list of privileges-related CLI commands. For more details on these commands and other CLI commands, refer to the *Text-Based Configuration CLI Reference Guide*.

- To create a new user login account, use the following command:

```
user user_name [password user-password]
```

where *user_name* is the new user login account name and *user-password* is the new user password. Both these values are defined by the user.

- To set or change the password of the current user account, use the following command:

```
password password
```

Where *password* is the new *password* for this user account.

- To delete a login account, use the following command:

```
no user user_name
```

where *user_name* is the current login you want to delete.

- To view user privileges for a specific user login account, use the following command:

```
view user [user_name]
```

where *user_name* is the name of the user login account for which you will view privileges.

Assigning Account Privileges Using the UI Command Mode

When you add a new user login account, the account has permission to log in and to log out. If you want the new account to have additional privileges you must add them separately. To add privileges to a user account, you must be logged into an account with administrative privileges. From the system prompt enter the **usermod** command. The following prompt displays:

Enter Username : () :

Enter the login name of the user account you are modifying. The following screen will display.

```
- CONFIG      : NO
- GROUP       : NO
- IPROUT      : NO
- IPXROUT     : NO
- BRIDGE      : NO
- SNMP        : NO
- XSWITCH     : NO
- HREFILTER   : NO
- ATMSEAR     : NO
- ATMUP       : NO
- CEM         : NO
- CSM         : NO
- PNNI        : NO
- ATMACCT     : NO
- VOIP        : NO
- MPOA        : NO
- MPLS        : NO
- USER       : NO
Subsets of the global family:
- SYSTEM      : NO
- STATUS      : NO
- SLOT        : NO
- TIMEOUT     : NO
- PROMPT      : NO
- DEFINE      : NO
- PREFIX      : NO
- REBOOT      : NO
- TELNET      : NO
- FTP         : NO
- PING        : NO
- SWAP        : NO
- RESET       : NO
- CD          : NO
- LS          : NO
- FM          : NO
- FILE        : NO
- INTERFACE   : NO
- ETHERNET    : NO
- GATED       : NO
- UI          : NO
1. MODIFY ONE FAMILY RIGHTS
2. SET ALL READ RIGHTS
3. SET ALL WRITE RIGHTS
4. SET NO READ RIGHTS
5. SET NO WRITE RIGHTS
6. MODIFY ONE GLOBAL SUBSET
7. SET NO GLOBAL SUBSET
8. SET ALL GLOBAL SUBSET
```

[1 TO 8, (c)ancel or (s)sav] () :

This screen displays the default privileges for a new user login account. Note that the default privileges give the new user neither read nor write permission. To grant privileges to the user account, enter a number from 1 to 5 as indicated in the display. To set WRITE privileges for a single family of commands, enter **1** and press **<Enter>**. The display will prompt you for the family number as shown here:

Give the family number : () :

Enter the number of the command family for which you want to set WRITE privileges. Refer to the “Command Family Table” on page 12-18 for the number.

For example, if you wanted to enable WRITE privileges for the Bridge command family, enter the number **5** as shown here.

Give the family number : () : 5

The following will display.

```
Give rights on family BRIDGE
  0.      NO
  1.      READ
  2.      WRITE
  3.      READ&WRITE
( ) :
```

Enter the number **2** at the prompt to assign WRITE privileges. The following shows a portion of the display.

```
User 'TechPubs1' user privileges (0:0X20:0) :
- CONFIG      : NO
- GROUP       : NO
- IPRROUT     : NO
- IPXROUT     : NO
- BRIDGE      : READ & WRITE
- SNMP        : NO
- XSWITCH     : NO
(Continued)
```

The privilege listed next to Bridge shows WRITE. This indicates that the user “TechPubs1” now has WRITE privileges for the Bridge family of commands.

Command Family Table

Number	Command Family
1	Configuration
2	Group
3	IP Routing
4	IPX Routing
5	Bridge
6	SNMP
7	QOS Policy
8	HRE Filter
9	ATM Service
10	WAN
11	CSM
12	PNNI
13	ATM Accounting
14	Voice Over IP
15	MPOA
17	(unsupported)
18	User

The global family contains commands that apply globally to the switch rather than to individual applications or services. Privileges for global family commands can be set on an individual command basis or altogether so the privilege applies to the whole global family. If you want to set privileges for the global commands, you must enter 6, 7 or 8 when the screen prompt displays the following:

1. MODIFY ONE FAMILY RIGHTS
2. SET ALL READ RIGHTS
3. SET ALL WRITE RIGHTS
4. SET NO READ RIGHTS
5. SET NO WRITE RIGHTS
6. MODIFY ONE GLOBAL SUBSET
7. SET NO GLOBAL SUBSET
8. SET ALL GLOBAL SUBSET

[1 TO 8, (c)ancel or (s)ave] () :

To give the user account the privilege to set all global commands, enter the numeral 8. To deny the user the privilege to set any of the global commands, enter the numeral 7. To set individual global commands, enter the number 6. If you are assigning privileges on an individual command basis the display will look like this:

[1 TO 8, (c)ancel or (s)sav] () : 6
Give the subset number : () :

Enter the number of the command for which you want to set WRITE privileges. Refer to the “Global Family Table” on page 12-19 for the number.

Global Family Table

Number	Global Family
1	System
2	Status
3	Slot
4	Timeout
5	Prompt
6	Define
7	Prefix
8	Reboot
9	Telnet
10	FTP
11	Ping
12	Swap
13	Reset
14	CD
15	LS
16	RM
17	File
18	Interface
19	Ethernet
20	Gated
21	UI

For example, if you wanted to assign the user account the privilege to use the define command, enter the number 6 as shown here.

Give the family number : () : 6

The following will display.

Give rights on subset DEFINE

0. NO
1. YES

() :

If you enter 1, all the command families will display and the DEFINE command under the global family will be shown as follows:

- DEFINE : YES

After you set the user account privileges, the switch displays the current configuration. At this point you may enter **s** to save your configuration or **c** to cancel.

◆ Warning◆

If partition management is implemented on a user account, that account *must* have the UI command family set to NO privilege. If an account has the privilege to use the UI command, partition management is effectively destroyed for that account.

Modifying a User Account

You can use the **usermod** command to modify account privileges as shown here. You must be logged into a user account with administrative privileges.

1. At the system prompt enter the **usermod** command. A prompt similar to the following displays:

```
Enter Username: ( ) :
```

2. Enter the name assigned to the user account you want to modify. A screen similar to the following displays where the account name is **TechPubs1**.

```
User 'TechPubs1' is configured with the following privileges:  
READ
```

1. READ
2. WRITE
3. ADMIN
4. FORCE new password

```
Select the privilege(s) number to add/remove.  
[ 1, 2, 3 (c)ancel or (s)ave] (c) :
```

◆ Note ◆

See “Managing User Login Accounts” on page 12-11 for definitions of the privileges.

3. Enter the number for the privilege you want to add or remove. The entry acts as a toggle to turn the privilege on or off for the user. In the current example, if you enter **2** at the prompt, a screen similar to the following displays:

```
User 'TechPubs1' is configured with the following privileges:  
READ WRITE
```

4. After modifying the privileges for the user, enter **s** at the selection prompt to save the change(s).

Deleting a User

To delete a user from the user database, you must be logged into an account with administrative privileges.

1. At the system prompt, enter the **userdel** command. The following prompt displays:

```
Enter Username to remove: ( ) :
```

2. Enter the username for the user you want to delete. A message similar to the following displays:

```
User 'TechPubs1' was removed.
```

◆ Note ◆

All users but one may be deleted from the switch, provided that the one remaining user is configured with all privileges.

13 Configuring Switch-Wide Parameters

The switch provides commands to display and configure parameters on a switch-wide basis. These commands are grouped into two menus: the Summary menu and the System menu. Descriptions for commands in the Summary menu begin below; descriptions for commands in the System menu begin on page 13-5.

In addition, this chapter contains documentation for configuring HRE-X and HRE-VX ports (described in *Configuring the HRE-X/HRE-VX Router Port* on page 13-27) duplicate MAC address support (described in *Duplicate MAC Address Support* on page 13-30), multicast claiming (described in *Multicast Claiming* on page 13-32), disabling flood limits (described in *Disabling Flood Limits* on page 13-32), and saving configurations (described in *Saving Configurations* on page 13-33).

Summary Menu

The Summary menu consists of commands for displaying summary switch information. To access this menu, enter

summary

at the UI prompt. Type the question mark (?) to see the following list of commands.

<u>Command</u>	<u>Summary Menu</u>
ss	Display MIB-II System group variables
sc	Display a summary of the chassis (type, id, serial no., base mac, etc.)
si	Current interface status

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

The Summary menu commands are described in the sections that follow.

Displaying the MIB-II System Group Variables

MIB-II is a core set of definitions created to define the SNMP-based management framework. This MIB module contains definitions for both end systems and routers using the Internet protocol suite. To display the MIB-II system group variables, enter

```
ss
```

at the system prompt. A screen similar to the following will be displayed.

```
System description:   Alcatel Omni Switch/Router
System Object ID:    1.3.6.1.4.1.800.3.1.1.2.
Agent Up Time:       5 days, 00:28:14.38
Contact:             Administrator
Name:                TechWrite
Location:            Bldg 46
Device Services:
  DataLink/Subnetwork Layer
  Internetwork Layer
  Host Layernetwork Layer
  Application Layer (Rlogin, Telnet, FTP)
```

The fields displayed by the **ss** command are described below.

System description. The specific type of chassis, which can be an OmniSwitch, OmniAccess, or Omni Switch/Router. This field is set by the **syscfg** command, which is described in *Configuring System Information* on page 13-23.

System Object ID. The MIB entry for the switch (where the object ID starts). This is read only. This value helps you locate Alcatel-specific variables in the MIB tree.

Agent Up Time. The time (in days, hours, minutes, and seconds) since the switch was re-initialized.

Contact. The name of a person to contact about this switch. This field is set by the **syscfg** command, which is described in *Configuring System Information* on page 13-23.

Name. The name the system administrator assigned to this switch (the node's fully qualified domain name, by convention). This field is set by the **syscfg** command, which is described in *Configuring System Information* on page 13-23.

Location. The physical location of the switch. This field is set by the **syscfg** command, which is described in *Configuring System Information* on page 13-23.

Device Services. The type of services provided by the switch. Supported service types are listed below:

- Data Link /Subnetwork Layer
- Internetwork Layer
- Host Layer
- Application Layer (Rlogin Telnet, FTP)

Displaying the Chassis Summary

To display the chassis summary information, enter

```
sc
```

at the system prompt. A screen similar to the following will be displayed.

```

Type:                Omni Switch/Router XFRAME 9-slot
Chassis ID:         Alcatel
Description:        DESCRIPTION NOT SET.
Backplane:          5 SLOT
Master MPM Serial No.: 52601675
Physical Changes:   7
Logical Changes:    0
Number of Resets:   26
Base MAC Address:   00:20:da:02:04:80
Free Slots:         0

```

The fields displayed by the **sc** command are described below.

Type. The description of the specific type of chassis or device.

Chassis ID. The chassis ID for this switch.

Description. The description of this chassis. This field is set by the **syscfg** command, which is described in *Configuring System Information* on page 13-23.

Backplane. The style of backplane in this chassis.

Master MPM Serial No. The serial number for the primary MPM.

Physical Changes. The number of physical changes that has occurred since the last reset or power-on.

Logical Changes. The number of logical changes that has occurred since the last reset or power-on.

Number of Resets. The number of times this switch has been reset since the configuration file (**mpm.cnf**) was first removed.

Base MAC Address. The base MAC address for the primary MPM.

Free Slots. The number of front panel slots not occupied by a switching module.

Displaying Current Router Interface Status

To display current interface status information, enter

si

at the system prompt. A screen similar to the following will be displayed.

Interface Summary Status			
4 Interfaces			
Logical Interface	Interface Type	Administrative Status	Operational Status
1	Slip	Enabled	Enabled
2	Virtual Router	Enabled	Active
3	Virtual Router	Enabled	Active
4	SoftwareLoopback	Enabled	Enabled

The fields displayed by the **si** command are described below.

Logical Interface. A number, in sequence, that has been assigned to the virtual router port.

Interface Type. The type of interface, which can be virtual router (the standard interface type), SLIP, and software loopback.

Administrative Status. Whether the administrator has enabled or disabled the port. The port can be enabled by the administrator but still be made inactive by the system.

Operational Status. Whether the port is active (operational) or inactive. This status is set by the system software.

System Menu

The System menu contains commands to view or set system-specific parameters. To access this menu, enter

system

at the UI prompt to enter the System menu. If you are not in verbose mode, press a question mark (?) and then press **<Enter>** to display the commands in the system menu, as shown below.

<u>Command</u>	<u>System Menu</u>
info	Basic info on this system
dt	Set system date and time
ser	View or configure the DTE or DCE port
mpm	Configure a Management Processor Module
slot	View Slot Table information
systat	View system stats related to system, power and environment
taskstat	View task utilization stats
taskshow	View detailed task information
memstat	View memory use statistics
fsck	Perform a file system check on the flash file system
newfs	Erase all file from /flash and create a new file system
syscfg	View/Configure info related to this system
uic	UI configuration; change - prompt, timeout, more, verbose.
camstat	View CAM info and usage
camcfg	Configure CAM info and usage
hrex	Enter HRE-X management command sub-menu
ver/ter	Enables/disables automatic display of menus on entry (obsolete)
echo/noecho	Enable/disable character echo
chpr	Change the prompt for the system (obsolete, use 'uic' command)
logging	View system logs.
health	Set health parameters or view health statistics
cli	Enter command line interface
saveconfig	Dump the cache configuration content to the mpm.cnf file.
cacheconfig	Set the flag to use cache configuration only.

Main File Summary VLAN Networking
Interface Security System Services Help

All of the System menu commands—except for the **mpm**, **ver**, **ter**, **echo**, **noecho**, **chpr**, **logging**, **health**, and **cli** commands—are described in the following sections. The **uic**, **ver/ter**, **echo**, **noecho**, **chpr**, and **cli** commands are described in Chapter 8, “The User Interface.” The **mpm** command is described in Chapter 10, “Configuring Management Processor Modules.”

◆ Note ◆

The **ver**, **ter**, and **chpr** commands now appear as items in the UI Configuration menu (displayed through the **uic** command). If you enter the **ver/ter** and **chpr** commands, a message will advise you to use the **uic** command, and the UI Configuration menu will automatically display. For more information on the UI Configuration menu, refer to Chapter 8, “The User Interface.”

Displaying Basic System Information

To display basic information on the switch, enter

```
info
```

at the system prompt. The following display is a typical example.

```
System Make: Alcatel OmniSwitch
System Type: 5-slot OmniSwitch
Description: DESCRIPTION NOT SET.

Backplane: 9 SLOT                Bus Speed: 1200 XFRAME

Physical changes to the system since power-up or reset: 2
Logical changes to the system since power-up or reset: 0
Number of Resets to this system: 8

The attached MPM, slot 1, is the Primary
Automatic configuration synchronization is enabled

System base MAC Address: 00:20:da:04:21:f0
Number of Free Slots: 0
Action on Cold Start: Load & go
Action on Reset: Restart

VBus Mode : Mode 1

Script File: /flash/mpm.cmd
Boot File: /flash/mpm.img
Ni Image Suffix: img
```

The fields displayed by the **info** command are described below.

System Make. The description of the specific type of chassis or device.

System Type. The OmniSwitch type.

Description. A description of the chassis and product. This field is set by the **syscfg** command, which is described in *Configuring System Information* on page 13-23.

Backplane. The style of backplane used in this chassis.

Bus Speed. The speed of backplane, in Mbs, used in this chassis.

Physical Changes to the system since power-up or reset. The number of physical changes that has occurred since the last reset or power-on.

Logical Changes to the system since power-up or reset. The number of logical changes that has occurred since the last reset or power-on.

No. of Resets to the System. The number of times this switch has been reset since the last cold start.

◆ **Note** ◆

The **info** command will also display the number of MPMs, their location in chassis, and which one is the primary and which one is the secondary. In addition, it also displays whether automatic configuration synchronization is enabled. See Chapter 10, “Configuring Management Processor Modules,” for more information on redundant MPMs and automatic configuration synchronization.

System Base MAC Address. The base MAC address for the primary MPM in chassis.

Number of Free Slots. The number of slots not occupied by a module.

Action on Cold Start. The action taken when you switch the power on.

Action on Reset. The action taken when you reboot.

Script File. The name of the command file (**mpm.cmd** is the default) containing user-configurable commands.

Boot File. The boot file (**mpm.img** is the default) used by the switch when it boots up or reboots.

Ni Image Suffix. The name of the file extension (**img** is the default) indicating that the file is an executable binary file. See Chapter 10, “Configuring Management Processor Modules,” to change this suffix.

Setting the System Date and Time

The **dt** command allows you to set the local date, time, and time zone. Additionally, you can set the system clock to run on Universal Time Coordinate (UTC or GMT). If applicable, you can also configure Daylight Savings Time (DST) parameters. To view or make changes to date, time, time zone, and DST for the switch, enter

dt

at the System prompt. This command displays a screen similar to the following:

Modify Date and Time Configuration

```
1) Local time                : 1:45:41
2) Local date                : 01/15/01
3) Timezone (-13 . . 12, name) : MST   UTC-7 hrs
4) Daylight Savings Time active : DisabledCommand
{Item=Value/?/Help/Quit/Redraw/Save} (Redraw) :
```

To use the **dt** command, you must have UI write privileges. Enter the line number for the variable that you would like to change, an equal sign (=), and then the new value for the variable. For example, to set a new date, you would enter:

2=4/20/99

After you have made changes, enter

save

to save your changes and to exit the **dt** menu. If you do not wish to make any changes, enter

quit

at the system prompt. The following sections describe the variables on this screen.

1) Local time

Indicates the current and local time. To set the time, enter the line number for **Local Time (1)** followed by the new time. The time format is as follows:

HH:MM:SS

where **HH** is the hour to be set based on a 24 hour (military) clock, **MM** is the minutes to be set, and **SS** is the seconds to be set. For example, if you wanted to set the time to 3:15 p.m., you would enter:

1=15:15:00

2) Local date

The current and local date. To set the date, enter the line number for **Local Date (2)** followed by the new date. The date format is as follows:

MM/DD/YY

where **MM** is the month to be set, **DD** is the day to be set, and **YY** is the last two digits of the year to be set. Remember to include a slash (/) between the month and the day and between the day and the year. For example, if you wanted to set the date to January 15, 2001, you would enter:

2=01/15/01

3) Timezone

This parameter specifies the time zone for the switch and sets the system clock to run on UTC time (or Greenwich Mean Time). Additionally, if Daylight Savings Time is enabled (see option 4 below), the clock automatically sets up default DST parameters (if applicable) for the local time zone. The local time remains active for all User Interface commands and other subsystems that require the local time. To set the time zone for the switch, you may use one of two methods:

- a. Enter the line number for **Timezone (3)** followed by the hour(s) offset from UTC. This can be a number from -13 to +12. The number you enter will set the system clock x hours from the local time. For example, if the local time, 1:45:00, is seven hours behind UTC time, you would enter:

3=-7

This specification sets the UTC time to 8:45:00, seven hours ahead of the local time, 1:45:00.

- b. Enter the line number for **Timezone (3)** followed by the time zone name. There is a limited number of time zone names available. For example, if the local time zone name is Mountain Standard Time (MST), you would enter:

3=MST

This specification automatically sets the switch to -7 hours, the number of hours MST is offset from UTC.

Daylight Savings Time. The software will automatically configure DST values for a specified time zone. However, the user can manually modify DST values.

Non-integer Offsets. Non-integer offsets are acceptable for **Timezone**. Some parts of the world are offset from UTC by increments of 15, 30, or 45 minutes. India, for example, is offset from UTC by 5 hours and 30 minutes. If you wanted to enter the time zone offset for India, for example, you would type the line number for Timezone (3), followed by the non-integer hour offset in the **HH:MM** format, as follows:

3=05:30

where the value of **05:30** is five hours and thirty minutes offset from UTC.

◆ Note ◆

The switch automatically enables UTC. However, if you do not want your system clock to run on UTC, simply enter the offset **+0** for the **Timezone** parameter. This sets UTC to run on local time.

The table on the following page lists the options available for **Timezone** names:

Timezone and DST Parameters

Abbr.	Name	Hours from UTC	DST Start	DST End	DST Change
NZST	New Zealand	+12:00	1st Sunday in Oct. at 2:00 a.m.	3rd Sunday in March at 3:00 a.m.	1:00
ZP11	No standard name	+11:00	No default	No default	No default
AEST	Australia East	+10:00	Last Sunday in Oct. at 2:00 a.m.	Last Sunday in March at 3:00 a.m.	1:00
GST	Guam	+10:00	No default	No default	No default
ACST	Australia Central Time	+9:30	Last Sunday in Oct. at 2:00 a.m.	Last Sunday in March at 3:00 a.m.	1:00
JST	Japan	+9:00	No default	No default	No default
KST	Korea	+9:00	No default	No default	No default
AWST	Australia West Time	+8:00	No default	No default	No default
ZP8	China, Manila, Philippines	+8:00	No default	No default	No default
ZP7	Bangkok	+7:00	No default	No default	No default
ZP6	No standard name	+6:00	No default	No default	No default
ZP5	No standard name	+5:00	No default	No default	No default
ZP4	No standard name	+4:00	No default	No default	No default
MSK	Moscow	+3:00	Last Sunday in March at 2:00 a.m.	Last Sunday in Oct. at 3:00 a.m.	1:00
EET	Eastern Europe	+2:00	Last Sunday in March at 2:00 a.m.	Last Sunday in Oct. at 3:00 a.m.	1:00
CET	Central Europe	+1:00	Last Sunday in March at 2:00 a.m.	Last Sunday in Oct. at 3:00 a.m.	1:00
MET	Middle European Time	+1:00	Last Sunday in March at 2:00 a.m.	Last Sunday in Oct. at 3:00 a.m.	1:00
BST	British Standard Time	+0:00	Last Sunday in March at 1:00 a.m.	Last Sunday in Oct. at 3:00 a.m.	1:00
WET	Western Europe	+0:00	Last Sunday in March at 1:00 a.m.	Last Sunday in Oct. at 3:00 a.m.	1:00

Timezone and DST Parameters Con't

Abbr.	Name	Hours from UTC	DST Start	DST End	DST Change
GMT	Greenwich Mean Time	+0:00	No default	No default	No default
WAT	West Africa	-1:00	No default	No default	No default
ZM2	No standard name	-2:00	No default	No default	No default
ZM3	No standard name	-3:00	No default	No default	No default
NST	Newfoundland	-3:30	1st Sunday in April at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
AST	Atlantic Standard Time	-4:00	1st Sunday in April at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
EST	Eastern Standard Time	-5:00	1st Sunday in April at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
CST	Central Standard Time	-6:00	1st Sunday in April at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
MST	Mountain Standard Time	-7:00	1st Sunday in April at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
PST	Pacific Standard Time	-8:00	1st Sunday in April at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
AKST	Alaska	-9:00	1st Sunday in April at 2:00 a.m.	Last Sunday in Oct. at 2:00 a.m.	1:00
HST	Hawaii	-10:00	No default	No default	No default
ZM11	No standard name	-11:00	No default	No default	No default

4) Daylight Savings Time active

Enables and disables DST (Daylight Savings Time). To enable DST, enter:

4=Enable

To disable DST, enter:

4=Disable

If DST is disabled, options 41-49 will not be displayed.

41) DST Start Month

Indicates which month of the year DST starts. To set the month when DST should start, enter the sequential number of the month (January=1, February=2, . . . December=12). For example, if you want DST to begin in April, you would enter the line number for **DST Start Month (41)** and the month, as follows:

41=4

42) DST Start Week

Indicates which week in a month DST starts. To set the week DST should start, enter the sequential number of the week. The possible values are 1st (1), 2nd (2), 3rd (3), 4th (4), and Last. For example, if you want DST to start on the 3rd Tuesday of a month, you would enter the line number for **DST Start Week (42)** and the week, as follows:

42=3

43) DST Start Day

Indicates which day of the week DST starts. To set the day DST should start, enter the sequential number of the day (Sunday=1, Monday=2, . . . Saturday=7). For example, if you want DST to begin on Friday, you would enter the line number for **DST Start Day (43)** and the day, as follows:

43=6

44) DST Start Time

Indicates what time of day (in local time) DST starts. To set the time DST should start, enter the time in the form **HH:MM**, where **HH** is the clock hours of a 24 hour (military) clock and **MM** is the clock minutes that DST should start. For example, if you want DST to start at 1:00 a.m., you would enter the line number for **DST Start Time (44)** and the time, as follows:

44=1:00

45) DST End Month

Indicates which month of the year DST ends. To set the month DST should end, enter the sequential number of the month (January=1, February=2, . . . December=12). For example, if you want DST to end in April, you would enter the line number for **DST End Month (45)** and the month, as follows:

45=4

46) DST End Week

Indicates which week in a month DST ends. To set the week DST should end, enter the sequential number of the week. The possible values are 1st (1), 2nd (2), 3rd (3), 4th (4), and Last. For example, if you want DST to end on the last Tuesday of a month, you would enter the line number for **DST End Week (46)** and the week, as follows:

46=Last

47) DST End Day

Indicates which day of the week DST ends. To set the day DST should end, enter the sequential number of the day (Sunday=1, Monday=2, . . . Saturday=7). For example, if you want DST to end on Wednesday, you would enter the line number for **DST End Day (47)** and the day, as follows:

47=4

48) DST End Time

Indicates what time of day (in local time) DST ends. To set the time DST should end, enter the time in the form of **HH:MM**, where **HH** is the clock hours of a 24 hour (military) clock and **MM** is the clock minutes that DST should end. For example, if you want DST to end at 2:00 a.m., you would enter the line number for **DST End Time (48)** and the time, as follows:

48=2:00

49) DST Offset

Indicates the amount of time to change the local time when DST changes. To set how much time DST should change, enter the change in the form of **HH:MM**, where **HH** is the clock hours and **MM** is the clock minutes that DST should change. For example, if you want the local time to move 1 hour when **DST** changes, you would enter the line number for **DST Offset** and the hour, as follows:

49=1:00

Viewing Slot Data

You can view slot table information by entering the **slot** command. To view information on a particular slot, enter the **slot** command together with the slot number. For example, to view information for slot 1, enter

```
slot 1
```

at the system prompt. You can also view information on all slots in the switch at the same time in a table. To view data, for all slots in the switch, enter

```
slot
```

at the system prompt. A table similar to the following will be displayed.

Slot	Module-Type Part-Number	Adm-Status Oper-Status	HW Rev	Board Serial #	Mfg Date	Firmware-Version Base-MAC-Address
1*	MPM	Enabled	L3	52601675	01/05/01	4.305002600 Operational 00:20:da:04:21:f0
2	HSM	Enabled	B11	53404264	01/19/01	4.3 05003106 Operational 00:20:da:02:28:60
2-1	FDDI		D	53404104	01/24/01	05003706
3	HSM Enabled	Enabled	L	53404645	01/21/01	4.3 05003106 Operational 00:20:da:04:87:30
3-1	ATM		B	53404116	01/11/01	05004400
4	Ether/8	Enabled	D	53404229	01/07/01	4.3 05000014 Operational 00:20:da:03:09:90
5	F-Ether/M	Enabled	A5	73250839	01/07/01	4.3 05015906 Operational 00:20:da:85:40:50

The fields display by the **slot** command are described below.

Slot. The slot number for the MPM or switching module.

Module-Type. The type of module in this slot.

Part-Number. The factory-assigned part number.

Adm-Status. The administration status. This can be enabled or disabled by the operator through the **reset** command, which is described in Chapter 58, "Running Hardware Diagnostics."

Oper-Status. The operational status. Whether the port is Up (Operational), Down, or Unknown. (Unknown means uninitialized or that the module is in a transitional state.)

HW Rev. The revision number for this module. This number may be helpful when troubleshooting.

Board Serial #. Serial number for this module.

Mfg Date. The manufacturing date for this module.

Firmware-Version. The version of the module's firmware. All modules should use the same version of software.

Base-MAC-Address. The base MAC address(es) of this module.

Viewing System Statistics

The **systat** command displays statistics related to system, power, and environment. To view these parameters, enter

```
systat
```

at the system prompt. A screen similar to the following will be displayed.

```

System Uptime                1 days, 12:09:22.64
MPM Transmit Overruns       : 0
MPM Receive Overruns       : 22
MPM total memory            : 16 MB
MPM free memory             : 6522536 bytes
MPM CPU Utilization ( 5 sec) : 5% ( 0% intr 0% kernel 3% task 95% idle)
MPM CPU Utilization ( 60 sec) : 5% ( 0% intr 0% kernel 3% task 96% idle)
Power Supply 1 State        : OK
Power Supply 2 State        : Not Present
Temperature Sensor          : OK - Under Threshold

Temperature                  : 37:00c 98.60f
Temperature Alarm Masking    : Disabled

```

The fields displayed by the **systat** command are described below.

System Uptime. The time since the last boot that the system has been running, displayed in days, hours, minutes, and seconds (to the nearest hundredth).

MPM Transmit Overruns. The number of times a VSE transmit buffer could not be allocated by a task on the MPM.

MPM Receive Overruns. The number of times packets were dropped because the bus had more packets to deliver than the MPM could handle. This is a “receive overrun” condition which can happen when a storm occurs or when the switch is first powered up and many unknown MAC frames are being forwarded to the MPM.

MPM total memory. The amount of total memory installed on the MPM.

MPM Free Memory. The amount of free, or unused, memory available in the MPM. This data is also displayed by the **memstat** command, which is described in *Viewing MPM Memory Statistics* on page 13-20.

MPM CPU Utilization (5 seconds). The amount of time, by percent, the MPM processor actually worked during the last 5 seconds.

MPM CPU Utilization (60 sec). The amount of time, by percent, that the MPM processor actually did work during the last minute.

Power Supply 1 State. Valid states are **OK**, **Not Present**, and **Bad**. A power supply that has been turned off will be in the **Bad** state. If not installed, it will be in the **Not Present** state.

Power Supply 2 State. Valid states are **OK**, **Not Present**, and **Bad**. A power supply that has been turned off will be in the **Bad** state. If not installed, it will be in the **Not Present** state.

Temperature Sensor. Indicates whether the MPM temperature sensor detects overheating. Valid states are **Under Threshold**, **Over Threshold**, and **Not Present**.

Temperature. Indicates the switch temperature Celsius and Fahrenheit.

Temperature Alarm Masking. Indicates whether temperature alarm masking is Enabled or Disabled. You enable masking through the **maskta** command, which is described in Chapter 58, “Running Hardware Diagnostics.”

Clearing System Statistics

You may want to clear statistics for a specific module, port or service for dialogistic or accounting purposes. To clear switch statistics enter

clearstat

at the system prompt. A screen similar to the following will display.

Usage: clearstat slot [,port] [,service] [,instance]

As indicated in the prompt, you can clear all statistics from a module by entering the slot number as shown here:

clearstat 3

This entry will clear all statistics for the module located in slot 3. If you want to clear statistics for a specific port, service or instance, enter the **clearstat** command followed by the appropriate numbers. You must use a comma (,) to separate the slot number from the port, service and instance numbers. The following command will clear all statistics for port 1 of the module located in slot 3.

clearstat 3,1

◆ Caution◆

When the **clearstat** command is used, no notification is sent to the SNMP manager about the cleared statistics. Use of this command can cause unpredictable results with your NMS statistics.

Viewing Task Utilization Statistics

The **taskstat** command displays the task utilization statistics of the switch. To display the task utilization statistics, enter

```
taskstat <task-number> <sample-period>
```

at the system prompt. The **<task-number>** is an optional number of tasks and the **<sample-period>** is an optional sample period of 1 to 60 seconds. You must enter the **<task-number>** if you want to enter the **<sample-period>**.

The default number for **<task-number>** is 5 and the default sample period for **<sample-period>** is 5 seconds. To display the task utilizations statistics for 10 tasks over a 20-second period, for example, enter

```
taskstat 10 20
```

at the system prompt. A screen similar to the following will display.

Task Name	Utilization (20 secs)
tUi_shellt0	0.76%
tCMProber	0.70%
tUi_shellC	0.60%
tSnmp_agent	0.34%
tNetTask	0.32%
tTelnetOut0	0.19%
tif_vblInput	0.19%
vseReceive	0.11%
tTelnetIn0	0.08%
bslMgr	0.07%
All Other Tasks:	0.68%
Total Task Utilization:	4.04%

The **taskstat** command displays the tasks in descending order in terms of the switch's CPU utilization. You may use the **taskstat 0** command if you want to list utilization statistics for all the tasks executed by the switch.

The **taskshow** command displays a table listing all tasks and their priority, status and memory allocation. A partial table is shown here.

NAME	ENTRY	TID	PRI	STATUS	PC	SP	ERRNO	DELAY
tExcTask	_excTask	499f7f20	0	PEND	4892067c	499f7d38	9	0
tLogTask	_logTask	499f5598	0	PEND	4892067c	499f53b0	0	0
tCMWatcher	_cmWatchdogK	4999f108	0	DELAY	4893c028	4999efb8	0	5
tHelperTask	_exc2Task	499fc018	2	PEND	4892067c	499fbc30	0	0
tAscSTimer	_ascSessTime	49a53498	10	DELAY	4893c028	49a53348	0	170
bpeMgr	_bpm_initial	46037630	20	PEND	4892a41c	46037430	3d0002	0
ipxTimer	_ipxTimerTas	49a83168	49	DELAY	4893c028	49a83010	0	26
ipxGapper	_ipxGapperTa	49a7cdc0	49	PEND	4892067c	49a7cb70	0	0
tNetTask	_netTask	499eee40	50	PEND	4892a0a4	499eec68	0	0
ipx	_ipxMain	49fe0350	50	PEND	4892a41c	49fe0168	3d0002	0

The fields displayed by the **taskshow** command are described below.

NAME. Name of the task whose statistics are being shown.

ENTRY. Shows the routines that are currently being executed by the specified task.

TID. Address of the task listed in this row.

Viewing Task Utilization Statistics

PRI. Priority of the specified task.

STATUS. Current status of the specified task.

PC. Program Counter. The program counter identifies the routing code as it enters the stack.

SP. Stack pointer. The stack pointer points to the code being loaded when the status is taken.

ERRNO. Error number indicator.

DELAY. The time elapsed between task routines.

Viewing Memory Utilization

The leak monitor diagnostic utility is used to display information about memory utilization. This utility requires the use of three UI commands: **leakstart**, **leakstop** and **leakdumpall**.

◆ Note◆

You may want to log this operation to a text file to make it easier to view the data.

To start the utility, enter

```
leakstart
```

at the system prompt. This command starts a leak monitor daemon that gathers memory information in the background until you stop it by using the **leakstop** command. The **leakstop** command stops the leak monitor daemon from recording data and preserves the data already recorded. To view the memory utilization information enter the following command

```
leakdumpall
```

at the system prompt. This command dumps all memory recorded by the leak daemon. A screen similar to the following will display.

```

Outstanding Memory - at TUE  APR  24  19:00:29  2001

Task ID   Name   Functi 1  Functi 2   Functi 3   Address  Len   Time
=====  =====  =====  =====  =====  =====  ==  =====
49a69a58  tUi_she 484fe4do 484f1284 484ffbc8 4800ef28  9 TUE APR 24 18:06:4 7 2001
49559bb8  t_AtMg 49db6e90 49d6a780 49d4c3bd 4800ef88 16 TUE APR 24 18:06:4 6 2001
49559bb8  t_AtMg 49db6e90 49d4be4c 49d8639c 4800efb8 64 TUE APR 24 18:06:4 6 2001
49559bb8  tUi_she 49db6e90 49d9cce4 49d9c910 4800f050  4 TUE APR 24 18:06:4 6 2001

```

End of memory report.

The length of the display shown will vary depending on the length of time between use of the **leakmon** command and the **leakstop** command. The fields displayed by the **leakdumpall** command are described below.

Task ID. The address of the task that is allocating the block of memory.

Name. Name of the task that is allocating the block of memory.

Functi 1, 2, 3. These three columns indicate functions entered above the *malloc* package. Function 1 is the function that called *malloc*. Function 2 is the function that called Function 1. Function 3 is the function that called Function 2.

Address. The starting address space for the memory that was allocated.

Length. The length of the block requested on the *alloc()* call

Time. The timestamp taken when the *alloc* call occurred.

Viewing MPM Memory Statistics

The **memstat** command displays the MPM's memory statistics. The statistics will tell you how memory is currently being used and help determine if memory problems exist, such as memory exhaustion. To view the MPM's memory statistics, enter

memstat

at the system prompt. A screen similar to the following will be displayed.

Summary of Memory Usage

<u>status</u>	<u>bytes</u>	<u>blocks</u>	<u>avg block</u>	<u>max block</u>
current				
free	4761672	64	74401	4719704
alloc	6429088	9114	705	-
cumulative				
alloc	24942880	148235	168	-
MPM total memory			: 16MB	

The fields displayed by the **memstat** command are described below.

status. The statistics appear in two groups: **current** and **cumulative**. The current status shows free and allocated memory. The cumulative status shows only allocated memory. Cumulative memory is the total amount of memory that has been allocated since the switch was started up. This value increases each time a memory allocation takes place. It can never decrease.

bytes. The number of bytes for free and allocated memory.

blocks. Block size is dynamic and depends upon memory usage and the amount of fragmentation.

avg block. The average block indicates the average size of all the memory blocks.

max block. The maximum block indicates the largest free memory block available. When this value drops to around 10K it usually indicates that the free memory is highly fragmented and probably near exhaustion.

MPM total memory. The total number of megabytes available in the MPM's memory.

Checking the Flash File System

The **fsck** command performs a file system check of flash memory, which consists of the flash file system. Image files are stored in flash memory and loaded into system memory when the switch boots up. It also provides diagnostics in the case of file corruption. To perform a file system check of flash memory, enter

```
fsck
```

at the system prompt. A screen similar to the following will be displayed.

```
Your bootroms support Flash File System Version 2 and greater.
```

```
Out of 16 file descriptors in use, 0 of these are opened on the /flash device.
```

```
Performing a file system check using manual mode. If a file is encountered  
with a potential problem, you may wish to consider preserving it for technical  
support analysis...
```

```
Flash file system check in progress...
```

```
Checking root file system... OK
```

```
Performing file consistency check...
```

```
Done.
```

```
There doesn't appear to be a system problem related to the Flash File  
system or kernel file system data structures. If you are experiencing  
problems with the flash file system, perhaps try using the "info",  
"systat", or "memstat" commands. They may indicate some other condition  
(such as low memory) which could prohibit correct operation of the  
file system.
```

If the **fsck** command finds a problem with the flash file system, a message will be displayed detailing the problems found and/or actions taken to correct those problems.

Checking the SIMM Files

Each logical file system (**/flash** and **/simm**) must be checked independently. If you have installed the 32 or 56 Mb SIMM upgrade and you want to check the SIMM's memory, enter

```
cd /simm
```

at the system prompt before you execute the **fsck** command.

Creating a New File System

The **newfs** command removes a complete flash file system and all files within it. It then creates a new flash file system, which is empty. You can use this command when you want to reload all files in the file system from a readily-accessible backup device or in the unlikely event that the flash file system becomes corrupted.

◆ Important Note◆

Before you execute the **newfs** command you should preserve your configuration file by saving it to another host.

To re-initialize the flash memory, enter

```
newfs
```

at the system prompt. The following screen will display.

```
You are about to destroy all files on file system /flash. If you  
are experiencing problems with the flash file system, you might  
want to use the "fsck" command to help determine where problems  
may exist.
```

```
Are you absolutely sure you want to strip the current file  
system and create a new one? (n)
```

Enter **y** to re-initialize the flash memory or **n** to cancel (the default is **n**). If you enter **y**, you will have to load new software into the switch.

◆ Warning ◆

Do not power-down the switch after running the **newfs** command until you reload your image and configuration files. If you do, you will have to reload the image files at the boot monitor prompt using the serial interface (e.g., ZMODEM), which can take several minutes.

You can then download new files via FTP or ZMODEM.

Creating a SIMM File System

If you have installed the 32 or 56 Mb SIMM upgrade and you want to create a new file system in the SIMM's memory, enter

```
cd /simm
```

at the system prompt before you execute the **newfs** command.

Configuring System Information

You can enter or modify a description of a switch, its location, and a contact person. Although this information is not required, you may find it helpful in managing the switch. To enter or modify the switch descriptions, perform the following steps.

1. At the system prompt, enter

```
syscfg
```

The current system information will appear with a prompt asking if you want to change any of the information; for example:

```
System Contact           : Usenet
System Name             : Testnet4
System Location         : Calabasas
System Description     : Marketing_testnet
Duplicate MAC Aging Timer : 0 (not configured)
Change any of the above {Y/N}? (N) :
```

If you enter **n**, the **syscfg** command will exit and no changes will be made (the default is **n**). If you enter **y**, the current system information will be displayed line by line. To keep the current value (shown in brackets) for a line, press **<Enter>**. To change a value, enter the new value and press **<Enter>**.

◆ Important Note ◆

Except for the **Duplicate MAC Aging Timer** field, all changes you make take place immediately.

If you entered **y**, something similar to the following will be displayed.

```
System Contact (Usenet) :
```

2. Enter the new system contact or just press **<Enter>** to accept the default. A screen similar to the following will be displayed.

```
System Name (no_name) :
```

3. Enter the new system name or just press **<Enter>** to accept the default. A screen similar to the following will be displayed.

```
System Location (Unset) :
```

4. Enter the new system location or just press **<Enter>** to accept the default. A screen similar to the following will be displayed.

```
System Description (DESCRIPTION NOT SET.) :
```

5. Enter the new system description or just press **<Enter>** to accept the default. A screen similar to the following will be displayed.

```
Duplicate Mac Aging Timer :
```

The **Duplicate MAC Aging Timer** indicates the time, in seconds, duplicate MACs remain in CAM if there is no traffic from those MACs. After this time, inactive MACs will age out of the CAM. You must reset the switch before this parameter takes effect. Duplicate MAC addresses will display as normal MAC addresses in other software commands, such as **fw** and **macinfo**. See *Duplicate MAC Address Support* on page 13-30 for further discussion.

6. Enter a new duplicate MAC aging timer value (the valid range is from 10 to 1000000) or just press **<Enter>** to accept the default.

Viewing CAM Information

The **camstat** command displays information and usage about the content addressable memory (CAM) on each switching module in the chassis. To view this CAM information, enter

```
camstat
```

at the system prompt. Something similar to the following will be displayed.

Slot	# of CAMs	Cfg Usage	Max Avail	Actual Usage
MPM	1	NA	NA	NA
2	4 (2 + 2)	0	3966	0
3	1 (1 + 0)	0	1008	0
4	1 (1 + 0)	0	1004	0
5	4 (2 + 2)	0	4093	0

The fields displayed by the **camstat** command are described below.

Slot. The slot number of the switching module for which CAM information is provided.

of CAMs. The number of CAM chips installed on the switching module.

Cfg Usage. The number of CAM entries this module is configured to support. By default a module will use the maximum amount of entries supported by on-board CAM. However, you can alter this default through the **camcfg** command (described in *Configuring CAM Distribution* on page 13-25) to make the most efficient use of the CAM distributed among all switching modules in the chassis. Up to 16K of CAM is supported over all modules in an OmniSwitch.

Max Avail. The number of CAM entries available. This number will be less than the number of CAM entries configured because some entries will be used by learned MAC addresses (shown in the **Actual Usage** column) and others are used internally by the OmniSwitch.

Actual Usage. The number of MAC addresses learned by the module in this slot.

◆ Note ◆

For CAM statistics for an entire chassis, use the **hdstat** command, which is described in Chapter 15, "Health Statistics."

Configuring CAM Distribution

CAM (Content Addressable Memory) on switching modules is used to look up the MAC address of endstations attached to the modules. The OmniSwitch and the OmniSwitch/Router each support a different amount of allowable CAM space (for more information on CAM distribution, see *OmniSwitch CAM Distribution* and *Omni Switch/Router CAM Distribution* below). You can use the **camstat** command to display each module's CAM usage. See *Viewing CAM Information* on page 13-24 for more information on the **camstat** command.

OmniSwitch CAM Distribution

The OmniSwitch supports up to 16K of CAM among all switching modules in a chassis. The 16K chassis-wide limitation is due to the size of the master Bridge Filter Table (BFT) managed by the MPM. For each entry in a module's CAM, there is a corresponding entry in the BFT.

When each switching module in a 9-slot chassis has 1K or 2K of CAM, the 16K limitation is not reached since only 8K or 16K (assuming 8 switching modules) is used. However, when some switching modules use 4K of CAM the 16K limitation could be reached quickly. If you exceed the limit of usable CAM memory among all the switching modules in a chassis, some switching modules will not come up.

For example, if six switching modules in a 9-slot chassis contained 2K CAMs and the remaining two modules contained 4K CAMs, then 20K of CAM would reside in the entire chassis. In this situation, some switching modules will not come up.

The **camcfg** command allows you to individually allocate CAM space to switching modules. This command configures the maximum entries a switching module may use, freeing up overall CAM space in the chassis so that some modules can use more of their on-board CAM. Follow these two additional rules:

- The CAM memory size for a switching module must be configured to at least one-half of the total memory available on the switching module. For example, if your switching module has 2 K of CAM memory, you must allocate at least 1 K of CAM to that switching module.
- The amount of CAM memory allocated for a switching module must be a whole-number multiple of 1024 (e.g., 1024, 2048, etc.).

Follow these steps to configure the number of CAM entries used by a switching module:

1. Enter **camcfg** followed by the slot number for the module that you want to configure. You can configure the CAM on switching modules only, not on the MPM. For example, to configure CAM for the module in slot 3, enter

```
camcfg 3
```

2. The system displays a prompt asking for the number of CAM entries to use for this module.

Enter maximum number of CAM entries for slot 3 (1024):

Enter the number of CAM entries to use for this module. The current value is listed in parentheses. The value you enter must be equal to or less than the total number of entries available on board this module. For example, you could not configure 2048 entries for a switching module with only 1K of CAM.

A message similar to the following will display:

**Slot 3 Configured to learn 256 MACs will round up to 256 MACs
This configuration will take effect only after system reboot**

3. The new CAM configuration will take effect after you reboot the system. For this reason, you may want to configure the CAM for all modules in this system. Reboot the system and check the updated CAM configurations through the **camstat** command.

Omni Switch/Router CAM Distribution

The Omni Switch/Router supports approximately 31.25 K of usable CAM among all the switching modules in a chassis. (A small amount of CAM memory is reserved by the Omni Switch/Router for its processing.)

If any of the switching modules in a 9-slot chassis have 1 K CAMs (e.g., ESX-100C-32W, TSX-C-32W), you will not reach the 31.25 K limit. However, if *all* the switching modules in a fully-loaded 9-slot chassis have 4 K CAMs you would exceed the 31.25 K limit. In this configuration, the Omni Switch/Router would subtract 256 K of available CAM memory from the first switching module to initialize and 512 K of available CAM memory from the last switching module to initialize. Generally, there is not need to configure CAM space on the Omni Switch/Router. However, if you need to configure CAM usage on an Omni Switch/Router, see *OmniSwitch CAM Distribution* on page 13-25 for information on using the **camcfg** command.

◆ Important Note ◆

If you use a configuration file (e.g., **mpm.cfg**) from an OmniSwitch on an Omni Switch/Router, any CAM configuration settings will be ignored.

Configuring the HRE-X/HRE-VX Router Port

Various services in the switch use the HRE-X/HRE-VX router port MAC registers. The registers are allocated as the services are loaded at startup. The **hrex** submenu contains five commands for use with the Hardware Routing Engines (HREs). The **hrexassign** command allows you to configure the switch so that registers are reserved for particular services. The **hrexdisplay** command allows you to view your current configuration. To display the **hrex** submenu, enter

hrex

at the system prompt. A screen similar to the following is displayed.

Command	HRE-X Management Menu
hrexassign	Assign an HRE-X router port MAC register to a service
hrexdisplay	Display HRE-X router port MAC register assignments
hrexutil	Display HRE-X Pseudo CAM and cache utilization
hrexhashopt	Optimize HRE-X Pseudo CAM hash function for current data
hrexhashdflt	Restore default HRE-X Pseudo CAM hash function

◆ Important Note ◆

The **hrex** submenu commands are only supported on Omni Switch/Routers or on OmniSwitches with an MPM-III. They are not supported on OmniSwitches with an MPM-1G or MPM-C. To view a list of modules in your switch, use the **slot** command.

To view the current HRE-X configuration enter

hrexdisplay

at the system prompt. A screen similar to the following is displayed.

Reg	Configured	Actual
1	Any	Routing
2	Any	Unused
3	Any	Unused

The fields displayed by the **hrexdisplay** command are described below:

Reg. The number of the MAC registers.

Configured. The service type assigned to the register.

Actual. The service that is actively using the register.

Configuring the HRE-X/HRE-VX Router Port

To reserve a register for a particular service, you can assign the registers to the service. To assign the registers on the HRE-X/HRE-VX router port, enter

```
hrexassign
```

at the system prompt. A screen similar to the following is displayed.

```
hrexassign <register number> <service type>
```

The **<register number>** is either 1, 2 or 3 referring to the MAC register. The **<service type>** parameter specifies the service configured to the registers. The service types are shown on the screen display are defined here.

any. This register is not reserved to a particular service.

routing. This register is assigned to standard routing.

cip. This register is assigned to Classical IP

m013. This register is assigned to Channelized DS-3 module (WSX-M013).

mpoa. This register is assigned to Multiprotocol Over ATM

vrrp. This register is assigned to Virtual Router Redundancy Protocol.

For example, to assign register 3 to the Classical IP service enter

```
hrexassign 3 cip
```

at the system prompt. A screen similar to the following is displayed.

```
HRE-X RPM 3 configured for "CIP"; reboot to make effective.
```

As indicated on the screen, the register assignment will not take effect until the switch is rebooted. If you use the **hrexdisplay** command after making a the register assignment shown in the above example, a screen similar to the following is displayed.

Reg	Configured	Actual
1	Any	Routing
2	Any	Unused
3	CIP	Routing

Configuration changed since last reboot.

This indicates that register 3 is assigned to the CIP service but is actually using the Routing service. Also, the message at the bottom of the table indicates that the HRE-X configuration has changed since the last reboot of the switch. After a reboot, the **hrexdisplay** command will display the following screen.

Reg	Configured	Actual
1	Any	Routing
2	Any	Unused
3	Routing	Routing

Configuring and Displaying the HRE-X/HRE-VX Hash Table

The HRE-Xs and HRE-VXs use a hardware implemented hash table to route packets for transmission. The switch employs a default hash function that works well in a broad range of data environments. In rare cases, you may want to change the hash table configuration to optimize it for your particular data flow. This should be done with care because the data population will change over time. A hash function that works well for one set of data may not work as well for another. Also, note that optimizing the hash function will cause all of the current entries in the HRE-X to be cleared and then relearned; therefore, this should be done with extreme caution.

Two HRE-X/HRE-VX commands are used to optimize the hash function. They are the **hrexutil** and the **hrexhashopt** commands. The **hrexutil** command displays the current utilization of the hash table. To view the HRE-X Utilization table, enter

```
hrexutil
```

at the system prompt. A screen similar to the following is displayed.

```
HRE-X Utilization
-----
Hash           - Total:    65536    Free:    65528
Collisions    - Total:    131072   Free:    131069
Cache         - Total:    40960    Free:    40949
Collision Length - Max:      3        Avg:     1
```

The fields displayed by the **hrexutil** command are described below:

Hash. The number of entries in the hash table.

Total. The total number of units available.

Free. The number of units that are not yet used.

Collisions. The number of entries that have hashed to the same index in the hash table.

Cache. The number of modifications required to route a packet.

Collision Length. The length of the longest (**Max**) collision list and the average length (**Avg**) of the collision lists.

The **hrexhashopt** command causes the switch to compute an optimized hash function based on the data currently in the HRE-X. This function is saved in the configuration file so it will be present after a reboot.

To use the **hrexhashopt** command, enter

```
hrexhashopt
```

at the system prompt. The screen does not display a confirmation message after this command. You can verify optimization by observing the changes in the HRE-X Utilization. After using **hrexhashopt**, the maximum and average collision lengths should be reduced as shown in the HRE-X Utilization table shown above. If they are not, you should consider returning to the default hash function by using the **hrexhashdfit** command.

To use the **hrexhashdfit** command, enter

```
hrexhashdfit
```

at the system prompt. The screen does not display a confirmation message after this command. The **hrexhashdfit** command will return the hash function back to the default value.

Duplicate MAC Address Support

When the switch sees the same MAC address sending traffic on a different switch port (a Duplicate MAC Address), it assumes the original network device moved. The switch sends a trap notifying network management of this station move event. It sends one trap for a device move within the same Group and another trap for a device move outside of the home Group.

A station move trap is normally sent after an actual station move. However, certain network configurations assign the same MAC address to different network devices (physical and virtual) as standard practice. In these situations, the duplicate MAC address appears as a station move when it is really a normal occurrence in these network configurations. These network configurations that use the same MAC address for different devices include:

- LAN Emulation under Cisco routers. Cisco routers use the same MAC address for each LAN Emulation Client (LEC). In LAN Emulation, each ELAN needs to be treated as a separate LAN and should therefore have a separate MAC address.
- IBM Front End Processor (FEP). Many IBM FEPs use the same MAC address assigned to the connecting devices for the purpose of redundancy.
- DECnet networks. The DECnet protocol assigns the special MAC address, AA000400XXYY (XXYY is an internal protocol ID) to each DECnet station or routing device regardless of the number of physical interfaces.

Initially, duplicate MAC addresses in these special situations may be no more of a problem than extra traps being sent for an event (station move) that did not really happen. However, when a large number of these network devices send the same MAC address out the same port, flooding can occur and the switch will eventually shut the port down.

To prevent a port from being shut down, the switch needs some way of knowing the duplicate MAC addresses originating from the port are not an error condition.

The switch will treat duplicate MAC addresses as separate addresses as long as they are learned from a different Group as the original MAC. Each duplicate MAC address will use one entry in the CAM. Up to 32 duplications of the same MAC address are supported. Duplicate MAC addresses learned from virtual ports within the same Group are treated as station moves and will generate corresponding traps. If the MAC address moves from one VLAN to another VLAN within the same Group, the switch will not treat the MAC addresses as separate.

If your network supports duplicate MAC addresses, there may be a significant performance impact due to the following reasons:

- A MAC address is usually stored only in the CAM of the switching module where its destination address is located. If duplicate MAC addresses are treated as separate addresses, then the same MAC address may have to be stored in the CAM of multiple switching modules, not just the module that originally learned the address.
- Every duplicate MAC address becomes a CAM table entry, so there will be less room in the CAM for other entries to be learned. Since up to 32 duplications of a single MAC address are possible, this CAM can become crowded with these duplicate entries.

You can reduce the impact of a crowded CAM by configuring the **Duplicate MAC Aging Timer** in the **syscfg** command, which is described in *Configuring System Information* on page 13-23. This timer allows you to age out Duplicate MAC CAM entries from devices that are inactive for the time period you specify.

- Extra search time will be required for each lookup of the same MAC address since it is treated as a separate entry in the CAM.

In addition to these performance impacts, you will lose the tracking of legitimate station moves. No traps will be sent for Duplicate MAC addresses that appear in different Groups.

Multicast Claiming

Multicast claiming can be enabled for networks with heavy multicast traffic. When enabled, multicast claiming frees the MPM from processing multicast packets by off-loading this traffic to the switching modules. When multicast claiming is enabled, the switch “claims” destination multicast addresses and places them in the CAMs of all switching modules in the switch.

You can enable multicast claiming by adding the following line to the **mpm.cmd** file:

```
bsiLearnMcPkt=1
```

You can use the **edit** command to make this change. (See Chapter 11, “Managing Files,” for instructions on using the **edit** command.) You will need to reboot the switch for this parameter to take effect. Multicast claiming can later be disabled by changing the setting for this parameter to zero (0), as follows:

```
bsiLearnMcPkt=0
```

An alternative method for managing multicast traffic is through the use of Multicast VLANs. See Chapter 27, “Managing AutoTracker” and Chapter 28, “Managing Multicast VLANs” for further information.

Disabling Flood Limits

Two UI commands are available for controlling flood limits for individual ports and Groups. The **modvp** command (described in Chapter 24, “Managing Groups and Ports”) allows you to control the flood limits for a specific port. The **flc** command (described in Chapter 22, “Configuring Bridging Parameters”) allows you to configure flood limits for all ports in a group.

You can also disable flood limits on a switch-wide basis by adding the following line to the **mpm.cmd** file:

```
disableFloodLimiting=1
```

You can use the **edit** command to make this change. See Chapter 11, “Managing Files,” for instructions on using the **edit** command. You will need to reboot the switch for this parameter to take effect.

Saving Configurations

Under normal conditions, configurations you make using the UI are written into cache and automatically saved into the switch's flash memory. In this case, it is not necessary to issue a special command to save your configurations. When you use the UI to enter multiple configurations, periodically the switch will display the following message.

File system compaction in progress . . .

This message indicates that the switch is compacting data in the cache buffer before writing it into the mpm.cnf file. This message normally disappears after a few seconds.

◆ Warning ◆

It is highly recommended that you use the default setting and allow the switch's save function to operate automatically.

You can change the switch's save function so that the cache is not saved automatically by executing the **cacheconfig** command. To turn off the switch's automatic save function, enter

cacheconfig on

at the system prompt. The following message will display.

Cache Configuration is now on

◆ Warning ◆

Any configurations you enter before executing the **saveconfig** command will not be saved in case of system failure or reboot.

Once **cacheconfig** is implemented, you must use the **saveconfig** command to manually synchronize your configurations into flash memory. When you execute the **saveconfig** command at the system prompt, the following message will display.

File system compaction in progress . . .

The UI does not indicate when the **cacheconfig** function is in operation. However, if you attempt a reboot the following message will display if you are in the cache configuration mode.

**!!!Warning!!! You are in the cache configuration mode.
Please enter 'n'/'N' to the following confirm prompt.
Then enter the UI command "saveconfig", or
enter the CLI command "dump configuration cache" to
save the current configuration to mpm.cnf in the flash.**

Otherwise, all/some your configuration changes will be lost!

Confirm? (n) :

This message gives you the opportunity to execute the **saveconfig** command prior to the reboot.

Saving Configurations

To determine whether you are in the cache configuration mode, enter the **cacheconfig** command. If cache config is operational the following message will display one of the following messages.

Cache Configuration is currently on.

or

Cache Configuration is currently off.

To turn off the cache configuration mode, enter the following command at the system prompt.

cacheconfig off

The following message will display.

**File system compaction in progress . . .
Cache Configuration is now off**

14 Switch Logging

Logging Overview

Whether you are troubleshooting, configuring, or simply monitoring the switch, you may find it useful to view a history of various switch activities. The Logging submenu contains a list of commands for viewing and configuring logging on the system. To enter the logging submenu, enter

logging

at the system prompt. Enter a question mark (?) and then press **<Enter>** to display the following list of commands:

<u>Command</u>	<u>Logging Menu</u>
syslog	Change the syslog parameters (not part of Switch Logging feature).
swlogc	Configure Switch Logging source/destination mapping and priority levels.
cmdlog	Show UI Command entries in the mpm.log file
conlog	Show Connection entries (logins/logouts) entries in the mpm.log file
caplog	Show Screen Capture entries in the mpm.log file.
debuglog	Show Debug message entries in the mpm.log file
seclog	Display Secure Access log file entries.

Commands in the submenu are described here.

System Log Messages

The **syslog** command is used to configure how system log messages, like diagnostic and error messages, are handled on the switch. See *Configuring the Syslog Parameters* on page 14-2.

Switch Logging Parameters

The **swlogc** and remaining commands in the submenu are part of the Switch Logging feature, which is a separate logging mechanism. The **swlogc** command is used for configuring the logging parameters of various switch activities such as FTP and Telnet, and is described in *Configuring Switch Logging* on page 14-6.

The other commands listed in the submenu above are support commands for Switch Logging.

- **cmdlog** command—displays the UI command entries in the mpm.log file, which is one of the possible destinations for Switch Logging data. See *Displaying the Command History Entries in the MPM Log* on page 14-9.
- **conlog** command—displays the connection entries in the mpm.log file. See *Displaying the Connection Entries in the MPM Log* on page 14-10.
- **caplog** command—displays the screen capture entries in the mpm.log file. See *Displaying Screen (Console) Capture Entries in the MPM Log* on page 14-11.
- **debuglog** command—shows the debug entries in the mpm.log file. See *Displaying Debug Entries in the MPM Log* on page 14-13.
- **seclog** command—shows the Secure Access violation event entries in the mpm.log file. See *Displaying Secure Access Entries in the MPM Log* on page 14-13.

Configuring the Syslog Parameters

Syslog messages are messages generated by individual processes in the switch. These messages contain information for conditions that range from debugging to emergency error conditions.

The **syslog** command allows you to control how these messages will be handled. You can designate what kinds of messages you will see and where the messages will be sent. This syslog implementation is compatible with the standard BSD UNIX implementation for syslog services.

To see the current syslog configuration, enter

```
syslog
```

at the system prompt. A screen similar to the following will be displayed.

```
SYSLOG current configuration:
```

```
1) Log host           - UNDEFINED
2) Log host IP       -
3) Syslog port (514) - 514
4) Default facility code - local0
  41) Override internals - no
5) Default priority mask - emerg
  51) Override internals - no
  52) Display internals - no
6) Console logging   - yes
7) Log Task ID       - yes
  71) Use Task Name   - no
8) Message tag       - switch
```

```
(save/quit/cancel)
```

```
:
```

Select the number of the item you want to change. To change any of the values on the previous page, enter the line number, followed by an equal sign (=), and then the new value. For example, to turn off console logging, enter:

```
6=no
```

The question mark (?) option refreshes the screen. To update the values you have changed, enter **save**. If you do not want to save the changes enter **quit** or **cancel**, or press **Ctrl-D**.

The parameters displayed by the **syslog** command are described below.

Log host

The name of the host where you want the syslog messages sent. The Domain Name Server (DNS) must be configured for this to work. Use the **res** command to configure the DNS. (The **res** command is described in Chapter 18, “RMON and DNS Resolver.”)

Log host IP

The IP address of the host where you want the syslog messages sent. If the IP address and the Log host name disagree, the IP address takes precedence.

Syslog port (514)

The port to which the syslog messages will be sent on the specified host. Port 514 is the normal port number used and is the default.

Default facility code

The facility code is used to identify which sub-system generated the syslog message. Note that this code is used only as a default for tasks that do not have a facility code. See the table below for a list of the facility codes. The default is **local0**.

Syslog Facility Codes

Facility	Source
LOG_KERN	Messages generated by the kernel
LOG_USER	Message generated by random user processes
LOG_MAIL	The mail system
LOG_DAEMON	System daemons
LOG_AUTH	The authorization system
LOG_LPR	The line printer spooling system
LOG_NEWS	Reserved for the USENET system
LOG_UUCP	Reserved for the UUCP system
LOG_CRON	The cron/at facility
LOG_LOCAL0-7	Reserved for local use

Override internals

This setting will force all syslog messages to use the default facility code specified in **Default facility code** instead of their own predefined facility codes.

Default priority mask

The mask for the priority code. Indicates the type of syslog message. Note that this mask is used only as a default for tasks that do not have a priority code. Priority codes for syslog messages are usually hardcoded. The following table is a list of priority codes.

Syslog Priority Codes

Level	Value	Meaning
LOG_EMERG	0	FATAL system event
LOG_ALERT	1	FATAL subsystem event
LOG_CRIT	2	Problem, subsystem unstable
LOG_ERR	3	Problem, bad event, recoverable
LOG_WARNING	4	Unexpected, non-fatal event
LOG_NOTICE	5	normal but significant condition
LOG_INFO	6	info
LOG_DEBUG	7	Internal debug messages

Override internals

This field will force all syslog messages to use the default priority mask specified instead of their own predefined priority masks.

Display internals

This field allows the user to display the task log level. Enter **52=yes** to display the sub-menu below. If, for example, you wanted to change the priority mask **CM via kern** from “warn” to “alert,” you would enter **4=alert**. Note that this change will take place immediately and you do not need to enter **save** for it to take effect. Type **save**, **quit**, or **cancel** and then press **<Enter>** to return to the main **syslog** menu.

Internal task syslog configuration:
(NOTE: changes take effect immediately and are NOT saved across reboots!)

- 0) PPM via kern - alert
- 1) LPM via kern - alert
- 2) VPM via kern - alert
- 3) SNMP via kern - alert
- 4) CM via kern - warn
- 5) ATMmgr via kern - alert
- 6) atmLANE via kern - alert
- 7) Q93bif via kern - alert
- 8) ILMlif via kern - alert
- 9) SSI0 via kern - alert
- 10) atmSNMP via kern - alert

Console logging

Determines whether or not you want to see syslog messages on your console (terminal). If set to yes, the messages will be displayed on either an **ASCII** terminal connected to the console port or via a Telnet session.

Log Task ID

Determines whether or not you want to see the task ID that can be included in the syslog message.

Use Task Name

This allows the user to display descriptive task names for syslog messages (see the **Display internals** sub-menu above) instead of numeric codes.

Message tag

Text of up to 10 characters that is added to every message leaving the switch. It is useful when multiple switches send messages to the same host.

Configuring Switch Logging

Switch logging is a feature that allows you to activate and configure the logging of various types of switch information. Once you activate logging for a specific facility through the switch logging command, you may also decide whether the log output should display on the console, be saved to a file, or be both displayed and saved to a file. To enter the switch logging submenu, enter

swlogc

at the system prompt. A screen similar to the following displays:

CONFIGURATION MENU FOR SWITCH LOGGING

```
1) Security Logging                : Disabled
   11) Output to File              : Yes
   12) Output to Console           : No
2) FTP Logging                    : Disabled
   21) Output to File              : Yes
   22) Output to Console           : No
3) Flash File Logging             : Disabled
   31) Output to Console           : Yes
4) Screen Capture                 : Disabled
   41) Output to File              : Yes
5) Console Event Logging          : Disabled
   51) Output to File              : Yes
   52) Output to Console           : No
6) User Interface Logging         : Disabled
   61) Output to File              : Yes
   62) Output to Console           : No
7) Telnet Logging                 : Disabled
   71) Output to File              : Yes
   72) Output to Console           : No
8) Log File (mpm.log) Size        : 20000 bytes
9) Return Logging to Default Configuration : No
```

Command {Item/ Item=Value/ ?/ Help/ Quit/ Cancel/ Save} (Redraw) :

The logging types are described here:

1) Security Logging

Enabling security logging allows you to view all security violations that occur within the switch. Set to **enable** to activate logging for any security violations that occur within the switch. Set to **disable** to de-activate logging for security violations.

◆ Note ◆

Security Logging must be enabled in order to display the Secure Switch Access violations log (**seclog**).

2) FTP Logging

FTP Session Events is a record of all FTP (File Transfer Protocol) activities since logging was activated. Once you enable FTP Logging by entering **2=enable**, you may view it through the **conlog** command (described in *Displaying the Connection Entries in the MPM Log* on page 14-10). To disable FTP Session Events logging, enter **2=disable**.

3) Flash File Logging

Flash file logging records debug information from the code that manages the switch logging feature itself (previously called “flash file system logging”). To enable flash file logging, enter **3=enable**. To disable flash file logging, enter **3=disable**. Flash file logging messages cannot be saved in the `mpm.log` file, but flash file logging messages may be displayed on the console by entering **31=yes**. To disable sending flash file logging messages to the console, enter **31=no**.

4) Screen Capture

Screen logging captures screen text for logging. To enable screen logging, enter **4=enable**. To disable screen logging, enter **4=disable**. Note that since screen text already goes to the screen, logging output to the screen is not permitted. If you want to display the screen capture entries for all logged users, use the **caplog** command (for more information, see *Displaying Screen (Console) Capture Entries in the MPM Log* on page 14-11).

◆ Note ◆

The screen capture feature has not yet been implemented.

5) Console Event Logging

Console Session Events is a record of all console login activities in the switch, including user names, and connection times. Once you enable Console Event logging by entering **5=enable**, you may view it through the **conlog** command (described in *Displaying the Connection Entries in the MPM Log* on page 14-10). To disable logging for Console Events, enter **5=disable**. Note that logging output to the console is not permitted.

6) User Interface Logging

User Interface Logging is executed on the switch since the UI log was activated. Once you enable UI logging by entering **6=enable**, you may view it through the **cmdlog** command (described in *Displaying the Command History Entries in the MPM Log* on page 14-9). To disable logging for the UI, enter **6=disable**.

7) Telnet Logging

Telnet Logging is a record of all Telnet activities since Telnet logging was activated. Once you enable Telnet logging by entering **7=enable**, you may view it through the **conlog** command (described in *Displaying the Connection Entries in the MPM Log* on page 14-10). To disable logging for Telnet, enter **7=disable**.

8) Log File Size

Use this parameter to set the `mpm.log` file size. The default is 20,000 bytes. The maximum number of bytes is dependent upon the available flash in your system. If you set a file that is too large, the command will tell you the maximum allowed size. (This is half of the remaining free space in your flash file system.) The minimum file size is 3,240 bytes.

9) Return Logging to Default Configuration

Use this parameter to return all of the switch logging options to their default values. Enter **9=yes** to reset the configuration at reboot. To keep the same logging configuration at the next reboot, make sure this parameter is set to **no**.

In addition to enabling or disabling each type of logging, you can also specify whether to output the log to a file or to the console:

Output to File

Set to **yes (y)** to store the log messages in the mpm.log file. Set to **no (n)** to disable sending log messages to this file. (This option is not available for flash file logging or screen capture.)

Output to Console

Set to **yes** to display the log messages on the console screen. Set to **no** to disable the screen as an output device for Security Logging.

Displaying the Command History Entries in the MPM Log

The **cmdlog** command displays a list commands executed since User Interface (UI) facility logging was activated by the **swlogc** command (described in *Configuring Switch Logging* on page 14-6). To display this data, enter

cmdlog

at the system prompt. The following is a sample display.

User	Line	Time	User Input
admin	198.206.187.113	08/14/00 16:42	cmdlog
admin	198.206.187.113	08/14/00 16:42	xlat
admin	198.206.187.113	08/14/00 16:43	conlog
admin	console	08/15/00 10:28	logging
admin	console	08/15/00 10:28	?
admin	198.206.187.113	08/15/00 14:03	taskstat
admin	198.206.187.113	08/15/00 14:05	taskstat

The fields displayed by the **cmdlog** command are described below.

User. The login name of the user who executed the command.

Line. The login type of the user who executed the command. If, for example, the user was connected through the console port, “console” will be displayed. If the user was connected through Telnet, on the other hand, then the IP address of that user will be displayed.

Time. The time that the command was executed.

User Input. The actual text (up to 32 characters) that the user entered at the system prompt.

◆ Note ◆

If you just want to display the commands executed during the current session you can use the **history** command, which is described in Chapter 8, “The User Interface.”

Displaying the Connection Entries in the MPM Log

The **conlog** command displays a list of connections made since console event, FTP, or Telnet logging was activated by the **swlogc** command (described in *Configuring Switch Logging* on page 14-6). To display this data, enter

```
conlog
```

at the system prompt. A screen similar to the following will be displayed.

User	Line	Peer	Start	Finish
-----	-----	-----	-----	-----
admin	Telnet	198.206.187.113	08/14/00 09:47 -	09:47 (00:00)
admin	Telnet	198.206.187.113	08/20/00 09:47 -	09:53 (00:05)
admin	Telnet	198.206.187.113	08/20/00 09:55 -	10:00 (00:05)
admin	console		08/20/00 10:35	logged in (00:27)
admin	Telnet	198.206.187.113	08/20/00 11:02	logged in (00:00)

The fields displayed by the **conlog** command are described below.

User. The name of the user who made the connection to the switch.

Line. The login type of connection to the switch (e.g., a Telnet or console port connection).

Peer. If the user was connected through Telnet, then the IP address of the user will be displayed. If the user was connected through the console port, then this field will be blank.

Start. The time that the connection started.

Finish. Displays the time the connection terminated or **logged in** for sessions that are still current. The value in parenthesis is the duration of the session, in minutes.

Displaying Screen (Console) Capture Entries in the MPM Log

The **caplog** command displays the screen capture entries in the mpm.log file. (*Note: This feature is not yet implemented.*) In order to view screen capture entries through this command, you must first enable the Screen Capture log facility through the **swlogc** command (see *Configuring Switch Logging* on page 14-6). To display screen capture entries in the log, enter

```
caplog
```

at the system prompt. A screen similar to the following will be displayed.

```

1) Console
2) Modem
3) Telnet (0)
4) Telnet (1)
5) Telnet (2)
6) Telnet (3)
    select ?

```

Select which user's screen entries you would like to view by entering the user's line number at the prompt. For example, if you enter **1** at the **select ?** prompt, a screen similar to the following displays:

```

=====Start Screen Capture Display for Console=====
/ % systat

System Uptime                : 0 days, 01:01:47.01
MPM Transmit Overruns       : 0
MPM Receive Overruns        : 0
MPM total memory             : 18548968 bytes
MPM CPU Utilization (5 sec)  : 3 % ( 0% kernel 1% task 97% idle)
MPM CPU Utilization (60 sec) : 4% ( 0% intr 0% kernel 2% task 96% idle)\
Power Supply 1 State         : OK
Power Supply 2 State         : Not Present
Temperature                   : 32.00c 89.60f
Temperature Sensor           : OF - Under Threshold
Temperature Alarm Masking    : Disabled
=====End Screen Capture Display for Console=====

```

The options displayed by the **caplog** command are described below.

- 1) **Console**. Displays screen capture entries for the user logged in from the console.
- 2) **Modem**. Displays screen capture entries for the user logged in from the modem.
- 3) **Telnet (0)**. Displays screen capture entries for the user logged in from the first telnet session.

Displaying Screen (Console) Capture Entries in the MPM Log

- 4) Telnet (1).** Displays screen capture entries for the user logged in from the second telnet session.
- 5) Telnet (2).** Displays screen capture entries for the user logged in from the third telnet session.
- 6) Telnet (3).** Displays screen capture entries for the user logged in from the fourth telnet session.

Displaying Debug Entries in the MPM Log

The **debuglog** command displays the debug entries in the mpm.log file. (*Note: Currently there are no facilities using debugging.*) Below is a sample display of the **debuglog** command.

Task Name	Time	Debug Message
tUdpRelay	14:33:36	Undersized DHCP req rcvd; discarding

The fields displayed by the **debuglog** command are described here.

Task Name. The task that generated the debug message.

Time. The time the message was generated by the task.

Debug Message. Information relevant to debugging.

Displaying Secure Access Entries in the MPM Log

The **seclog** command displays the secure access violation event entries in the mpm.log file. To display this data, enter

seclog

at the system prompt. A screen similar to the following will be displayed.

Secure Access Violations Log

Time	Protocol	Source IP	Attempts	Slot/ Intf	Elapsed Time (secs)
12:49:02	FTP	172.23.8.801	1	5/1	23
03:15:34	Telnet	198.20.2.101	10	2/3	240

Descriptions of the fields are as follows:

Time. The first time the access violation occurred.

Protocol. The IP protocol for which the violation occurred.

Source IP. The source IP address of the unauthorized user.

Attempts. The number of access attempts made by this user within the sample period (5 minutes).

Slot/Intf. The physical port that received the unauthorized user information.

Elapsed Time (secs). The duration (in seconds) from the first unauthorized access to the end of the sampling period (5 minutes). Secure access violations will take 5 minutes to display in the log file.

15 Health Statistics

The health statistics feature monitors the consumable resources of a switch, and provides a single integrated source for Network Management Software (NMS), such as X-Vision, to use in obtaining statistics on switch performance. With the health statistics, the user can set specific threshold levels for consumable resources in the switch. Such resources include bandwidth capacity, CAM and CPU usage, and RAM memory usage. If a threshold for a particular resource is exceeded, a notification is sent to the NMS via an SNMP trap.

◆ Important ◆

You must configure your NMS to accept traps from the monitored switch. X-Vision allows you to set which network management stations receive traps. For more information, see the X-Vision online help.

The health statistics software monitors the resource utilization levels and thresholds of a switch, and at fixed intervals collects the current values for each resource being monitored. After obtaining the statistics, the health statistics software checks to see if any rising or falling threshold crossings occurred since its last poll by comparing the current poll data with the previous poll data. If a threshold crossing has occurred, a trap is sent to NMS (such as X-Vision), allowing the system administrator to pinpoint possible performance issues.

Through the UI (user interface), threshold levels can be set, the sampling interval can be changed, and statistics (for a switch, module, or port) can be viewed or cleared.

The Health Statistics Management Menu

To access the Health menu, log on to a switch via a Telnet or console session, and type the following command:

```
health
```

If the session is in terse mode, you will need to type `?` to see the menu. If you are in verbose mode, the following screen is displayed:

Command	Health Menu
hdcfg	Set or view parameters
hdstat	View device-level statistics
hmstat	View module-level statistics
hpstat	View port-level statistics
hreset	Reset health statistics

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

/System/Health %

The **hdcfg** command allows you to set global thresholds for the switch. The **hdstat**, **hmstat**, **hpstat** commands allow you to view the statistics on a switch, module, or port level, respectively. The **hreset** command resets the statistics for this switch.

Setting Resource Thresholds

The health statistics software operates by monitoring set threshold levels on consumable resources. When a resource exceeds a set level, a trap is generated and sent. These threshold levels are set for the entire switch (or device) by using the **hdcfg** command. To set the threshold level for a switch's consumable resources, enter the **hdcfg** command at the system prompt. The following screen appears:

Device-level Resource Monitoring Configuration

- 1) Set Bandwidth Thresholds :
- 2) Set Miscellaneous Thresholds :
- 3) Set Sampling Interval :

There are three sets of resources that are configurable:

- **Bandwidth thresholds.** These settings allow you to set a percentage of available bandwidth for received traffic, sent traffic, and the backplane. For more information on setting bandwidth thresholds, see *Setting Bandwidth Thresholds* on page 15-3.
- **Miscellaneous thresholds.** These settings allow to set a percentage for memory usage, VCC usage, virtual port usage, and temperature. For more information on setting miscellaneous thresholds, see *Setting Miscellaneous Thresholds* on page 15-4.
- **Sampling interval.** The sampling interval is the number of seconds between health statistics checks. For information on how to set the sampling interval, see *Setting the Sampling Interval* on page 15-6.

Setting Bandwidth Thresholds

Bandwidth is a measure of the amount of traffic a switch can handle for receiving, sending, and on the backplane. The health statistics allow you to set a percentage of available bandwidth, at which an SNMP trap is generated to alert the network administrator that the threshold has been exceeded. To set the threshold levels for switch bandwidth:

1. Enter **health** at a system prompt. The health menu (described above) displays.
2. Enter a **1** at the health menu prompt. The following menu displays:

Bandwidth Resource Monitoring Configuration

```

1) Receive Threshold           : 80
2) Transmit/Receive Threshold : 80
3) Backplane Threshold         : 80

```

3. Threshold values are measured as a percentage of the total capacity of the resource. To change a threshold or sampling interval value, type the index for the field, followed by an equals sign, then the new value. For example, to change the **Receive Threshold** to 50 percent, you would type the following at the prompt:

```
1=50
```

The Receive Threshold would now be set to 50 percent of its total capacity (bandwidth).

4. When you have finished entering the new values, you must enter **save** to keep the new configuration settings.

◆ Note ◆

Changing a threshold value sets the value for all levels of the switch (switch, module, and port). You cannot set different threshold values for each level.

Below is a description of the fields in the **hdcfg** command menu. The default for all monitored resources is eighty (80) percent of the maximum capacity of the resource.

Receive Threshold

The receive threshold sets a percentage of total bandwidth of the switch, module, or port. When the amount of received data exceeds this percentage, an SNMP trap is sent.

Transmit/Receive Threshold

The transmit/receive threshold sets a percentage of the total bandwidth of the switch, module, or port. When the amount of transmitted and received data exceeds this percentage, an SNMP trap is sent.

Backplane Threshold

The backplane threshold sets a percentage of total backplane bandwidth of the switch, module, or port. When backplane usage exceeds this percentage, an SNMP trap is sent.

◆ **Note** ◆

When “U-turn” switching (i.e., data enters a module port and is transmitted from a port on the same module) is employed, the backplane threshold reading will not be correct. Switched frames are not transmitted over the backplane but are counted by health statistics, causing the backplane percentage reading to be higher than it should be.

Setting Miscellaneous Thresholds

The miscellaneous thresholds cover consumable resources such as memory, VCCs, temperature, and virtual ports. The health statistics allow you to set a percentage of the available resource, at which an SNMP trap is generated to alert the network administrator that the threshold has been exceeded. To set the threshold levels for switch bandwidth:

1. Enter **health** at a system prompt. The health menu (described above) displays.
2. Enter a **2** at the health menu prompt. The following menu displays:

Miscellaneous Resource Monitoring Configuration

1) CAM Threshold	: 80
2) CPU Threshold	: 80
3) Memory Threshold	: 80
4) Vcc Threshold	: 80
5) Temperature Threshold	: 80
6) Virtual Port Threshold	: 80

3. Threshold values are measured as a percentage of the total capacity of the resource. To change a threshold or sampling interval value, type the index for the field, followed by an equals sign, then the new value. For example, to change the **CAM Threshold** to 50 percent, you would type the following at the prompt:

1=50

The CAM Threshold would now be set to 50 percent of its total capacity (memory).

4. When you have finished entering the new values, you must enter **save** to keep the new configuration settings.

◆ **Note** ◆

Changing a threshold value sets the value for all levels of the switch (switch, module, and port). You cannot set different threshold values for each level.

CAM Threshold (MPM/HRE or NI)

The CAM threshold sets a percentage of the total amount of space available for storing the cache tables. Cache tables maintain associations between received MAC addresses and the ports they were received on. For the switch level, the CAM threshold separately monitors the MPM and the HRE daughtercard (if it is installed) CAM tables. For the module level, it monitors the switching module CAM tables. CAM thresholds are not available on the port level.

When this percentage is exceeded, an SNMP trap is sent.

CPU Threshold

The CPU threshold sets a percentage of the total amount of processing ability for the MPM. When the CPU usage exceeds this percentage, an SNMP trap is sent. The CPU threshold is only used for the switch level.

Memory Threshold

The memory threshold sets a percentage of the total amount to MPM RAM memory for the switch. When RAM usage exceeds this percentage, an SNMP trap is sent. The memory threshold is only used for the switch level.

Vcc Threshold

This threshold sets a percentage of the total number of available VCCs for the switch. When the set percentage of available VCCs is exceeded, an SNMP trap is sent.

Temperature Threshold

This threshold sets the number of degrees for the switch at which an SNMP trap is sent. This threshold is measured in degrees Celsius. The range is from 0 to 100.

Virtual Port Threshold

This threshold sets a percentage of the total number of available virtual ports for the switch. When the set percentage of available virtual ports is exceeded, an SNMP trap is sent.

Setting the Sampling Interval

The sampling interval is the time interval between polls of the switch's consumable resources to see if it is performing within the set thresholds. To set the amount of time between polls:

1. Enter **health** at a system prompt. The health menu (described above) displays.
2. Enter a **3** at the health menu prompt. The following menu displays:

Resource Monitoring Interval Configuration

1) Sampling Interval : 5

3. To change the sampling interval, enter a 1, and equal sign, and the new interval in seconds. For example, to change the sampling interval to 4 seconds, you would enter the following:

1=4

4. When you have finished entering the new value, you must enter **save** to keep the new configuration setting.

Sampling Interval

This sets the number of seconds between internal polling intervals. The health statistics compares the current poll statistics with the last poll statistics to determine whether or not to send a trap. The default for the **Sampling Interval** is five (5) seconds.

View Switch-Level Statistics

To view the statistics for the entire switch, enter the **hdstat** command at a system prompt. The following table is displayed:

Device Resources	Limit	Curr	1 Min Avg	1 Hr Avg	1 Hr Max
Receive	80	00	00	00	00
Transmit/Receive	80	00	00	00	00
Backplane	80	01	01	01	01
CAM [MPM]	80	00	00	00	00
CAM [HRE]	80	00	00	00	00
CPU	80	93*	13	13	22
Memory	80	50	50	50	50
Temperature	45	44	44	44	44
Virtual Ports	80	11	11	11	11

/System/Health %

Statistics are displayed as percentages of the total resource capacity, and represent data taken from the last sampling interval. If a threshold for a resource was exceeded, then that statistic is marked with an asterisk (*).

◆ Important Note ◆

The **hdstat** command displays CAM usage for the entire chassis. To see CAM usage for switching modules only, use the **camstat** command as described in Chapter 13, "Switch Wide Parameters."

For field descriptions of the device resources column, see *Setting Bandwidth Thresholds* on page 15-3 and *Setting Miscellaneous Thresholds* on page 15-4 above.

◆ **Note** ◆

When calculating percentages, the health statistics cannot display less than one percent. If a single packet is sent through a port, for example, the receive resource usage is represented as one percent.

The following section describes the statistics displayed using the **hdstat** command.

Limit

The set threshold for this resource. You can set the resource levels using the **hdcfg** command. See *Setting Resource Thresholds* on page 15-2 for specific procedures.

Current

The current resource usage. This number is a percentage of the total resource capacity.

1 Minute Average

The average percent of resource use for the last sixty seconds.

1 Hour Average

The average percent of resource use for the last sixty minutes.

1 Hour Maximum

The maximum percent of resource use for the last sixty minutes.

View Module-Level Statistics

To view module level statistics, type the **hmstat** command at a system prompt followed by the slot number. For example, to view the statistics for a module in slot three, type the following:

```
hmstat 3
```

The following screen is displayed:

Slot 3 Resources	Limit	Curr	1 Min Avg	1 Hr Avg	1 Hr Max
Receive	80	00	00	00	00
Transmit/Receive	80	00	00	00	00
Backplane	80	95*	00	00	00
CAM	80	00	00	00	00

/System/Health %

Statistics are displayed as percentages of the total resource capacity, and represent data taken from the last sampling interval. If a threshold for a resources was exceeded, then that statistic is marked with an asterisk (*). For descriptions of the monitored resources, see *Setting Bandwidth Thresholds* on page 15-3 and *Setting Miscellaneous Thresholds* on page 15-4 above.

For descriptions of the statistics, see *View Switch-Level Statistics* on page 15-6.

◆ **Note** ◆

The CPU and memory resources are not applicable to the module level statistics display, and therefore are not shown.

View Port-Level Statistics

To view port-level statistics, type the **hpstat** command at a system prompt as shown:

```
hpstat <slot>/<port>
```

where **<slot>** is the slot number and **<port>** is the port number. For example to view port 1 on slot 3, enter the following:

```
hpstat 3/1
```

The following screen is displayed:

Port 3/1 Resources	Limit	Curr	1 Min Avg	1 Hr Avg	1 Hr Max
Receive	80	00	00	00	00
Transmit/Receive	80	92*	00	00	00
Backplane	80	00	00	00	00

```
/System/Health %
```

Statistics are displayed as percentages of the total resource capacity, and represent data taken from the last sampling interval. If a threshold for a resource was exceeded, then that statistic is marked with an asterisk (*). For descriptions of the monitored resources, see *Setting Bandwidth Thresholds* on page 15-3 and *Setting Miscellaneous Thresholds* on page 15-4 above.

For descriptions of the statistics, see *View Switch-Level Statistics* on page 15-6.

Reset Health Statistics

To reset the health statistics for the switch, type the **hreset** command at a system prompt. The following message is displayed:

```
Are you sure you want to reset health statistics? (n) :
```

To confirm your choice to clear the switch health statistics, type **y** at the prompt. After you confirm your choice, the following confirmation notice is displayed:

```
RESET HEALTH STATISTICS
```

◆ **Note** ◆

The **hreset** command clears the statistics for the entire switch. You cannot clear statistics for the module or port level only.

16 Network Time Protocol

Introduction

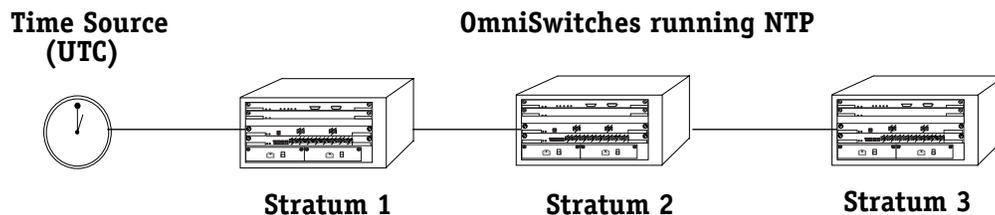
The Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver. It provides client time accuracies within a millisecond on LANs, and up to a few tens of milliseconds on WANs relative to a primary server synchronized to Coordinated Universal Time (UTC) (via a Global Positioning Service receiver, for example). Typical NTP configurations utilize multiple redundant servers and diverse network paths in order to achieve high accuracy and reliability. Some configurations include cryptographic authentication to prevent accidental or malicious protocol attacks.

It is important for networks to maintain accurate time synchronization between network nodes. The standard timescale used by most nations of the world is based on a combination of Universal Coordinated Time (UTC) (representing the Earth's rotation about its axis) and the Gregorian Calendar (representing the Earth's rotation about the Sun). The UTC timescale is disciplined with respect to International Atomic Time (TAI) by inserting leap seconds at intervals of about 18 months. UTC time is disseminated by various means, including radio and satellite navigation systems, telephone modems, and portable clocks.

Special purpose receivers are available for many time-dissemination services, including the Global Position System (GPS) and other services operated by various national governments. For reasons of cost and convenience, it is not possible to equip every computer with one of these receivers. However, it is possible to equip some computers with these clocks, which then act as primary time servers to synchronize a much larger number of secondary servers and clients connected by a common network. In order to do this, a distributed network clock synchronization protocol is required which can read a server clock, transmit the reading to one or more clients, and adjust each client clock as required. Protocols that do this include the Network Time Protocol (NTP).

Stratum

Stratum is the term used to define the relative proximity of a node in a network to a time source (such as a radio clock). Stratum 1 is the server connected to the time source itself. (In most cases the time source and the stratum 1 server are in the same physical location.) An NTP client or server connected to a stratum 1 source would be stratum 2. A client or server connected to a stratum 2 machine would be stratum 3, and so on, as demonstrated in the diagram below.



The farther away from stratum 1 a device is, the more likely there will be discrepancies or errors in the time adjustments done by NTP. A list of stratum 1 and 2 sources available to the public can be found on the Internet.

◆ Note ◆

It is not required that NTP be connected to an officially recognized time source (for example, a radio clock). NTP can use any time source to synchronize time in the network.

Using NTP in a Network

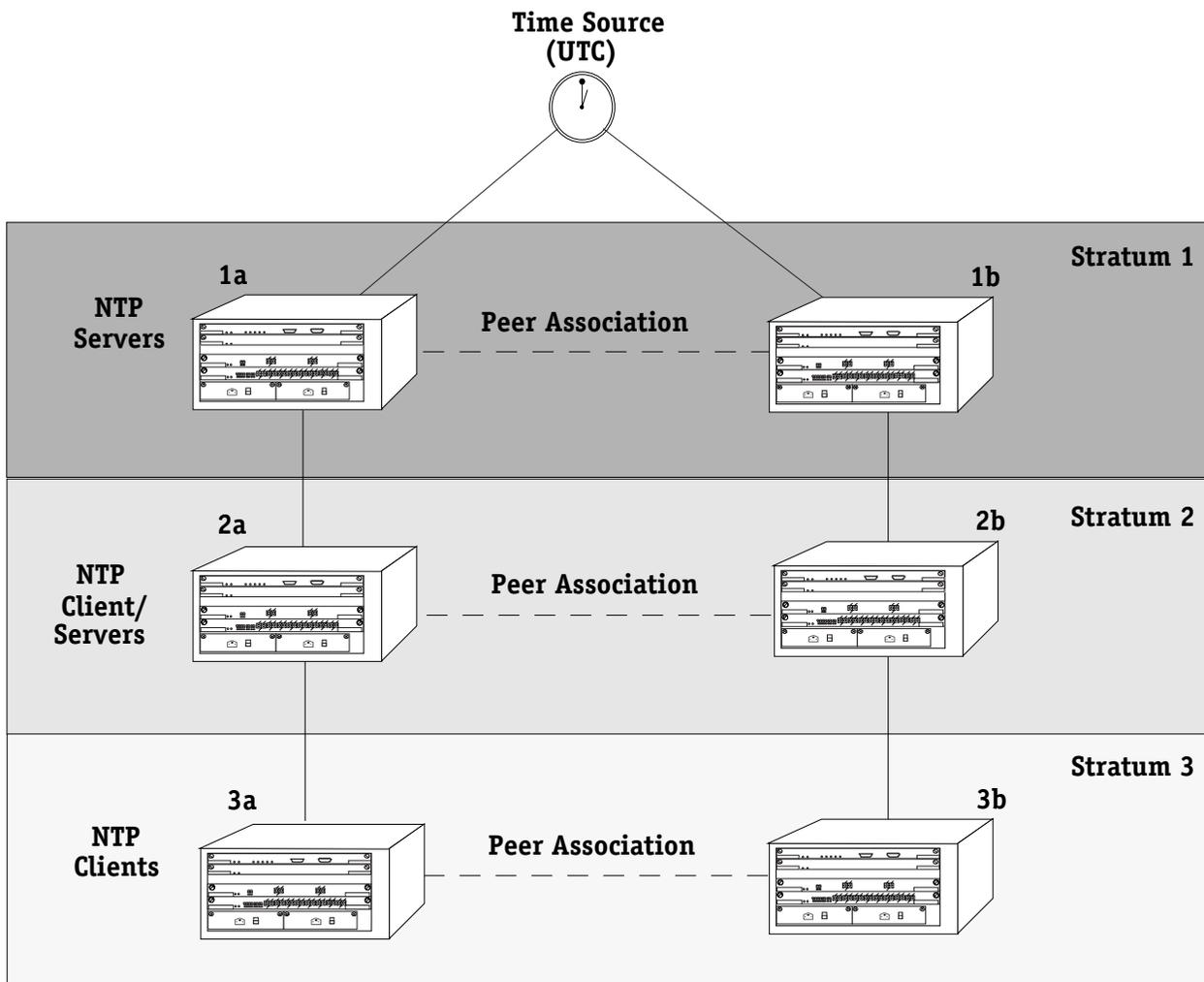
NTP operates on the premise that there is one true standard time (defined by UTC), and that if several servers claiming synchronization to the standard time are in disagreement, then one or more of them must be out of synchronization or not functioning correctly.

The stratum gradation is used to qualify the accuracy of a time source along with other factors such as advertised precision and the length of the network path between connections. NTP operates with a basic distrust of time information sent from other network entities, and is most effective when multiple NTP time sources are integrated together for checks and cross-checks.

To achieve this end, there are several modes of operation that an NTP entity can use when synchronizing time in a network. These modes help predict how the entity behaves when requesting or sending time information, listed below:

- A switch can be a client of an NTP server (usually of a lower stratum), receiving time information from the server but not passing it on to other switches.
- A switch can be a client of an NTP server, and in turn be a server to another switch or switches.
- A switch (regardless of its status as either a client or server) must be *peered* with another switch. Peering allows NTP entities in the network of the same stratum to regard each other as reliable sources of time and exchange time information.

Examples of these are shown in the simple network diagram on the following page:



Servers 1a and 1b receive time information from, or synchronize with, a UTC time source such as a radio clock. (In most cases, these servers would not be connected to the same UTC source, though it is shown this way for simplicity.) Servers 1a and 1b become stratum 1 NTP servers and are peered with each other, allowing them to check UTC time information against each other. These machines support machines 2a and 2b as clients, and these clients are synchronized to the higher stratum servers 1a and 1b.

Clients 2a and 2b are also peered with each other for time checks, and become stratum 2 NTP servers for more clients (3a and 3b, which are also peered).

In this hierarchy, the stratum 1 servers synchronize to the most accurate time source available, then check the time information with peers at the same stratum. The stratum 2 machines synchronize to the stratum 1 servers, but do not send time information to the stratum 1 machines. Machines 2a and 2b in turn provide time information to the stratum 3 machines.

It is important to consider the issue of robustness when selecting sources for time synchronization. It is suggested that at least three sources should be available, and at least one should be “close” to you in terms of network topology. It is also suggested that each NTP client is peered with at least three other same stratum clients, so that time information crosschecking will be performed.

When planning your network, it is helpful to use the following general rules:

- It is usually not a good idea to synchronize a local time server with a peer (in other words, a server at the same stratum), unless the latter is receiving time updates from a source that has a lower stratum than from where the former is receiving time updates. This minimizes common points of failure.
- Peer associations should only be configured between servers at the same stratum level. Higher Strata should configure lower Strata, not the reverse.
- It is inadvisable to configure time servers in a domain to a single time source. Doing so invites common points of failure.

NTP and Authentication

NTP is designed to use either DES or MD5 encryption authentication to prevent outside influence upon NTP timestamp information. This is done by using a key file. The key file is loaded into the switch memory, and consists of a text file that lists key identifiers that correspond to particular NTP entities.

If authentication is enabled on an NTP switch, any NTP message sent to the switch must contain the correct key ID in the message packet to use in decryption. Likewise, any message sent from the authentication enabled switch will not be readable unless the receiving NTP entity possesses the correct key ID.

Key files are created by a system administrator independent of the NTP protocol, and then placed in the switch memory. An example of a key file is shown below:

1	N	29233e0461ecd6ae	# des key in NTP format
2	M	Rlrop8KPPvQvYotM	# md5 key as an ASCII random string
14	M	sundial	# md5 key as an ASCII string
15	A	sundial	# des key as an ASCII string

In a key file, the first token is the key number ID, the second is the key format, and the third is the key itself. (The text following a “#” is not counted as part of the key, and is used merely for description.) There are 4 key formats:

N	Indicates a DES key written as a hex number, in NTP standard format with the high order bit of each octet being the odd parity bit.
M	Indicates an MD5 key written as a 1 to 31 character ASCII string with each character standing for a key octet.
A	Indicates a DES key written as a 1 to 8 character string in 7-bit ASCII format, where each character stands for a key octet string.
S	Indicates a DES key written as a hex number in the DES standard format, with the low order bit of each octet being the odd parity bit.

For information on activating authentication, specifying the location of a key file, and configuring key IDs for switches, see the following sections:

- *Configuring an NTP Client* on page 16-6
- *Configuring a New Peer Association* on page 16-12
- *Configuring a New Server* on page 16-13
- *Configuring a Broadcast Time Service* on page 16-13

Network Time Protocol Management Menu

To access the NTP management menu, connect to a switch via a console or telnet session and enter **NTP** at the system prompt. If you are in verbose mode, or enter a question mark (?) at the prompt, the following screen is displayed:

Command	NTP Management Menu
Ntconfig	Enter the NTP configuration menu
Ntinfo	Enter the NTP information menu
Ntstats	Enter the NTP statistics menu
Ntadmin	Enter the NTP administration menu
Ntaccess	Enter the NTP access control menu

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

Ntconfig. This command accesses the NTP configuration menu, which allows you to configure this NTP device, add or remove peer associations, add an NTP server, configure this NTP device's broadcast time, and set or change this NTP device's fudge factor. See *NTP Configuration Menu* on page 16-6 for more information on the NTP configuration menu.

Ntinfo. This command accesses the NTP information menu, which allows you to view a list of all peers for this NTP device, display a list of peers with summary information (in two different formats), display detailed information for one or more peers, and display local server information. See *NTP Information Menu* on page 16-15 for more information.

Ntstats. This command accesses the NTP statistics menu, which allows you to view the statistics for the loop filter, peer memory usage, I/O subsystem, local server, event time subsystem, packet counts, leap second state, clock status, monitoring routines data. See *NTP Statistics Menu* on page 16-23 for more information.

Ntadmin. This command accesses the NTP administration menu, which allows you to set the receive timeout, set an encryption delay, specify a remote NTP server, set a password and key ID for this NTP device, set and clear a system flag, and restart the NTP software. See *NTP Administration Menu* on page 16-33 for more information.

Ntaccess. This command accesses the NTP access control menu, which allows you to change the authentication key ID for request and control messages, reinitialize the key ID list, add a key ID to or remove a key ID from the trusted list, display the state of the authentication code, create or remove restrict and add flags to an entry, view a servers restriction list, remove a restriction entry from this NTP device, and configure, remove or view traps set in the server. See *NTP Access Control Menu* on page 16-36 for more information.

NTP Configuration Menu

To view the NTP configuration menu, enter the **ntconfig** command at the system prompt. If you are in verbose mode the NTP configuration menu is displayed. Otherwise, enter a question mark (?) at the prompt to display this menu:

Command	NTP Configuration Menu
ntpiconfig	Initial NTP configuration
ntpaddpeer	configure a new peer association
ntpaddserv	configure a new server
ntpbcast	configure broadcasting time service
ntpunconfig	unconfigure existing peer associations
ntpprec	set the server's advertised precision
ntpfudge	set/change one of a clock's fudge factors

Related Menus:
Ntconfig Ntinfo Ntstats Ntadmin Ntaccess

The main menu options are shown in the **Related Menus** list for quick access if you need to change menus.

A switch can be configured to act as an NTP client, or an NTP client/server. An NTP client receives updates from an NTP server without passing on time information to other clients, while an NTP client/server receives time information from a server, and acts as a server for other clients in a higher stratum.

Configuring an NTP Client

To set up the NTP client, use the **ntpiconfig** command as follows:

1. Enter the command as shown, at the system prompt:

```
ntpiconfig
```

The following menu appears:

NTP Startup Configuration

```

1) Response timeout           : 0
2) Authentication delay      : No
3) Authentication key file name : UNSET
4) NTP client mode           : Ucast
5) Enable monitor            : No
6) Enable NTP server         : No

```

2. Adjust the configurable variables for this NTP client as needed by entering the line number, and equal sign, and a new value at the system prompt, as shown:

```
<lineNumber>=<value>
```

For example, to change the **Response timeout** to 10, you would enter **1** (the line number for **Response timeout**), an equal sign (=), and the number **10** (the new value), as shown:

```
1=10
```

After enabling NTP for this switch, you need to configure at least one peer association, unless you will be supplying time synchronization. In that case, you need to configure a reference clock.

For information on adding a peer association, see *Configuring a New Peer Association* on page 16-12.

Field Descriptions

The following section describes the fields displayed using the `ntpconfig` command.

1) Response timeout

This field sets the timeout period for responses to server queries. Server queries come from the server responsible for providing this client with NTP time information. The default is 8000 milliseconds.

2) Authentication delay

This field sets a specified time interval that is added to timestamps included in requests to the server that required authentication. Typically this delay is needed in cases of long delay paths, or of servers whose clocks are unsynchronized.

3) Authentication key file name

The key file is a file that holds the NTP authentication keys used during remote access or configuration of the server responsible for this client. This field allows you to specify the name of the key file. The key file should be kept in the `/flash` directory of the switch.

Specifying a key file expands the NTP Startup Configuration menu. For more information on configuring authentication, see *Configuring Client/Server Authentication* on page 16-9.

4) NTP client mode

This field allows you to set how the client mode of this device sends its server queries. The options are **U** (for unicast), **B** (for broadcast), or **M** (for multicast).

Setting the NTP client mode to broadcast or multicast expands the NTP Startup Configuration menu. A suboption for the NTP client mode appears, allowing you to specify the broadcast or multicast address, as shown:

41) NTP multicast address :

Enter the broadcast or multicast address at the prompt by typing line number **41**, an equal sign (=), and the IP address. For example, to specify a multicast address of 204.0.1.1, you would enter the following:

41=204.0.1.1

5) Enable monitor

This field turns NTP monitoring on or off. Entering **yes** activates NTP monitoring, while entering **no** deactivates this function. The statistics for monitoring can be viewed using the `ntpmon` command in the statistics menu. See *NTP Statistics Menu* on page 16-23 for more information.

6) Enable NTP server

This field allows you to enable the server portion of the NTP software for this NTP device. When set to **yes**, this device can act as an NTP server for other clients. When set to **no**, this device is only a client of another NTP server.

Configuring an NTP Client/Server

A switch can be configured to act both as a client and a server. If you want to run both the client and server portions of the NTP software, follow the steps below:

1. Enter the command as shown, at the system prompt:

```
ntpconfig
```

The following menu appears:

NTP Startup Configuration

```
1) Response timeout           : 0
2) Authentication delay       : No
3) Authentication key file name : UNSET
4) NTP client mode            : Ucast
5) Enable monitor              : No
6) Enable NTP server           : No
```

2. Adjust the configurable variables for this NTP client as needed by entering the line number, and equal sign, and a new value at the system prompt, as shown:

```
<lineNumber>=<value>
```

For example, to change the **Response timeout** to 10, you would enter **1** (the line number for **Response timeout**), an equal sign (=), and the number **10** (the new value), as shown:

```
1=10
```

3. Enable the NTP server by entering a **6**, an equal sign (=), and **yes** at the prompt, as shown:

```
6=yes
```

The NTP Startup Configuration menu expands to display new options. The menu now appears similar to the following:

NTP Startup Configuration

```
1) Response timeout           : 0
2) Authentication delay       : No
3) Authentication key file name : UNSET
4) NTP client mode            : Ucast
5) Enable monitor              : No
6) Enable NTP server           : No
  61) Client limit              : 3
  62) Client limit period       : 3600
  63) Enable server authentication : No
  64) Advertised precision       : -7
  65) Broadcast delay           : 0
```

4. Adjust the configurable variables for this NTP server as needed by entering the line number, and equal sign, and a new value at the system prompt, as shown:

```
<lineNumber>=<value>
```

For example, to change the **Client limit** to 10, you would enter **61** (the line number for **Client limit**), an equal sign (=), and the number **10** (the new value), as shown:

```
61=10
```

Field Descriptions

The following section describes the expanded menu options.

61) Client limit

This field allows you to set a specific number of clients that are allowed to make requests of the server during a specified time period. Setting this field to **0** allows an unlimited number of clients to connect to the server.

62) Client limit period

This field allows you to set the client limit time period (in seconds). This along with the **client limit** field above determine how many clients are allowed to make requests of this server.

63) Enable server authentication

This field enables the authentication of unsynchronized peers. If set to **yes**, NTP only synchronizes with peers that has been authenticated with the correct key ID.

64) Advertised precision

Sets the precision which the server advertises to the specified value. This should be a negative integer in the range -4 through -20.

65) Broadcast delay

This fields allows you to set a specified network delay time. Normally, NTP automatically compensates for the network delay between the broadcast/multicast server and the client. If this calibration fails, the delay set here is used instead.

Configuring Client/Server Authentication

In order to use authentication, you must specify a key file. A key file contains the keys necessary for NTP to decode encrypted NTP messages. To specify a key file, follow the steps below:

1. Enter the command as shown, at the system prompt:

```
ntpiconfig
```

The following menu appears:

NTP Startup Configuration

```

1) Response timeout           : 0
2) Authentication delay      : No
3) Authentication key file name : UNSET
4) NTP client mode           : Ucast
5) Enable monitor            : No
6) Enable NTP server         : No

```

2. Adjust the configurable variables for this NTP client as needed by entering the line number, and equal sign, and a new value at the system prompt, as shown:

<lineNumber>=<value>

For example, to change the **Response timeout** to 10, you would enter **1** (the line number for **Response timeout**), an equal sign (=), and the number **10** (the new value), as shown:

1=10

3. Enable authentication by entering a **3**, and equal sign (=), and a key file name at the prompt, as shown:

3=ntp.keys

The NTP Startup Configuration menu expands to display new options. The menu now appears similar to the following:

NTP Startup Configuration

1) Response timeout	: 0
2) Authentication delay	: No
3) Authentication key file name	: ntp.keys
31) Configuration info authentication key	:
32) Control request authentication key	:
33) Configuration change authentication key	:
4) NTP client mode	: Ucast
5) Enable monitor	: No
6) Enable NTP server	: No

4. Adjust the configurable variables for authentication as needed by entering the line number, and equal sign, and a new value at the system prompt, as shown:

<lineNumber>=<value>

For example, to change the **Configuration info authentication key** to 10, you would enter **1** (the line number for **Configuration info authentication key**), an equal sign (=), and the number **10** (the new value), as shown:

1=10

Field Descriptions

The following section describes the expanded menu options.

31) Configuration info authentication key

The number of the key in the key file used to authenticate configuration information. Configuration information sets configuration parameters. For more information on the key file, see *NTP and Authentication* on page 16-4.

32) Control request authentication key

The number of the key in the key file used to authenticate control requests. Control requests come from other NTP clients and servers. For more information on the key file, see *NTP and Authentication* on page 16-4.

33) Configuration change authentication key

The number of the key in the key file used to authenticate configuration change requests. Configuration change requests come from other NTP clients and servers. For more information on the key file, see *NTP and Authentication* on page 16-4.

Configuring a New Peer Association

When you have configured the NTP client and/or server, you will need to set at least one peer association for the switch. An NTP peer is a machine of the same stratum that will compare and check time information sent from the switch, and in turn send time information to the switch.

To configure a new peer, enter the **ntpaddpeer** command in the following manner:

```
ntpaddpeer <address> [<keyld> <version> <minpol>] [prefer]
```

where **<address>** is either the domain name or IP address of the peer machine. The optional configuration items are described below:

<keyld>. An unsigned 32-bit integer key identifier for encryption authentication. The default is for no key ID.

<version>. The version of NTP being used. The options are versions 1, 2, or 3. If no number is entered, it is assumed that version 3 is being used.

<minpol>. The minimum poll interval for time checks to this peer. The number entered is seconds raised to the power of 2.

prefer. An identifier that marks this peer as a preferred source of time information. In a situation where multiple peers could provide time information to this client, the preferred peer is the one that is used.

For example, to add a peer with an address of 1.1.1.1, a key identifier of 5, using version 3 of NTP, minimum poll of 16 seconds, and marked as a preferred server, you would enter the following:

```
ntpaddpeer 1.1.1.1 5 3 4 prefer
```

When you have finished press **<return>**. A brief message appears confirming the addition of a new peer.

Configuring a New Server

For the switch to synchronize its time, you must specify a server, or servers, from which the switch receives time information. This is done with the **ntpaddserv** command.

To add a synchronization server to a switch, use the command that follows:

```
ntpaddserv <address> [<keyId><version><minpol>] [prefer]
```

where **<address>** is either the domain name or IP address of the server. The optional configuration items are described below:

<keyId>. An unsigned 32-bit integer key identifier for encryption authentication. The default is no key ID.

<version>. The version of NTP being used. The options are versions 1, 2, or 3. If no number is entered, it is assumed that version 3 is being used.

<minpol>. The minimum poll interval for time checks to this server. The number entered is seconds raised to the power of 2.

prefer. An identifier that marks this peer as a preferred source of time information. In a situation where multiple peers could provide time information to this client, the preferred peer is the one that is used.

For example, to add a peer with an address of 1.1.1.1, a key identifier of 5, using version 3 of NTP, with a poll time of 16, and marked as a preferred server, you would enter the following:

```
ntpaddpeer 1.1.1.1 5 3 4 prefer
```

When you have finished press **<return>**. A brief message appears confirming the addition of a new server.

Configuring a Broadcast Time Service

The NTP server can be configured to operate in broadcast mode, where the server sends periodic broadcast messages to a client population by using the broadcast or multicast address specified. To configure the server to use a broadcast or multicast address, enter the **ntpbcast** command as shown:

```
ntpbcast <address> [<keyId>] [<version>] [<minpol>]
```

where **<address>** is either the domain name or the broadcast or multicast address.

◆ Important Note ◆

A multicast address of 224.0.1.1 has been assigned to NTP. Presently, this is the only address that should be used for multicast messages.

The optional configuration items are described below:

<keyId>. An unsigned 32-bit integer key identifier for encryption authentication. The default is no key ID.

<version>. The version of NTP being used. The options are versions 1, 2, or 3. If no number is entered, it is assumed that version 3 is being used.

<minpol>. The minimum poll interval for time checks to this server. The number entered is in seconds raised to the power of 2.

For example, to add broadcast address 1.1.1.1 with a key identifier of 5, using version 3 of NTP, and a minimum poll time of 16 seconds, you would enter the following:

```
ntpbcast 1.1.1.1 5 3 4
```

When you have finished press **<return>**. A brief message appears confirming the addition of a new server.

Unconfigure Existing Peer Associations

You can remove server, peer, or reference clock associations for this switch using the **ntpunconfig** command. This will remove a selected address from this switch's list of configured addresses. To do this, enter the **ntpunconfig** command as follows:

```
ntpunconfig <address>
```

where **<address>** is either the domain name or IP address of the association. For example, to remove a peer association with address 1.1.1.1, enter the following:

```
ntpunconfig 1.1.1.1
```

When you have finished press **<return>**. A brief message appears confirming the addition of a new server.

You can remove multiple addresses at one time by adding additional addresses to the command. For example, to remove a peer association with address 1.1.1.1 and a reference clock association with address 1.1.1.2, enter:

```
ntpunconfig 1.1.1.1 1.1.1.2
```

When you have finished press **<return>**. A brief message appears confirming the removal of the association.

Set the Server's Advertised Precision

If necessary, you can adjust the server's advertised precision. The precision of a server is a signed integer indicating the precision of the clocks in seconds to the nearest power of 2. It determines how accurate the clock is under normal circumstances, and allows NTP to determine which is the best time source for synchronization. To set the server's advertised precision, enter the **ntpprec** command as shown:

```
ntpprec <interval>
```

where **<interval>** is the signed integer in seconds. This number must be between -4 and -20. For example, to set the server's advertised precision to -5, you would enter the following:

```
ntpprec -5
```

When you have finished press **<return>**. A brief message appears confirming the change of the advertised precision.

◆ Note ◆

The determination of a server's advertised precision is based largely on the clock type used as the ultimate time source (stratum 1).

NTP Information Menu

To view the NTP configuration menu, enter the **ntinfo** command at the system prompt. If you are using verbose mode, the NTP configuration menu is displayed. Otherwise, enter a question mark (?) at the prompt to display this menu:

Command	NTP Information Menu
ntplpeers	display list of peers the server knows about
ntppeers	display peer summary information
ntpdmpeers	display peer summary info the way Dave Mills likes it
ntpshowpeer	display detailed information for one or more peers
ntpvers	print version number
ntpinfo	display local server information

Related Menus:

Ntconfig Ntinfo Ntstats Ntadmin Ntaccess

The main menu options are shown in the **Related Menus** list for quick access if you need to change menus.

Display List of Peers the Server Knows About

The **ntplpeers** command is used to display a brief list of all NTP associations related to this switch (servers, peers, etc.).

To display a list of NTP associations, enter the **ntplpeers** command at the system prompt. A display similar to the following is shown:

```
client 1.1.1.1
client 1.1.1.2
sym_active 1.1.1.3
```

The list shows the mode this switch is using in relation to the association, and the address of the remote association. The address is either a domain name or an IP address. The available modes are as follows:

- Symmetric Active (1)** A host in this mode sends periodic messages regardless of the reachability state of stratum of its peer. By operating in this mode the host announces its willingness to synchronize and be synchronized by the peer.
- Symmetric Passive (2)** This type of association is ordinarily created upon the arrival of a message from a peer operating in the symmetric active mode and persists only as long as the peer is reachable and operating at a stratum level less than or equal to the host; otherwise the association is dissolved. The association will always persist until at least one message has been sent in reply. By operating in this mode the host announces its willingness to synchronize and be synchronized by the peer.
- Client (3)** A host operating in this mode sends periodic messages regardless of the reachability state of stratum of its peer. By operating in this mode the host, usually a LAN workstation, announces its willingness to be synchronized, but not to synchronize the peer.

- Server (4)** This type of association is ordinarily created upon arrival of a client request message and exists only in order to reply to that request, after which the association is dissolved. By operating in this mode the host, usually a LAN time server, announces its willingness to synchronize, but not be synchronized by the peer.
- Broadcast (5)** A host operating in this mode sends periodic messages regardless of the reachability state or stratum of the peers. By operating in this mode, the host, usually a LAN time server operating on a high-speed broadcast medium, announces its willingness to synchronize all peers, but not be synchronized by any of them.

◆ **Note** ◆

The mode of the switch in relation to the remote association is determined when you create the association. See *NTP Configuration Menu* on page 16-6 for more information on creating NTP associations.

Display Peer Summary Information

The **ntppeers** command displays a more detailed version of the **ntplpeers** command. To display a list of peers that includes summary information, enter the **ntppeers** command at the system prompt. A screen similar to the following appears:

	remote	local	st	poll	reach	delay	offset	disp
=	1.1.1.1	0.0.0.5	16	64	0	0.00000	0.00000	16.0000
+	1.1.1.2	0.0.0.5	1	64	0	0.00000	0.00000	16.0000
=	1.1.1.3	0.0.0.5	2	64	0	0.00000	0.00000	16.0000

The symbols at the very left of this table note the relationship (mode) of the switch to the remote association. The section below is a key for interpreting these symbols:

- + The switch is in symmetric active mode.
- The switch is in symmetric passive mode.
- = The switch is in client mode.
- ^ The switch is broadcasting to this address.
- ~ The switch is receiving broadcasts from this address.
- * The switch is currently synchronizing with this address.

Field Descriptions

The following sections describe the fields displayed using the **ntppeers** command

Remote. The IP address of the remote association.

Local. The local interface address assigned by NTP to the remote association. If this address is **0.0.0.0**, then the local address has yet to be determined.

St. The stratum level of the remote peer. If this number is **16**, the remote peer has not been synchronized.

Poll. The polling interval, in seconds.

Reach. The reachability register of the remote association, in octal format. This number is determined by the NTP algorithm.

Delay. The currently estimated delay of this remote association, in seconds. This time is determined by the NTP algorithm.

Offset. The currently estimated offset of this remote association, in seconds. This time is determined by the NTP algorithm.

Disp. The currently estimated dispersion of this remote association, in seconds. This time is determined by the NTP algorithm.

Display Alternate Peer Summary Information

The **ntpdmpeers** command displays a more detailed version of the **ntpshowpeer** command with a slightly different output than the **ntppeers** command. To display a list of peers that includes summary information, enter the **ntpdmpeers** command at the system prompt. A screen similar to the following appears:

	remote	local	st	poll	reach	delay	offset	disp
+	1.1.1.1	0.0.0.5	16	64	0	0.00000	0.00000	16.0000
+	1.1.1.2	0.0.0.5	1	64	0	0.00000	0.00000	16.0000
*	1.1.1.3	0.0.0.5	2	64	0	0.00000	0.00000	16.0000

This table is identical to the **ntppeers** command except for the symbols displayed on the far left side. A key for the symbols is provided below:

- . Indicates that the remote association was cast aside during the false ticker detection.
- +
- Indicates that the remote association was accepted and not discarded by the false ticker detection.
- *
- Indicates the remote association the switch is currently synchronizing with.

Display Detailed Information for One or More Peers

The `ntpshowpeer` command allows you to view detailed NTP information about any remote associations of this switch. To view detailed NTP information about a remote association enter the `ntpshowpeer` command in the following manner:

```
ntpshowpeer <address>
```

where `<address>` is either the domain name or IP address of the remote association. For example, to show information for a peer with IP address 1.1.1.4, enter:

```
ntpshowpeer 1.1.1.4
```

A screen similar to the following is displayed:

```
remote 1.1.1.4, local 0.0.0.6
hmode sym_active, pmode server, stratum 16, precision -7
leap 11, refid [0.0.0.0], rootdistance 0.00000, rootdispersion 0.00000
ppoll 6, hpoll 6, keyid 0, version 3, association 41807
valid 0, reach 000, unreachable 0, flash 000, boffset 0.00391, ttl/mode 0
timer 32s, flags config, bclient
reference time:      00000000.00000000 Thu, Feb 7 1936 6:28:16.000
originate timestamp: 00000000.00000000 Thu, Feb 7 1936 6:28:16.000
receive timestamp:   00000000.00000000 Thu, Feb 7 1936 6:28:16.000
transmit timestamp:  00000000.00000000 Thu, Feb 7 1936 6:28:16.000
filter delay:        0.00000 0.00000 0.00000 0.00000
                    0.00000 0.00000 0.00000 0.00000
filter offset:       0.000000 0.000000 0.000000 0.000000
                    0.000000 0.000000 0.000000 0.000000
filter order:        7   6   5   4
                    3   2   1   0
offset 0.000000, delay 0.00000, dispersion 16.00000, selectdisp 0.00000
```

It is possible to display information from more than one remote association by adding more addresses when entering the `ntpshowpeer` command. For example, to display information on a peer with IP address 1.1.1.4 and a peer with IP address 1.1.1.5, enter:

```
ntpshowpeer 1.1.1.4 1.1.1.5
```

Field Descriptions

The following section describes the fields displayed using the `ntpshowpeer` command.

Remote. The IP address of the remote association.

Local. The local interface address assigned by NTP to the remote association. If this address is `0.0.0.0`, then the local address has yet to be determined.

Hmode. The host mode of this remote association. There are five possible modes: symmetric active, symmetric passive, client, server, and broadcast. The displayed mode is assumed if this association becomes the switch's host NTP server. For a description of the modes, see *Display List of Peers the Server Knows About* on page 16-15. For a description of how to set a switch host NTP server, see *Specify the Host Whose NTP Server We Talk To* on page 16-34.

Pmode. The peer mode of this remote association. There are five possible modes: symmetric active, symmetric passive, client, server, and broadcast. The displayed mode is assumed if this association becomes the switch's host NTP server. For a description of the modes, see *Display List of Peers the Server Knows About* on page 16-15. For a description of how to configure a peer, see *Configuring a New Peer Association* on page 16-12.

Stratum. The stratum level of the remote peer. If this number is `16`, the remote peer has not been synchronized.

Precision. The advertised precision of this association, which is a number from -4 to -20. For information on setting the advertised precision, see *Configuring an NTP Client* on page 16-6 and *Set the Server's Advertised Precision* on page 16-14.

Leap. The status of leap second insertion for this association. Leap seconds are seconds that are added to the timestamp of an NTP entity to correct accumulated time errors. The possible values are:

00	No warning.
01	Last minute has 61 seconds.
10	Last minute has 59 seconds.
11	Alarm condition (clock not synchronized).

Refid. This is a 32-bit code identifying the particular reference clock. In the case of stratum 0 (unspecified) or stratum 1 (primary reference source), this is a four-octet, left-justified, zero-padded ASCII string. In the case of stratum 2 and greater (secondary reference) this is the four-octet Internet address of the peer selected for synchronization.

Rootdistance. This is a signed fixed-point number indicating the total roundtrip delay to the primary reference source at the root of the synchronization subnet, in seconds. Note that this variable can take on both positive and negative values, depending on clock precision and skew.

Rootdispersion. This is a signed fixed-point number indicating the maximum error relative to the primary reference source at the root of the synchronization subnet, in seconds. Only positive values are possible.

Ppoll. The poll time for this association when it is a peer. This number is the minimum interval between transmitted messages, in seconds as a power of two. For instance, a value of six indicates a minimum interval of 64 seconds.

Hpoll. The poll time for this association when it is a host. This number is the minimum interval between transmitted messages, in seconds as a power of two. For instance, a value of six indicates a minimum interval of 64 seconds.

KeyID. This is an integer identifying the cryptographic key used to generate the message authentication code.

Version. The version of NTP this association is using; the options are **1**, **2**, or **3**.

Association. The number of seconds since this NTP entity was associated with the switch.

Valid. This is an integer counter indicating the valid samples remaining in the filter register. It is used to determine the reachability state of an association, and when the poll interval should be increased or decreased.

Reach. This is a shift register used to determine the reachability status of this peer. The NTP algorithm uses this when determining timestamp information.

Unreach. The number of times this NTP entity was unreachable.

Flash. This field displays the number of error bits from the packet procedure.

Boffset. This field displays the default broadcast delay in seconds.

TTL/mode. This fields displays the Time-to-Live (TTL) time in seconds and the mode (unicast, multicast, or broadcast) of NTP messages sent to a broadcast address. For information on configuring an NTP broadcast address, see *Configuring a Broadcast Time Service* on page 16-13.

Timer. Shows the number of seconds until the next NTP message is sent to an association.

Flags Config. This counter lists what flags have been configured for this NTP entity. For more information about setting flags, see *Set a System Flag (Auth, Bclient, Monitor, Stats)* on page 16-35.

Reference Time. This is the local time, in timestamp format, when the local clock was last updated. If the local clock has never been synchronized, the value is zero.

Originate Timestamp. This is the local time, in timestamp format, of the peer when its last NTP message was sent. If the peer becomes unreachable the value is set to zero.

Receive Timestamp. This is the local time, in timestamp format, when the latest NTP message from the peer arrived. If the peer becomes unreachable the value is set to zero.

Transmit Timestamp. This is the local time, in timestamp format, when the last NTP message was sent from this association.

Filter delay. NTP comes with various filter routines as part of the algorithm that determines timestamp information. This field shows the delay in seconds the NTP algorithm uses to correct for delays caused by messages traversing through the NTP filters.

Filter offset. NTP comes with various filter routines as part of the algorithm that determines timestamp information. This counter indicates the offset of the peer clock relative to the local clock due to filters.

Filter order. The order in which NTP messages pass through filters.

Delay. The currently estimated delay of this remote association, in seconds. This number indicates the roundtrip delay of the peer clock relative to the local clock over the network path between them, in seconds. Note that this variable can take on both positive and negative values, depending on clock precision and skew-error accumulation. This time is determined by the NTP algorithm.

Offset. The currently estimated offset of this remote association, in seconds. This counter indicates the offset of the peer clock relative to the local clock. This time is determined by the NTP algorithm.

Disp. The currently estimated dispersion of this remote association, in seconds. This counter indicates the maximum error of the peer clock relative to the local clock over the network path between them, in seconds. Only positive values greater than zero are possible. This time is determined by the NTP algorithm.

Print Version Number

The **ntpvers** is used to show the version number of the xntp file. To display the version number, enter the **ntpvers** command at the system prompt. A message similar to the following is shown:

```
xntp Fri Apr 9 22:52:46 PDT 1999 (1)
```

Display Local Server Information

The `ntpinfo` command is used to display information about the local switch's implementation of NTP. To view local switch NTP information, enter the `ntpinfo` command at the system prompt. A screen similar to the following is shown:

```

system peer:          0.0.0.0
system peer mode:    unspec
leap indicator:      11
stratum:             16
precision:           -7
root distance:       0.00000 s
root dispersion:     0.00000 s
reference ID:        [0.0.0.0]
reference time:      00000000.00000000 Thu, Feb 7 1936 6:28:16.000
system flags:        monitor stats
frequency:           0.000 ppm
stability:           0.000 ppm
broadcastdelay:      0.003906 s
authdelay:           0.000122 s

```

Field Descriptions

The following section explains the fields shown using the `ntpinfo` command.

System peer. The IP address of the switch.

System peer mode. The peer mode of this remote association. There are five possible modes: symmetric active, symmetric passive, client, server, and broadcast. The displayed mode is assumed if this association becomes the switch's host NTP server. For a description of the modes, see *Display List of Peers the Server Knows About* on page 16-15. For a description of how to configure a peer, see *Configuring a New Peer Association* on page 16-12.

Leap indicator. The status of leap second insertion for this association. Leap seconds are seconds that are added to the timestamp of an NTP entity to correct accumulated time errors. The possible values are:

00	No warning.
01	Last minute has 61 seconds.
10	Last minute has 59 seconds.
11	Alarm condition (clock not synchronized)

Stratum. The stratum level of the remote peer. If this number is **16**, the remote peer has not been synchronized.

Precision. The advertised precision of the switch. It will be a number between -4 and -20.

Root distance. This is a signed fixed-point number indicating the total roundtrip delay to the primary reference source at the root of the synchronization subnet, in seconds. Note that this variable can take on both positive and negative values, depending on clock precision and skew.

Rootdispersion. This is a signed fixed-point number indicating the maximum error relative to the primary reference source at the root of the synchronization subnet, in seconds. Only positive values are possible.

Reference ID. This is a 32-bit code identifying the particular reference clock. In the case of stratum 0 (unspecified) or stratum 1 (primary reference source), this is a four-octet, left-justified, zero-padded ASCII string. In the case of stratum 2 and greater (secondary reference) this is the four-octet Internet address of the peer selected for synchronization.

Reference time. This is the local time at which the local clock was last set or corrected.

System Flags. This counter lists what flags have been configured for this NTP entity. For more information about setting flags, see *Set a System Flag (Auth, Bclient, Monitor, Stats)* on page 16-35.

Frequency. A number indicating the local clock's frequency in relation to a reference clock's Pulse per Second (PPS). If the clock is running in perfect synchronization, this number should be 1. Otherwise, it will be slightly lower or higher in order to compensate for the time difference.

Stability. The residual frequency error (in seconds) remaining after the system frequency correction is applied.

Broadcastdelay. The broadcast delay, in seconds, of this association. For information on how to set the broadcast delay, see *Configuring a Broadcast Time Service* on page 16-13.

Authdelay. The authentication delay, in seconds, of this association. For information on how to set the authentication delay, see *Set the Delay Added to Encryption Time Stamps* on page 16-33.

NTP Statistics Menu

To view the NTP Statistics Menu, enter the **ntstats** command at the system prompt. If you are in verbose mode the NTP configuration menu is displayed. Otherwise, enter a question mark (?) at the prompt to display this menu:

Command	NTP Statistics Menu
ntpstat	display local server statistics
ntppstat	display server statistics associated with particular peer(s)
ntploopinfo	display loop filter information
ntpmem	display peer memory usage statistics
ntpio	display I/O subsystem statistics
ntptimer	display event timer subsystem statistics
ntppreset	reset various subsystem statistics counters
ntppreset	reset stat counters associated with particular peer(s)
ntpctlstat	display packet count statistics from the control module
ntpleap	display the current leap second state
ntpmon	turn the server's monitoring facility on or off
ntpmlist	display data the server's monitor routines have collected

Related Menus:

Ntconfig Ntinfo Ntstats Ntadmin Ntaccess

The main menu options are shown in the **Related Menus** list for quick access if you need to change menus.

Display Local Server Statistics

The **ntpstat** command allow you to view statistics for the local NTP entity (switch). To view statistics, enter the **ntpstat** command at the system prompt. A display similar to the following is displayed:

```

system uptime:           0
time since reset:       0
bad stratum in packet:  0
old version packets:    0
new version packets:    16
unknown version number: 0
bad packet length:      0
packets processed:      0
bad authentication:     0
limitation rejects:     0

```

Field Descriptions

The following section describes the fields displayed using the **ntpstat** command.

system uptime. The number of seconds the local NTP server has been associated with the switch.

time since reset. The number of seconds since the last time the local NTP server was restarted.

bad stratum in packet. The number of NTP packets received that had a corrupted stratum bit in the data of the packet.

old version packets. The number of NTP packets received that were of an older version of NTP (either version 1 or 2).

new version packets. The number of NTP packets received that were version 3 of NTP.

unknown version number. The number of NTP packets received for which the version was unknown (most likely due to packet corruption).

bad packet length. The number of NTP packets received that did not fit the NTP packet structure (most likely due to packet corruption).

packets processed. The total number of NTP packets processed.

bad authentication. The number of NTP packets rejected because they did not meet authentication standards.

limitation rejects. The number of NTP packets rejected because there were restrictions set on their point of origin. For information on setting restrictions, see *Create Restrict Entry/Add Flags to Entry* on page 16-39.

Display Server Statistics Associated with Particular Peer(s)

The **ntppstat** command allows you to view statistics for a specific NTP peer. To view statistics for a peer, enter the **ntppstat** command as shown:

```
ntppstat <ipAddress>
```

where **<ipAddress>** is the address of the peer for which you want to view statistics. For example, to view statistics for a peer with IP address 131.218.18.4, enter the following:

```
ntppstat 131.216.18.4
```

A screen similar to the following displays:

```
remote host           : 131.216.18.4
local interface       : 0.0.0.0
time last received    : 9s
time until next send  : 6s
reachability change   : 2973s
packets sent          : 184
packets received      : 181
bad authentication    : 2
bogus origin          : 2
duplicate             : 6
bad dispersion        : 69
bad reference time    : 1
candidate order       : 1
```

Field Descriptions

The following section describes the fields displayed using the **ntpstat** command.

remote host. The IP address of the host whose statistics you are viewing.

local interface. The local interface address assigned by NTP to the remote association. If this address is **0.0.0.0**, then the local address has yet to be determined.

time last received. The number of seconds since the last NTP message packet was received from another NTP entity in the network.

time until next send. The number of seconds until this NTP peer sends out an NTP message packet.

reachability change. This field displays the number of times this client/server's reachability has changed.

packets sent. The number of NTP message packets this peer has sent out.

packets received. The number of NTP message packets this peer has received.

bad authentication. The number NTP message packets this peer has rejected due to failed authentication.

bogus origin. The number of times a response packet from another NTP entity doesn't match the request packet sent out by this client/server.

duplicate. The number of identical NTP message packets this peer has received.

bad dispersion. The number of packets that were discarded due to overly large error dispersions.

bad reference time. The number of packets that were discarded because the contained reference time didn't match the local peer expectation.

candidate order. A number that represents this client/server's synchronization order. A lower number represents a reliable synchronization source.

Display Loop Filter Information

The loop filter is used to control and correct the phase of timestamps as processed by the local clock. The loop filter examines timestamps sent to and from the local clock and can adjust them to account for natural wander and jitter.

To view the statistics of the loop filter, enter the **ntploop** command at the system prompt. A screen similar to the following is shown:

```

offset:          0.000000 s
frequency:      0.000 ppm
poll adjust:    0
watchdog timer: 0 s
    
```

All of these field variables are determined by the NTP algorithm

Field Descriptions

The following section describes the fields displayed using the **ntploop** command.

offset. The currently estimated offset of this remote association, in seconds. This counter indicates the offset of the peer clock relative to the local clock.

frequency. A number indicating the local clock's frequency in relation to a reference clock's Pulse per Second (PPS). If the clock is running in perfect synchronization, this number should be 1. Otherwise, it will be slightly lower or higher in order to compensate for the time discrepancy between the reference clock and the local clock.

poll adjust. The number of times the poll time has been adjusted to conform to the network.

watchdog timer. The number of seconds since the local clock for this client/server was last adjusted.

Display Peer Memory Usage Statistics

The memory usage for the NTP information on the switch can be displayed using the **ntpmem** command. To view memory information, enter the **ntpmem** command at the system prompt. A screen similar to the following is shown:

```

time since reset: 0
total peer memory: 15
free peer memory: 11
calls to findpeer: 0
new peer allocations: 0
peer demobilizations: 0
hash table counts: 1 0 1 0 0 1 0 0
                   0 0 0 0 0 0 0 0
                   0 0 0 0 0 0 0 0
                   0 0 0 0 0 0 1 0
    
```

Field Descriptions

The following section describes the fields displayed using the **ntpmem** command.

time since reset. The number of seconds since the last reset of NTP (usually a reboot of the switch).

total peer memory. The total number of NTP associations possible for this switch.

free peer memory. The number of available spots on this switch for NTP associations.

calls to findpeer. The number of times the switch sent an NTP packet of any kind to a configured NTP association.

new peer allocations. The number of new NTP associations created since the last restart.

peer demobilizations. The number NTP associations lost since the last restart.

hash table counts. The number of peer tables hashed to the index.

Display I/O Subsystem Statistics

The **ntpio** command allows you to view general statistics on received and transmitted NTP packets for this switch. To view the I/O statistics, enter the **ntpio** command at the system prompt. A screen similar to the following is displayed:

```

time since reset:      0
receive buffers:      10
free receive buffers:  9
used receive buffers:  0
low water refills:    0
dropped packets:      0
ignored packets:      0
received packets:     18
packets sent:         17
packets not sent:     0
interrupts handled:   18
received by int:      18

```

Field Descriptions

The following section describes the fields displayed using the **ntpio** command.

time since reset. The number of seconds since the last restart of NTP.

receive buffers. The number of switch receive buffers currently allocated by this NTP entity.

free receive buffers. The number of free receive buffers.

used receive buffers. The number of receive buffers being used.

low water refills. The number of times memory has been added.

dropped packets. The number of packets discarded due to lack of resources (i.e., memory).

ignored packets. The number of packets ignored by this client/server.

received packets. The total number of NTP packets received by the switch.

packets sent. The total number of NTP packets sent by the switch.

packets not sent. The number of NTP packets generated but not sent due to restrictions. For information on NTP restrictions, see *Create Restrict Entry/Add Flags to Entry* on page 16-39.

interrupts handled. The number of times NTP information was interrupted in the process of transmitting or receiving.

received by int. The number of packets received by interrupts.

Display Event Timer Subsystem Statistics

The **ntptimer** command allows you to view significant NTP events that have occurred on this switch. To view significant NTP events, enter the **ntptimer** command at the system prompt. A screen similar to the following is displayed:

```
time since reset:      0
alarms handled:       0
alarm overruns:       0
calls to transmit:    0
```

Field Descriptions

The following section describes the fields displayed using the **ntptimer** command.

time since reset. The number of seconds since the last reset of NTP.

alarms handled. The number of NTP alarms generated by this switch. NTP alarms occur when the NTP algorithm determines that an NTP entity is out of synchronization.

alarm overruns. The number of times the NTP alarm routine was backed up.

calls to transmit. The number of requests from other NTP entities for information, either configuration, statistical, or timestamp.

Reset Various Subsystem Statistics Counters

To reset the counters displayed for the commands used in the NTP Statistics Menu (**ntpstat**, **ntploopinfo**, **ntpio**, and **ntptimer**), use the **ntppreset** command. To reset the statistics, enter the **ntppreset** command at the system prompt followed by one or more of the following flags:

- **io**
- **sys**
- **mem**
- **timer**
- **auth**
- **allpeers**

A brief message is displayed confirming the command.

Reset Stat Counters Associated With Particular Peer(s)

It is possible to remotely reset statistics for other NTP associations from the switch. To reset statistics for an NTP association, enter the **ntppreset** command as follows:

```
ntppreset <address>
```

where **<address>** is either the domain name or IP address of the remote association. For example, to reset statistics for a peer with IP address 1.1.1.4, enter:

```
ntppreset 1.1.1.4
```

It is possible to reset the statistics for more than one NTP association at a time by adding more than one address to the command. For example, to reset statistics for a peer with IP address 1.1.1.4 and a peer with IP address 1.1.1.5, you would enter:

```
ntppreset 1.1.1.4 1.1.1.5
```

A brief message is displayed confirming the command.

Display Packet Count Statistics from the Control Module

In a comprehensive network-management environment, facilities should exist to perform routine NTP control and monitoring functions. The control module of NTP is responsible for sending and receiving control messages. To display the statistics for the control module, enter the **ntpctlstat** command at the system prompt. A screen similar to the following is shown:

```
time since reset:      0
requests received:    0
responses sent:       0
fragments sent:       0
async messages sent:  0
error msgs sent:      0
total bad pkts:       0
packet too short:     0
response on input:    0
fragment on input:    0
error set on input:   0
bad offset on input:  0
bad version packets:  0
data in pkt too short: 0
unknown op codes:    0
```

Field Descriptions

The following section describes the fields displayed using the **ntpctlstat** command.

time since reset. The number of seconds since the last reset of NTP (usually a switch reboot).

requests received. The number of NTP requests received from any NTP association.

responses sent. The number of NTP messages sent from this switch in response to NTP association requests.

fragments sent. The number of NTP messages sent from this switch that did not contain all appropriate NTP data. This can occur if timestamp information from other NTP entities is judged by this switch to be incorrect.

async messages sent. The number of async trap packets sent.

error msgs sent. The number of error messages sent from the switch to other NTP entities because the switch was not able to respond to the NTP entity's request.

total bad pkts. The total number of packets received that NTP was not able to read.

packet too short. The number of packets received that NTP rejected because the packet was the incorrect length.

response on input. The number of packets received that required the switch to respond to the sender with an NTP message.

fragment on input. The number of packets received that the switch that did not contain complete NTP data.

error set on input. The number of input control packets received with the error bit set.

bad offset on input. The number of NTP timestamps received that the switch disallowed because the added time offset parameter appeared to be incorrect. This can occur if an NTP entity becomes unsynchronized and generates false timestamp information.

bad version packets. The number of packets received where the version number of NTP was undefinable. This is usually caused by packet corruption.

data in pkt too short. The number of packets received that NTP rejected because the packet information was incomplete.

unknown op codes. The number of NTP packets received that contained an unreadable request or information. This is usually caused by packet corruption.

Display the Current Leap Second State

If necessary, NTP adds or subtracts a second from the timestamps sent out on the network to correct for errors in time information. These modifications are called leap seconds. To display leap second information for the switch, enter the **ntpleap** command at the system prompt. A screen similar to the following is displayed:

```
sys.leap:                11 (clock out of sync)
leap.indicator:          00 (leap controlled by lower stratum)
leap.warning:            00 (leap controlled by lower stratum)
leap.bits:               00 (no leap second scheduled)
time to next leap interrupt: 1 s
date of next leap interrupt: Tue, Jul 6 1999 12:38:45
calls to leap process:   0
leap more than month away: 0
leap less than month away: 0
leap less than day away: 0
leap in less than 2 hours: 0
leap happened:           0
```

Field Descriptions

The following section describes the fields displayed using the **ntpleap** command.

sys.leap. The current status of the leap second monitor. There are four possible codes:

00	No warning.
01	Last minute has 61 seconds.
10	Last minute has 59 seconds.
11	Alarm condition (clock not synchronized)

leap.indicator. The number of leap seconds that occurred during the current day.

leap.warning. The number of leap seconds that will occur in the current month.

leap.bits. The number of leap bits set within the last hour.

time to next leap interrupt. A leap interrupt occurs when the NTP algorithm examines the topology of the network and determines if a leap second is needed (it may or may not be necessary at the time of the interrupt). This counter displays seconds until the next interrupt.

date of next leap interrupt. The time, in standard date notation, of the next leap interrupt after the most current leap interrupt is finished.

calls to leap process. The number of times a leap second has been added or subtracted.

leap more than month away. A scheduled leap second insertion more than a month away.

leap less than month away. A scheduled leap second insertion less than a month away.

leap less than day away. A scheduled leap second insertion less than a day away.

leap in less than 2 hours. A scheduled leap second insertion less than two hours away.

leap happened. The date of the last leap second insertion.

Turn the Server's Monitoring Facility On or Off

The Server Monitoring Facility keeps track of all NTP association for this switch. When it is On, it is possible to display a list of all NTP associations. For more information on displaying the Monitoring Facility list of NTP associations, see *Display Data The Server's Monitor Routines Have Collected* on page 16-31.

To turn the Monitoring Facility on or off, enter the **ntpmon** command as shown:

```
ntpmon <on:off>
```

where **<on:off>** is the status of the monitoring facility. For example, to turn the facility on, enter:

```
ntpmon on
```

Display Data The Server's Monitor Routines Have Collected

If the NTP monitoring facility is turned on, you can display a list of all known NTP associations with general information using the **ntpmlist** command.

To display a list of collected monitoring statistics, enter the **ntpmlist** command at the system prompt. A screen similar to the following is displayed:

remote address	port	local address	count	m	ver	drop	last	first
127.0.0.1	1025	127.0.0.1	1	7	3	0	0	0

This table is useful in establishing which entity is associated with the switch, and if entities have formed associations independent of administrator configuration (for example, if a user sets up an association with NTP without notifying the network administrator).

Field Descriptions

The following section describes the fields displayed using the **ntpmlist** command.

remote address. The IP address of the remote association.

port. The port the association was learned on and on which the association communicates with the switch.

◆ **Note** ◆

This is the TCP and UDP definition of a port, not a switch interface port.

local address. The local interface address for this association as created by the NTP configuration on the switch.

count. The number of NTP packets received from this association.

m. The mode the NTP associations uses in relation to the switch.

ver. The version of NTP the association is using (1,2, or 3)

drop. The number of NTP packets received from this association that were dropped (due to restrictions, bad packet data, etc.).

last. The number of seconds since the last NTP message was received from this association.

first. The number of seconds since the first NTP message was received from this association.

NTP Administration Menu

To view the NTP Administration Menu, enter the **ntadmin** command at the system prompt. If you are using verbose mode the NTP configuration menu is displayed. Otherwise, enter a question mark (?) at the prompt to display this menu:

Command	NTP Administration Menu
ntptimeo	set the primary receive time out
ntpdelay	set the delay added to encryption time stamps
ntphost	specify the host whose NTP server we talk to
ntpasswd	specify a password to use for authenticated requests
ntpkeyid	set keyid to use for authenticated requests
ntpkeytype	set key type to use for authenticated requests (des md5)
ntpdisable	clear a system flag (auth, bclient, monitor, stats)
ntpenable	set a system flag (auth, bclient, monitor, stats)

Related Menus:

Ntconfig Ntinfo Ntstats Ntadmin Ntaccess

The main menu options are shown in the **Related Menus** list for quick access if you need to change menus.

Set the Primary Receive Timeout

The **ntptimeo** command allows you to specify the number of milliseconds the server waits for a response to queries before the operation times out. The default is 8000 milliseconds. To change the timeout, enter the **ntptimeo** command as shown:

```
ntptimeo <value>
```

where **<value>** is the number of milliseconds of the new timeout length. For example, to set the timeout value to 3000 milliseconds, enter the following:

```
ntptimeo 3000
```

To view the current timeout setting with out changing it, enter the **ntptimeo** command with no value. A message similar to the following is shown:

```
primary timeout is 6000 ms
```

Set the Delay Added to Encryption Time Stamps

The **ntpdelay** command specifies a set time interval to add to timestamps included in server requests that require authentication. This can be used to enable server configuration over long delay network paths or between machines whose clocks are not synchronized.

To set the delay time, enter the **ntpdelay** command as shown:

```
ntpdelay <value>
```

where **<value>** is the number of milliseconds of the new delay time length. For example, to set the delay value to 30 milliseconds, enter the following:

```
ntpdelay 30
```

To view the current delay setting with out changing it, enter the **ntpdelay** command with no value. A message similar to the following is shown:

```
delay 30 ms
```

Specify the Host Whose NTP Server We Talk To

The **ntpghost** command specifies the name of the NTP server to which server queries are sent. This can be a domain name or an IP address. The default is localhost (the local server).

To change the NTP server for the switch, enter the **ntpghost** command as shown:

```
ntpghost <address>
```

where **<address>** is either the domain name or IP address of the NTP server. For example, to configure the switch to use an NTP server with an IP address of 1.1.1.4, enter:

```
ntpghost 1.1.1.4
```

To view the current NTP server used by the switch, enter the **ntpghost** command at the prompt with no address. A message similar to the following is shown:

```
current host is 1.1.1.4
```

Specify a Password to Use for Authenticated Requests

The **ntpasswd** command allows you to specify a password that must be entered when making configuration requests. The password must correspond to the key configured for use by the NTP server.

To specify a password:

1. Enter the **ntpasswd** command at the system prompt. A prompt displays asking for the Key ID number for the server, as shown:

```
Keyid:
```

Enter the key ID number for the server (as specified in the key file) and press **<return>**.

2. The following prompt appears requesting a password, as shown:

```
Password:
```

Enter the new password. This password is now required before making a configuration request of the server.

Set Key ID to Use for Authenticated Requests

The **ntpkeyid** command allows you to specify a key number to be used to authenticate configuration requests. This must correspond to the key number the server has been configured to use in the key file.

To set a new key ID, enter the **ntpkeyid** command as shown:

```
ntpkeyid <value>
```

where **<value>** is the new key ID number. For example, to set the key ID to 2, you would enter the following:

```
ntpkeyid 2
```

To view the currently configured key ID, enter the **ntpkeyid** command at the prompt and press **<return>**. A message similar to the following is shown:

```
keyid is 2
```

Set Key Type to Use for Authenticated Requests (DES|MD5)

NTP supports two types of encryption: DES or MD5. If you decide to use encryption to authenticate NTP information and configuration requests, you must specify which type of encryption to use.

To specify an encryption type enter the **ntpkeytype** command as shown:

```
ntpkeytype <value>
```

where **<value>** is either DES or MD5. For example, to set the key type to MD5, you would enter:

```
ntpkeytype MD5
```

To view the currently specified key type, enter the **ntpkeytype** command at the system prompt, and press **<return>**. A message similar to the following is displayed:

```
keytype is MD5
```

Set a System Flag (Auth, Bclient, Monitor, Stats)

The **ntpenable** command provides a way to enable various server options by creating flags added to NTP messages sent to the server.

To set a system flag, enter the **ntpenable** command as shown:

```
ntpenable <flag>
```

where **<flag>** is the type of flag the server will receive. There are six flag types that can be set:

auth	This flag causes the server to synchronize with unconfigured peers only if the peer has been correctly authenticated using a trusted key and key identifier. The default for this flag is disabled (off).
bclient	This flag causes the server to listen for a message from a broadcast or multicast server, following which an association is automatically instantiated for that server. The default for this flag is disabled (off).
monitor	This flag enables the monitoring facility. The default for this flag is disabled (off).
stats	This flag enables the statistics facility file generator. The default for this flag is enable (on).

When you have finished specifying a flag, press **<enter>**. A brief message appears to confirm the operation.

Clear a System Flag (Auth, Bclient, Monitor, Stats)

The **ntpdisable** command allows you to remove previously set flags from NTP messages sent to the server.

To disable a flag, enter the **ntpdisable** command as follows:

```
ntpdisable <flag>
```

where **<flag>** is the type of flag the server will receive. There are six flag types that can be set and removed. The flags are described in the section *Set a System Flag (Auth, Bclient, Monitor, Stats)* on page 16-35.

NTP Access Control Menu

To view the NTP Access Control Menu, enter the **ntaccess** command at the system prompt. If you are using verbose mode the NTP configuration menu is displayed. Otherwise, enter a question mark (?) at the prompt to display this menu:

Command	NTP Access Control Menu
ntpreqk	change the request message authentication keyid
ntpctlk	change the control message authentication keyid
ntpckey	add one or more key ID's to the trusted list
ntpvkey	display the trusted key ID list
ntpdkey	remove one or more key ID's from the trusted list
ntpauth	display the state of the authentication code
ntpcres	create restrict entry/add flags to entry
ntpvres	view the server's restrict list
ntpmres	remove flags from a restrict entry
ntpdres	delete a restrict entry
ntpctrap	configure a trap in the server
ntpvtrap	display the traps set in the server
ntpdtrap	remove a trap (configured or otherwise) from the server

Related Menus:

Ntconfig Ntinfo Ntstats Ntadmin Ntaccess

The main menu options are shown in the **Related Menus** list for quick access if you need to change menus.

Change the Request Message Authentication Key ID

There are two types of messages an NTP entity can send to another NTP entity: request and control. Request messages ask for information from the NTP entity such as timestamp information, statistics, etc. It is possible to change the authentication key identifier for request messages sent from the switch to another NTP entity.

To change the authentication key ID, enter the **ntpreqk** command as shown:

```
ntpreqk <value>
```

where **<value>** is the new key ID. Press **<return>**, and a brief message is displayed confirming the operation.

◆ Note ◆

The authentication key ID must match in both the switch sending the message and the switch receiving the message.

Change the Control Message Authentication Key ID

There are two types of messages an NTP entity can send to another NTP entity: request and control. Control messages attempt to change the configuration of the NTP entity in some fashion. It is possible to change the authentication key identifier for control messages sent from the switch to another NTP entity.

To change the authentication key ID, enter the **ntpctlk** command as shown:

```
ntpctlk <value>
```

where **<value>** is the new key ID. Press **<return>**, and a brief message is displayed confirming the operation.

◆ Note ◆

The authentication key ID must match in both the switch sending the message, and the switch receiving the message.

Add One or More Key ID's to the Trusted List

The trusted list in the key file is a list of all keys that are considered authentic and uncompromised. Messages from an NTP entity using one of these keys are accepted and acted upon. It is possible to add a key to the trusted list.

To add a key ID to the trust list in the key file, enter the **ntpckey** command as shown:

```
ntpckey <value>
```

where **<value>** is the new key ID to be added to the trusted list. For example, to add key ID 5 to the trusted list, enter the following:

```
ntpckey 5
```

A brief message is displayed confirming the operation.

◆ Note ◆

Adding a key ID using the **ntpckey** command adds the key to the working version of the key file in the switch's RAM. If you reset the switch or re-initialize NTP, the added key is lost.

Display the Trusted Key ID List

The trusted list in the key file is a list of all keys that are considered authentic and uncompromised. Messages from an NTP entity using one of these keys are accepted and acted upon.

To display a list of the trusted keys for this NTP client or server, enter the **ntpkey** command at the system prompt. A list of the key numbers accepted by this client or server is displayed. For more information on authentication, see *NTP and Authentication* on page 16-4.

Remove One or More Key ID's from the Trusted List

The trusted list in the key file is a list of all keys that are considered authentic and uncompromised. Messages from an NTP entity using one of these keys are accepted and acted upon. It is possible to remove a key from the trusted list.

To remove a key ID from the trusted list, enter the **ntpdkey** command as shown:

```
ntpdkey <value>
```

where **<value>** is the new key ID to be remove from the trusted list. For example, to remove key ID 5 from the trusted list, enter the following:

```
ntpdkey 5
```

A brief message is displayed confirming the operation.

◆ Note ◆

Removing a key ID using the **ntpdkey** command removes the key from the working version of the key file in the switch's RAM. If you reset the switch or re-initialize NTP, the removed key is reinstated.

Display the State of the Authentication Code

The **ntpauth** command allows you to look at the statistics of the authentication routine. These statistics consist of counters for various functions of the authentication code.

To view the statistics of the authentication code, enter the **ntpauth** command at the system prompt. A screen similar to the following is shown:

```
time since reset:      0
key lookups:          0
keys not found:       0
uncached keys:        0
encryptions:          0
decryptions:          0
```

Field Descriptions

The following sections explains the fields displayed using the **ntpauth** command.

time since reset. The number of seconds since the last restart of the switch.

key lookups. The number of times the switch has examined the key file to find a key.

keys not found. The number of times the switch failed to find a key in its key file.

uncached keys. The number of keys added to the key file using the **ntpckey** command.

encryptions. The number of times the switch sent NTP messages or information out in encrypted form.

decryptions. The number of times the switch received NTP messages of information that was encrypted, and successfully decrypted the information.

Create Restrict Entry/Add Flags to Entry

It is possible to place restriction flags on specific NTP entities in relation to the switch. Restriction flags prevent messages or information coming from the NTP entity from affecting the switch.

To create a restriction flag, enter the **ntpcres** command as shown:

```
ntpcres <address> <mask> <restriction>
```

where **<address>** is the IP address of the NTP entity, **<mask>** is the entity's subnet mask, and **<restriction>** is the specific flag you want to place on the entity. For example to put an **ignore** restriction on an entity with address 1.1.1.1 and a subnet mask of 255.255.0.0, enter the following:

```
ntpcres 1.1.1.1 255.255.0.0 ignore
```

The following is a list of possible restriction flags that can be used:

ignore	Ignore all packets from hosts which match this entry. If this flag is specified neither queries nor time server polls will be responded to.
noquery	Ignore all NTP information queries and configuration requests from the source. Time service is not affected.
nomodify	Ignore all NTP information queries and configuration requests that attempt to modify the state of the server (i.e., run time reconfiguration). Queries which return information are permitted.
notrap	Decline to provide control message trap service to matching hosts. The trap service is a subsystem of the control message protocol which is intended for use by remote event logging programs.
lowpriotrap	Declare traps set by matching hosts to be low priority. The number of traps a server can maintain is limited (the current limit is 3). Traps are usually assigned on a first come, first serve basis, with later trap requestors being denied service. This flag modifies the assignment algorithm by allowing low priority traps to be overridden by later requests for normal priority traps. For more information on setting traps see <i>Configure a Trap in the Server</i> on page 16-41
noserve	Ignore NTP packets other than information queries and configuration requests. In effect, time service is denied, though queries may still be permitted.
nopeer	Provide stateless time service to polling hosts, but do not allocate peer memory resources to these hosts even if they otherwise might be considered useful as future synchronization partners.
notrust	Treat these hosts normally in other respects, but never use them as synchronization sources.

limited	These hosts are subject to a limitation of the number of clients from the same net. Net in this context refers to the IP notion of net (class A, class B, class C, etc.). Only the first client limit hosts that have shown up at the server and that have been active during the last client limit period (in seconds) are accepted. Requests from other clients from the same net are rejected. Only time request packets are taken into account. Query packets sent by the ntpq and xntpd programs are not subject to these limits. A history of clients is kept using the monitoring capability of xntpd. Thus, monitoring is always active as long as there is a restriction entry with the limited flag. For more information on enabling monitoring, see <i>Turn the Server's Monitoring Facility On or Off</i> on page 16-31.
ntpport	This is actually a match algorithm modifier, rather than a restriction flag. Its presence causes the restriction entry to be matched only if the source port in the packet is the standard NTP UDP port (123). Both ntpport and non-ntpport may be specified. The ntpport is considered more specific and is sorted later in the list.

View the Server's Restrict List

The **ntpvres** command allows you to view a list of all the configured restrictions for the switch. To view a list of configured restriction, enter the **ntpvres** command at the system prompt. A screen similar to the following appears:

address	mask	count	flags
0.0.0.0	0.0.0.0	12	none
127.0.0.1	255.255.255.255	0	ntpport, ignore

Field Descriptions

The following section describes the fields displayed with the **ntpvres** command.

address. The IP address of the NTP entity for which flags have been configured.

mask. The subnet mask of the NTP entity for which flags have been configured.

count. The number of NTP messages from the NTP entity that have been affected by the configured flags.

flags. The flags configured for this NTP entity. For a description of all possible flags, see *Create Restrict Entry/Add Flags to Entry* on page 16-39.

Remove Flags from a Restrict Entry

It is possible to place restriction flags on specific NTP entities in relation to the switch. Restriction flags prevent messages or information coming from the NTP entity from affecting the switch.

To remove a restriction flag from an NTP entity, enter the **ntpmres** command as shown:

```
ntpmres <address> <mask> <restriction>
```

where **<address>** is the IP address of the NTP entity, **<mask>** is the entity's subnet mask, and **<restriction>** is the specific flag you want to remove from the entity. For example, to remove an **ignore** restriction from an entity with address 1.1.1.1 and a subnet mask of 255.255.0.0, enter the following:

```
ntpmres 1.1.1.1 255.255.0.0 ignore
```

Delete a Restrict Entry

To remove an entry completely from the restriction list, enter the **ntpdres** command in the following manner:

```
ntpdres <address> <mask>
```

where **<address>** is the IP address of the NTP entity, and **<mask>** is the entity's subnet mask. For example to remove an entity with address 1.1.1.1 and a subnet mask of 255.255.0.0, enter the following:

```
ntpmres 1.1.1.1 255.255.0.0
```

This entity will no longer be listed in the restriction list and has no restriction flags placed on messages it sends to the switch.

Configure a Trap in the Server

The **ntpctrap** command allows you to set a trap receiver for the given address and port number. The trap receiver will log event messages and other information for the server in a log file.

To create a trap receiver, enter the **ntpctrap** command in the following manner:

```
ntpctrap <address> [<port>] [<interface>]
```

where address is the IP address of the switch. There are two optional items you can specify:

port The port on the switch used for sending NTP messages. If no port is specified, a default port of 18447 is used.

◆ Note ◆

This is the TCP and UDP definition of a port, not a switch interface port.

interface The local interface address for this NTP entity. If no interface is specified, the interface for the local NTP entity is used. For more information on interface addresses, see *Display Peer Summary Information* on page 16-16.

Display the Traps Set in the Server

The **ntpvttrap** command allows you to view a list of trap receivers set for the server. To view the trap list, enter the **ntpvttrap** command at the system prompt. A display similar to the following is shown:

```
address 127.0.0.1, port 18447
interface: 0.0.0.5, configured
set for 0 seconds, last set 0 seconds ago
sequence 1, number of resets 1
```

Field Descriptions

The following section describes the fields shown with the **ntpvttrap** command.

address. The address of the server where the trap was set.

port. The port on which the server is listening for NTP messages.

◆ Note ◆

This is the TCP and UDP definition of a port, not a switch interface port.

interface. The local interface address of the NTP server.

set for n seconds. The time the trap was initially set.

last set. The time in seconds from when the last trap was set for this server.

sequence. The number of times the trap was set.

number of resets. The number of times the trap has been reset.

Remove a Trap (Configured or Otherwise) from the Server

The **ntpdtrap** command allows you to remove a trap receiver for the given address. The trap receiver will log event messages and other information for the server in a log file.

To delete a trap receiver, enter the **ntpdtrap** command in the following manner:

```
ntpdtrap <address> [<port>] [<interface>]
```

where address is the IP address of the switch. There are two optional items you can specify:

port. The port on the switch used for sending NTP messages.

◆ Note ◆

This is the TCP/IP and UDP definition of a port, not a switch interface port.

interface. The local interface address for this NTP entity. For more information on interface addresses, see *Display Peer Summary Information* on page 16-16.

17 SNMP (Simple Network Management Protocol)

Introduction

Simple Network Management Protocol (SNMP) is an application layer protocol that allows network devices to exchange management information. SNMP works by sending messages, called protocol data units (PDUs), to network devices. Network administrators use SNMP to monitor network performance and to solve network problems.

An SNMP-managed network is comprised of three fundamental parts: agents, managed devices, and network management systems (NMSs). An agent, which resides within a managed device (i.e., a switch), is responsible for translating its local knowledge of management information into a form compatible with SNMP. When certain defined asynchronous events occur within a switch, the managed device sends traps, using the SNMP protocol, to a designated NMS. The NMS then views and monitors the switch's information through management software applications such as HP Open View or X-Vision.

SNMP parameters and traps are configurable through the **snmpc** command. For more information on this command, refer to *Configuring SNMP Parameters and Traps* on page 17-2. You can view SNMP statistics through the **snmps** command. For more information on this command, refer to *Viewing SNMP Statistics* on page 17-8. Both of these commands are also listed on the **Networking** menu.

Configuring SNMP Parameters and Traps

The **snmpc** command allows you to configure SNMP parameters and set traps that will be sent to network management stations. The **snmpc** command also enables you to add, modify, or delete SNMP parameters. The **snmpc** command is listed under the **Networking** menu. For more information about the networking menu, see Chapter 30, “IP Routing.” To configure SNMP parameters, enter the following command:

```
snmpc
```

A screen similar to the following displays:

```
SNMP current configuration:
```

```
1) Process SNMP Packets - enabled
2) Set Community Name   - public
3) Get Community Name   - public
4) Trap Community Name  - public
5) Broadcast Traps      - disabled
6) 0 Unicast Traps      - disabled
```

```
(save/quit/cancel)
```

```
:
```

- To change a value, enter the number corresponding to that value, an equal sign (=), and the new value. For example, to enable broadcast traps, enter **5=enabled**.
- To clear an entry, specify the value as a period (.), as in **2=.** Note that true/false values and enabled/disabled values cannot be cleared.
- To save all your modifications, enter **save**.
- To cancel all your modifications, enter **Cancel** or **Ctrl-C**.
- To view the parameters currently configured, enter a question mark (?).

1) Process SNMP Packets

To enable or disable SNMP, enter 1, an equal sign (=), and the enable or disable command. The following is an example:

```
1=enable
```

2) Set Community Name

The Set Community Name variable is a password (up to 16 characters) that enables NMS stations to read and write objects through SNMP. The default Set Community Name is “public,” which allows all NMS stations read access to readable objects. If you want to specify a Set Community Name password, enter a 2, an equal sign (=), and the new Set Community Name. The following is an example:

```
2=alpha
```

◆ Note ◆

Set Community Names with spaces must be enclosed in quotations (e.g., “test lab”).

3) Get Community Name

The Get Community Name variable is a password (up to 16 characters) that enables NMS stations to read objects defined in the MIBs. The default Get Community Name is “public,” which allows all NMS station read access to readable objects. If you want to specify a Get Community Name password, enter a **2**, an equal sign (=), and the new Get Community Name. The following is an example display:

```
2=beta
```

◆ **Note** ◆

Get Community Names with spaces must be enclosed in quotations (e.g., “**data center**”).

4) Trap Community Name

The Trap Community Name (up to 16 characters) is a password that enables NMS stations to collect traps (provided the NMS stations are configured with the same corresponding Trap Community Name). The default Trap Community Name is “public,” which allows the switch to send traps to all NMS stations configured with the Trap Community Name, “public.” If you want to specify a Trap Community Name password, enter a **4**, an equal sign (=), and the new Trap Community Name. The following is an example display.

```
4=trap1
```

◆ **Note** ◆

Trap Community Names with spaces must be enclosed in quotations (e.g., “**trap 1**”).

5) Broadcast Traps

When broadcast traps are enabled, the switch transmits traps to all NMS stations in the default group. If you enable this parameter, unicast traps (see option 6 below) will automatically be disabled. The default for broadcast traps is **disabled**. To enable broadcast traps, enter the following command:

```
5=enabled
```

The following prompt displays:

```
UDP destination port (162):
```

Enter the UDP destination port for the traps. UDP port 162 is the default port and is commonly used for traps; however, the destination port can be re-defined to accommodate a network management station using a nonstandard port.

◆ **Note** ◆

The destination port configured here must correspond to the UDP destination port configured at the receiving network management station(s).

6) Unicast Traps

When unicast traps are enabled, the switch transmits traps only to the IP address(es) defined in the **snmpc** list below this field.

◆ **Note** ◆

If both broadcast and unicast traps are disabled, then the switch does not transmit any traps.

If you enable this parameter, broadcast traps (see option 5 above) will automatically be disabled. The default for unicast traps is disabled. To enable unicast traps, enter the following command:

6=enabled

Configuring a New Network Management Station

- a. To define a new network management station, enter 7, followed by an equal sign (=), and the IP address of the network management station to receive traps. You can define a maximum of ten network management stations. They must be numbered sequentially from 7 through 16. If network management stations are already shown on the display for this menu, use the next highest number to add another station. The following is an example of how to define the first network management station:

7=123.12.1.1

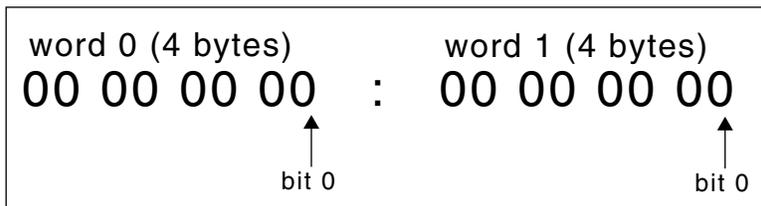
The following prompt displays:

Enter trap mask words 0:1 (ffffff.ffffff):

Each trap in the switch is assigned a mask that consists of “words”. The mask value **ffffff.ffffff** indicates that *all* traps are enabled for words 0 and 1. If you want to accept this default (all traps enabled for words 0 and 1), press **<Enter>**. If you want to enable one or more specific traps for words 0 and 1, you must calculate their bit configurations and enter the new mask value at the prompt. Trap types and their bit positions are listed in the tables beginning on page 17-11.

Here is a sample configuration for setting a combination of traps.

Bit Configurations for Setting Traps



Example: To set a combination of trap types, add the hex values of the bits as follows:

Trap Type	Bit Settings	
	Word 0	Word 1
tempAlarm	00 00 00 00	: 00 00 00 01
risingAlarm	00 00 40 00	: 00 00 00 00
fallingAlarm	00 00 80 00	: 00 00 00 00
portPartitioned	00 00 00 00	: 00 00 02 00
Total =	00 00 C0 00	: 00 00 02 01

You would then enter the total mask value of the traps, as follows:

Enter trap mask words 0:1 (ffffff:ffffff): 0000C000:00000201

This setting would enable only these four traps for words 0 and 1.

- b. The following prompt displays:

Enter trap mask words 2:3 (ffffff:ffffff):

Enter the trap type(s) for words 2 and 3. If you want to accept the default (all traps enabled for words 2 and 3), press **<Enter>**. To set one or more specific traps, again calculate the bit configurations and enter the new mask value at the prompt.

- c. The following prompt displays:

Enter destination port (162):

Enter the UDP destination port for the traps configured above. If you choose the default in field four, port 162, press **<Enter>** at the prompt.

- d. The following prompt displays:

NMS state (on):

Indicate whether or not traps will be sent to this Network Management Station (the NMS defined in step a). If the NMS state is enabled (**on**), the NMS will be notified of traps. Press **<Enter>** to accept the default (**on**). If the NMS state is disabled (**off**), the NMS will not be notified of traps.

- e. The following prompt displays:

Special Access? (no): yes

Select whether or not this Network Management Station has special access. If you enter **yes**, this NMS will have administrative privileges such as modifying, deleting, or adding to other trap entries as well as its own. Without special access, an NMS can only update its own entry. If you choose the default, **no**, simply press **<Enter>** at the prompt.

Save your configuration by typing **save** and then **<Enter>**.

- f. After you have saved your configuration, the prompt re-displays. The above entries will create an NMS number 6 in the list. Traps will be sent to the IP address specified for that NMS station (provided the NMS state is **on** and unicast traps are **enabled**).

To view your new SNMP configuration, enter the **snmpc** command. The following is a sample display of the output from the **snmpc** command after the above sample configuration:

SNMP current configuration:

```
1) Process SNMP Packets - enabled
2) Set Community Name  - admin
3) Get Community Name  - public
4) Trap Community Name - trap1
5) Broadcast Traps     - disabled
6) 1 Unicast Traps     - enabled
7) NMS IP address      - 123.12.1.1           /162 --bfffffff:ffffff (on) (SA)
                                                -- ffffffff:ffffff
```

(save/quit/cancel)

:

The values that appear to the immediate right of the NMS IP address are: the UDP destination port number (**162**), the trap bit masks (**fffffff.bfffffff**), the functional state of the NMS (**on**), and the special access (**SA**) status (this does not appear if you selected **no** for special access in step above).

To add network management stations to this current SNMP configuration, enter the next highest entry number from the last defined NMS. For example, if you wanted to add another NMS to the above sample configuration, you would enter the following:

8=123.22.2.2

Please note that any additional NMS entries must have a unique IP address. Repeat steps **b** through **f** to continue configuring additional NMS entries. Once you save your configuration and re-enter the **snmpc** command at the prompt, the screen refreshes to include the new NMS entry. The following is a sample display:

SNMP current configuration:

```

1) Process SNMP Packets - enabled
2) Set Community Name  - public
3) Get Community Name  - public
4) Trap Community Name - public
5) Broadcast Traps     - disabled
6) 1 Unicast Traps     - enabled
7) NMS IP address      - 123.12.1.1      /162 -- ffffffff:bfffffff (on) (SA
                                           -- ffffffff:ffffffff)
8) NMS IP address      - 123.22.2.2      /162 -- ffffffff:ffffffff (on)
                                           -- ffffffff:ffffffff

(save/quit/cancel)
:
```

- g.** To delete an IP address added to this list, enter the NMS index number of the entry followed by the decimal (.) character. The following example would delete the NMS IP address listed at number **8**.

8=.

Viewing SNMP Statistics

The **snmps** command is used to display SNMP statistics. The command displays the SNMP activities since the last time the switch was powered on, or since the last Reset was executed. It also displays a list of the current traps.

The **snmps** command is listed on the **Networking** menu. For more information about the networking menu, see Chapter 30, "IP Routing." To display SNMP statistics, enter the following command:

```
snmps
```

A screen similar to the following displays:

SNMP Statistics		
	In	Out
Total Packets	67	67
Bad Versions	0	
Bad Community Names	0	
Bad Community Use	0	
Bad Type Discards:	0	
ASN Parse Errors	0	
Too Big Errors	0	0
No Such Name Errors	0	1
Bad Value Errors	0	0
Read Only Errors	0	0
General Errors	0	0
Total Variable Requests	186	
Total Set Variable Requests	0	
Get Requests	17	0
Get Next Requests	50	0
Set Requests	0	0
Get Responses	0	67
Authentication Trap Enables:	0	
Traps	0	0

Trap generation is ENABLED to these management stations:

```
198.206.1.1 /162 -- ffffffff:bfffffff (on)
198.2.1.1   /162 -- ffffffff:7fffffff (off) (SA)
```

Total Packets

The total number of packets received and sent.

Bad Versions

The total number of SNMP messages delivered to the switch SNMP protocol entity that were for an unsupported SNMP version.

Bad Community Names

The total number of SNMP message names delivered to the switch SNMP protocol entity that used an unknown SNMP community name.

Bad Community Use

The total number of SNMP messages delivered to the SNMP protocol entity which represented an SNMP operation that was not allowed by the SNMP community named in the message.

Bad Type Discards

The total number of SNMP entries discarded because the request type was not recognized.

ASN Parse Errors

The total number of ASN.1 or BER errors encountered by the SNMP protocols entity when decoding received SNMP Messages.

Too Big Errors

The total number of SNMP PDUs delivered to the SNMP protocol entity with a value in the error-status field of 'tooBig'.

No Such Name Error

The total number of SNMP PDUs delivered to the SNMP protocol entity with value in the error-status field of 'noSuchName'.

Bad Value Errors

The total number of valid SNMP PDUs delivered to the SNMP protocol entity with a value in the error-status field of 'readOnly.' It is a protocol error to generate an SNMP PDU that contains the value 'readOnly' in the error-status field; as such this object is provided as a means of detecting incorrect implementations of the SNMP.

Read Only Errors

The total number of valid SNMP PDUs delivered to the SNMP protocol entity for with an error-status field value of 'Read Only'.

General Errors

The total number of SNMP PDUs delivered to the switch SNMP protocol entity with an error-status field value of 'GenError'.

Total Variable Requests

The total number of MIB objects from which Requests have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.

Total Set Variable Requests

The total number of MIB objects from which Requests have been retrieved successfully by the SNMP entity as the result of receiving valid SNMP Set-Request PDUs.

Get Requests

The total number of SNMP Get-Request PDUs accepted and processed by the switch SNMP protocol entity.

Get Next Requests

The total number of SNMP Get-Next PDUs accepted and processed by the switch SNMP protocol entity.

Set Requests

The total number of SNMP Set-Request PDUs which have been accepted and processed by the switch SNMP protocol entity.

Get Responses

The total number of SNMP Response PDUs accepted and processed by the switch SNMP protocol entity.

Authentication Trap Enables

Indicates whether the SNMP agent Enable process is permitted to generate authentication-failure traps. The value of this object overrides any configuration information, providing a means to enable all authentication-failure traps.

Traps

The number of SNMP Trap PDUs generated by the SNMP protocol entity. Traps are broadcast only.

Traps are broadcast only

This appears if traps are set to broadcast. The address is the broadcast address of the default VLAN of AutoTracker group 1.

Trap generation is ENABLED to these management stations

This appears if you have used the **snmpc** command to set up one or more management stations to receive traps. The trap tables on the following pages list the traps that are currently supported.

Trap Tables

The following table is a summary list of the supported SNMP traps and their values.

Trap or Mask Name	Object ID	Bit Position	Hex Value	Page
coldStart	1.3.6.1.2.1.11.0	(word 0) 0	(word 0) 1	17-15
warmStart	1.3.6.1.2.1.11.1	(word 0) 1	(word 0) 2	17-16
linkDown	1.3.6.1.2.1.11.2	(word 0) 2	(word 0) 4	17-16
linkUp	1.3.6.1.2.1.11.3	(word 0) 3	(word 0) 8	17-17
authentication failure	1.3.6.1.2.1.11.4	(word 0) 4	(word 0) 10	17-17
egpNeighborLoss	1.3.6.1.2.1.11.5	(word 0) 5	(word 0) 20	17-18
frDLCIStatusChange	1.3.6.1.2.1.11.7	(word 0) 7	(word 0) 80	17-18
ipxTrapCircuitDown	1.3.6.1.4.1.23.2.5.5.1	(word 0) 8	(word 0) 100	17-19
ipxTrapCircuitUp	1.3.6.1.4.1.23.2.5.5.2	(word 0) 9	(word 0) 200	17-19
newRoot	1.3.6.1.2.17.0.1	(word 0) 10	(word 0) 400	17-19
topologyChange	1.3.6.1.2.17.0.2	(word 0) 11	(word 0) 800	17-20
atmfVpcChange	1.3.6.1.4.1.353.0.1	(word 0) 12	(word 0) 1000	17-21
atmfVccChange	1.3.6.1.4.1.353.0.2	(word 0) 13	(word 0) 2000	17-22
rising Alarm	1.3.6.1.2.16.0.1	(word 0) 14	(word 0) 4000	17-23
falling Alarm	1.3.6.1.2.16.0.2	(word 0) 15	(word 0) 8000	17-24
dsx3LineStatusChange	1.3.6.1.2.1.10.20.15.0.1	(word 0) 16	(word 1) 1 0000	17-25
dsx1LineStatusChange	1.3.6.1.2.1.10.18.15.0.1	(word 0) 17	(word 1) 2 0000	17-26
POS3_STAT_CHANGE_MASK *		(word 0) 19	(word 0) 8 0000	
IMA_FAILURE_ALARM_MASK *		(word 0) 20	(word 0) 10 0000	
SYSLOG_TRAP_MASK *		(word 0) 29	(word 0) 2000 0000	
NMS_MASTER_MASK *		(word 0) 30	(word 0) 4000 0000	
NMS_TRAP_DISABLE_MASK *		(word 0) 31	(word 0) 8000 0000	
* This mask name does not necessarily match the trap name.				
tempAlarm	1.3.6.1.4.1.800.3.1.1.4.0.1	(word 1) 0	(word 1) 1	17-27
moduleChange	1.3.6.1.4.1.800.3.1.1.4.0.2	(word 1) 1	(word 1) 2	17-28

Trap Tables

<i>Trap or Mask Name</i>	<i>Object ID</i>	<i>Bit Position</i>	<i>Hex Value</i>	<i>Page</i>
powerEvent	1.3.6.1.4.1.800.3.1.1.4.0.3	(word 1) 2	(word 1) 4	17-29
controllerEvent	1.3.6.1.4.1.800.3.1.1.4.0.4	(word 1) 3	(word 1) 8	17-30
loginViolation	1.3.6.1.4.1.800.3.1.1.4.0.5	(word 1) 4	(word 1) 10	17-31
macVlanViolation	1.3.6.1.4.1.800.3.1.1.4.0.6	(word 1) 5	(word 1) 20	17-31
macDuplicatePort	1.3.6.1.4.1.800.3.1.1.4.0.7	(word 1) 6	(word 1) 40	17-32
portLinkUpEvent	1.3.6.1.4.1.800.3.1.1.4.0.8	(word 1) 7	(word 1) 80	17-33
portLinkDownEvent	1.3.6.1.4.1.800.3.1.1.4.0.9	(word 1) 8	(word 1) 100	17-34
portPartitioned	1.3.6.1.4.1.800.3.1.1.4.0.10	(word 1) 9	(word 1) 200	17-35
portRecordMismatch	1.3.6.1.4.1.800.3.1.1.4.0.11	(word 1) 10	(word 1) 400	17-36
groupChange	1.3.6.1.4.1.800.3.1.1.4.0.14	(word 1) 13	(word 1) 2000	17-37
vlanChange	1.3.6.1.4.1.800.3.1.1.4.0.15	(word 1) 14	(word 1) 4000	17-38
portMove	1.3.6.1.4.1.800.3.1.1.4.0.16	(word 1) 15	(word 1) 8000	17-39
moduleResetReload	1.3.6.1.4.1.800.3.1.1.4.0.17	(word 1) 16	(word 1) 1 0000	17-40
systemEvent	1.3.6.1.4.1.800.3.1.1.4.0.18	(word 1) 17	(word 1) 2 0000	17-41
vlanRouteTableFull	1.3.6.1.4.1.800.3.1.1.4.0.19	(word 1) 18	(word 1) 4 0000	17-42
sapTableFull	1.3.6.1.4.1.800.3.1.1.4.0.20	(word 1) 19	(word 1) 8 0000	17-42
atmSSCOPstate	1.3.6.1.4.1.800.3.1.1.4.0.21	(word 1) 20	(word 1) 10 0000	17-43
ilmiState	1.3.6.1.4.1.800.3.1.1.4.0.22	(word 1) 21	(word 1) 20 0000	17-43
atmConnection	1.3.6.1.4.1.800.3.1.1.4.0.23	(word 1) 22	(word 1) 40 0000	17-44
atmService	1.3.6.1.4.1.800.3.1.1.4.0.24	(word 1) 23	(word 1) 80 0000	17-45
dlciNew	1.3.6.1.4.1.800.3.1.1.4.0.27	(word 1) 26	(word 1) 400 0000	17-46
dlciDel	1.3.6.1.4.1.800.3.1.1.4.0.28	(word 1) 27	(word 1) 800 0000	17-47
dlciUp	1.3.6.1.4.1.800.3.1.1.4.0.29	(word 1) 28	(word 1) 1000 0000	17-48
dlciDn	1.3.6.1.4.1.800.3.1.1.4.0.30	(word 1) 29	(word 1) 2000 0000	17-49
portManualForwarding Mode	1.3.6.1.4.1.800.3.1.1.4.0.31	(word 1) 30	(word 1) 4000 0000	17-50
fdciCFStateChange	1.3.6.1.4.1.800.3.1.1.4.0.32	(word 1) 31	(word 1) 8000 0000	17-51
duplicateIPAddress	1.3.6.1.4.1.800.3.1.1.4.0.35	(word 2) 2	(word 2) 4	17-52
duplicateMACAddress	1.3.6.1.4.1.800.3.1.1.4.0.36	(word 2) 3	(word 2) 8	17-53
healthThresholdRising	1.3.6.1.4.1.800.3.1.1.4.0.37	(word 2) 4	(word 2) 10	17-54
healthThresholdFalling	1.3.6.1.4.1.800.3.1.1.4.0.38	(word 2) 5	(word 2) 20	17-54

Trap or Mask Name	Object ID	Bit Position	Hex Value	Page
healthThresholdDevice	1.3.6.1.4.1.800.3.1.1.4.0.39	(word 2) 6	(word 2) 40	17-55
healthThresholdModule	1.3.6.1.4.1.800.3.1.1.4.0.40	(word 2) 7	(word 2) 80	17-55
xylanXIPXMAPPort StatusChange	1.3.6.1.4.1.800.3.1.1.4.0.41	(word 2) 8	(word 2) 100	17-56
xylanSIPXMAPPortState Change	1.3.6.1.4.1.800.3.1.1.4.0.42	(word 2) 9	(word 2) 200	17-57
clkBusLineStateChange	1.3.6.1.4.1.800.3.1.1.4.0.45	(word 2) 10	(word 2) 400	17-60
xylanXIPGMAPPFailed Update	1.3.6.1.4.1.800.3.1.1.4.0.44	(word 2) 11	(word 2) 800	17-59
avlAuthAttempt	1.3.6.1.4.1.800.3.1.1.4.0.43	(word 2) 16	(word 2) 1 0000	17-58
mcpStatisticsOverflow	1.3.6.1.4.1.800.3.1.1.4.0.67	(word 2) 18	(word 2) 4 0000	17-62
mcpShortCut	1.3.6.1.4.1.800.3.1.1.4.0.68	(word 2) 19	(word 2) 8 0000	17-66
mcpIngressRetryTime	1.3.6.1.4.1.800.3.1.1.4.0.69	(word 2) 20	(word 2) 10 0000	17-67
vrrpTrapNewMasterOut	1.3.6.1.2.1.46.1.3.1.0.3	(word 2) 21	(word 2) 20 0000	17-68
vrrpAuthFailure	1.3.6.1.2.1.46.1.3.1.0.4	(word 2) 22	(word 2) 40 0000	17-69
blind-violation	1.3.6.1.4.1.800.3.1.1.1.0.46	(word 2) 23	(word 2) 80 0000	17-61
mpcStatisticsOverflow	1.3.6.1.4.1.800.3.1.1.1.0.47	(word 2) 18	(word 2) 4 0000	17-62
fddiLerFlagChange	1.3.6.1.4.1.800.3.1.1.4.0.65	(word 3) 0	(word 3) 1	17-63
fddiCLTFailCntIncr	1.3.6.1.4.1.800.3.1.1.4.0.66	(word 3) 1	(word 3) 2	17-64
oamVCAIS	1.3.6.1.4.1.800.3.1.1.4.0.71	(word 3) 10	(word 3) 400	17-70
oamVCRDI	1.3.6.1.4.1.800.3.1.1.4.0.72	(word 3) 11	(word 3) 800	17-71
oamVCLOC	1.3.6.1.4.1.800.3.1.1.4.0.73	(word 3) 12	(word 3) 1000	17-72
oamVCUnsuccessLoop	1.3.6.1.4.1.800.3.1.1.4.0.74	(word 3) 13	(word 3) 2000	17-73
oamVPAIS	1.3.6.1.4.1.800.3.1.1.4.0.75	(word 3) 14	(word 3) 4000	17-74
oamVPRDI	1.3.6.1.4.1.800.3.1.1.4.0.76	(word 3) 15	(word 3) 8000	17-75
oamVPLOC	1.3.6.1.4.1.800.3.1.1.4.0.77	(word 3) 16	(word 3) 1 0000	17-76
oamVPUnsuccessLoop	1.3.6.1.4.1.800.3.1.1.4.0.78	(word 3) 17	(word 3) 2 0000	17-77
accountEvent	1.3.6.1.4.1.800.3.1.1.4.0.86	(word 3) 21	(word 3) 20 0000	17-78
Over1Alarm	1.3.6.1.4.1.800.3.1.1.4.0.87	(word 3) 22	(word 3) 40 0000	17-78
Under1Event	1.3.6.1.4.1.800.3.1.1.4.0.88	(word 3) 23	(word 3) 80 0000	17-79
Over2Alarm	1.3.6.1.4.1.800.3.1.1.4.0.89	(word 3) 24	(word 3) 100 0000	17-79

Trap Tables

<i>Trap or Mask Name</i>	<i>Object ID</i>	<i>Bit Position</i>	<i>Hex Value</i>	<i>Page</i>
Under2Event	1.3.6.1.4.1.800.3.1.1.4.0.90	(word 3) 25	(word 3) 200 0000	17-80
Over3Alarm	1.3.6.1.4.1.800.3.1.1.4.0.91	(word 3) 26	(word 3) 400 0000	17-80
Under3Event	1.3.6.1.4.1.800.3.1.1.4.0.92	(word 3) 27	(word 3) 8000 0000	17-81
NoDeviceAlarm	1.3.6.1.4.1.800.3.1.1.4.0.93	(word 3) 28	(word 3) 1000 0000	17-81
FileAlarm	1.3.6.1.4.1.800.3.1.1.4.0.94	(word 3) 29	(word 3) 2000 0000	17-82
lecStateChangeEvent	1.3.6.1.4.1.800.3.1.1.4.0.96	(word 2) 26	(word 2) 40 0000	17-83

SNMP Standard Traps

This section lists the standard traps that are defined within RFC (MIB) documents. These traps signify events as they occur on common network devices. The following information on traps is provided in the tables.

Trap. The object name of the trap as it is defined in the corresponding MIB (Management Information Base). Alcatel supports standardized and proprietary MIBS.

Object ID. The SNMP object identifier (OID) for this trap.

Description. A brief explanation describing the circumstances under which a specific trap is generated.

Bit Position. The trap's specific position in a bit mask (a bit mask is a binary notation which represents a combination of all four trap words). By mapping a specific trap to its binary position, you can determine whether or not a trap is enabled. For example, a trap is enabled if its corresponding bit is set to 1 and disabled if its corresponding bit is set to 0.

Word. A word is a set of four consecutive bytes within a system's memory. Alcatel allocates a total of four words for trap representation. Each of the 32 bit positions within a word corresponds to a specific trap. The first word, Word 0, contains only standard traps as they are defined within RFC (MIB) documents. Words 1, 2, and 3 contain Alcatel-specific traps.

Hex Value. The resulting hexadecimal value of the bit mask.

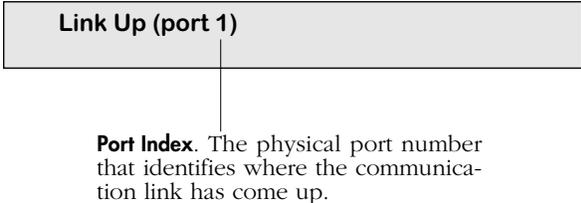
Trap Text and Variable Description. Trap text is a brief statement containing additional information that can help you narrow down the source of the trap, such as slot/port numbers, module types, and MAC addresses (variable descriptions have been added for your convenience). When a specific trap is triggered, it may display in various text formats, depending on the software application through which it is viewed. The trap text in the following tables are examples of trap text displayed through the HP OpenView Alarm Log and the Traps window in X-Vision Discovery. For more information on X-Vision, see the on-line documentation included with the application.

Trap	coldStart
Object ID	1.3.6.1.2.1.11.0
Description	The sending protocol entity is re-initializing itself such that the agent's configuration or the protocol entity implementation may be altered.
Bit Position (Word 0)	0
Hex Value (Word 0)	1
Trap Text and Variable Descriptions	Cold Start

Trap Tables

Trap	warmStart
Object ID	1.3.6.1.2.1.11.1
Description	The sending protocol entity is re-initializing itself such that neither the agent's configuration nor the protocol entity implementation may be altered.
Bit Position (Word 0)	1
Hex Value (Word 0)	2
Trap Text and Variable Descriptions	Warm Start

Trap	linkDown
Object ID	1.3.6.1.2.1.11.2
Description	The sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.
Bit Position (Word 0)	2
Hex Value (Word 0)	4
Trap Text and Variable Descriptions	<div data-bbox="391 1354 972 1423" style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; display: inline-block; margin-bottom: 10px;">Link Down (port 1)</div> <p>Port Index. The physical port number that identifies the failed communication link.</p>

Trap	linkUp
Object ID	1.3.6.1.2.1.11.3
Description	The sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.
Bit Position (Word 0)	3
Hex Value (Word 0)	8
Trap Text and Variable Descriptions	 <p>Port Index. The physical port number that identifies where the communication link has come up.</p>

Trap	authenticationFailure
Object ID	1.3.6.1.2.1.11.4
Description	The sending protocol entity is the addressee of a protocol message that is not properly authenticated.
Bit Position (Word 0)	4
Hex Value (Word 0)	10
Trap Text and Variable Descriptions	Authentication Failure

Trap	egpNeighborLoss
Object ID	1.3.6.1.2.1.11.5
Description	An EGP neighbor for whom the sending protocol entity was an EGP peer has been marked down and the peer relationship no longer exists.
Bit Position (Word 0)	5
Hex Value (Word 0)	20
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;">Neighbor Loss (neigh addr 192.168.10.1)</div> <p style="text-align: center; margin-top: 10px;">Neighbor IP Address. The IP address of this entry's EGP neighbor.</p>

Trap	frDLCIStatusChange
Object ID	1.3.6.1.2.1.11.6
Description	This trap is sent when the indicated virtual circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states. However, if the reason for the state change is due to the DLCMI going down, traps should not be generated for each DLCI.
Bit Position (Word 0)	7
Hex Value (Word 0)	80
Variable Description	<p>frCircuitIfIndex - The ifIndex value of the ifEntry this virtual circuit is layered into.</p> <p>frcircuitDlci - The DLCI for this virtual circuit.</p> <p>frCircuitState - Indicates whether this virtual circuit is active or inactive.</p>

Trap	ipxTrapCircuitDown
Object ID	1.3.6.1.4.1.23.2.5.5.1
Description	This trap indicates that the specified circuit has gone down.
Bit Position (Word 0)	8
Hex Value (Word 0)	100
Variable Description	ipxCircSysInstance - The identifier of this instance of IPX. ipxCircIndex - The identifier of this circuit, for this instance of IPX.

Trap	ipxTrapCircuitUp
Object ID	1.3.6.1.4.1.23.2.5.5.2
Description	This trap indicates that the specified circuit has come up.
Bit Position (Word 0)	9
Hex Value (Word 0)	200
Variable Description	ipxCircSysInstance - The identifier of this instance of IPX. ipxCircIndex - The identifier of this circuit, for this instance of IPX.

Trap Type	newRoot
Object ID	1.3.6.1.2.1.17.0.1
Description	Sent by a bridge that became the new root of the Spanning Tree.
Bit Position (Word 0)	10
Hex Value (Word 0)	400
Trap Text and Variable Descriptions	Spanning Tree: A new agent has become the root of the Spanning Tree.

Trap Tables

Trap	topologyChange
Object ID	1.3.6.1.2.1.17.0.2
Description	A bridge's configured ports either transitioned from Learning state to Forwarding state or from Forwarding state to Blocking state. This trap will not be sent if a newRoot trap was sent for the same transition.
Bit Position (Word 0)	11
Hex Value (Word 0)	800
Trap Text and Variable Descriptions	Spanning Tree: A configured port's state has transitioned.

Trap	atmfVpcChange
Object ID	1.3.6.1.4.1.353.0.1
Description	Either a permanent VPC was added or deleted at this ATM interface, or an existing VPC was modified.
Bit Position (Word 0)	12
Hex Value (Word 0)	1000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>A permanent VPC has been added or deleted at this ATM Interface, or the attributes of an existing VPC have been modified (index 0, Vpi 2, Status 3)</p> </div> <p>Port Index. The port number of this ATM interface. Valid values range from 0 to 2147483647.</p> <p>VPI. The Virtual Path Identifier at this ATM interface. Valid values range from 0 to 4095.</p> <p>Operational Status. The present operating status of the VPC. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 unknown 2 end2endUp 3 end2endDown 4 localUpEnd2endUnknown 5 localDown

Trap	atmfVccChange
Object ID	1.3.6.1.4.1.353.0.2
Description	Either a permanent VCC was added or deleted at this ATM interface, or an existing VCC was modified.
Bit Position (Word 0)	13
Hex Value (Word 0)	2000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>A permanent VCC has been added or deleted at this ATM Interface, or the attributes of an existing VPC have been modified (index 0, Vpi 2, Vci 6, status 3)</p> </div> <p>Operational Status. The present operational status of the VCC. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 unknown 2 end2endUp 3 end2endDown 4 localUpEnd2endUnknown 5 localDown <p>Port Index. The port number which identifies this ATM interface. Valid values range from 0 to 2147483647.</p> <p>VPI. The Virtual Channel Identifier at this ATM interface. Valid values range from 0 to 4095. For virtual interfaces, this value has no meaning and is set to zero.</p> <p>VCI. The Virtual Channel Identifier at this ATM interface. Valid values range from 0 to 65535. For virtual interfaces, this value has no meaning and is set to zero.</p>

Trap	risingAlarm
Object ID	1.3.6.1.2.1.16.0.1
Description	The value of an Ethernet statistical variable (i.e., a member of the Ethernet statistics group as defined by RFC 1757) has exceeded its rising threshold. The variable's rising threshold and whether it will generate an SNMP trap for this condition are configured by a network management station running RMON.
Bit Position (Word 0)	14
Hex Value (Word 0)	4000
Trap Text and Variable Descriptions	<p>Variable. The MIB object identifier for the variable being sampled.</p> <p>Alarm Index. An index value for this entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device.</p> <p>An RMON alarm entry crossed its rising threshold (index 25 var 2 type 1 value 201 rising threshold 200)</p> <p>Value. The value of the statistic during the last sampling period. For example, if the sample method is Delta Value, this value will be the difference between the samples at the beginning and end of the period. If the sample method is Absolute Value, this value will be the sampled value at the end of the period. This is the value that is compared with the rising threshold.</p> <p>Rising Threshold. A threshold for the sampled statistic. This trap is generated when the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold.</p> <p>After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the Falling Threshold value.</p> <p>Sampling Method. The method of sampling the selected variable and calculating the value for comparison with the thresholds. Possible values are integers 1 and 2:</p> <ol style="list-style-type: none"> 1 Absolute Value. The value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. 2 Delta Value. The value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.

Trap	fallingAlarm
Object ID	1.3.6.1.2.1.16.0.2
Description	The value of an Ethernet statistical variable (i.e., a member of the Ethernet statistics group as defined by RFC 1757) has dipped below its falling threshold. The variable's falling threshold and whether it will generate an SNMP trap for this condition are configured by a network management station running RMON.
Bit Position (Word 0)	15
Hex Value (Word 0)	8000
Trap Text and Variable Descriptions	<p>Variable. The MIB object identifier for the variable being sampled.</p> <p>Alarm Index. An index value for this entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device.</p> <div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; text-align: center;"> <p>An RMON alarm entry crossed its falling threshold (index 25 var 2 type 1 value 100 falling threshold 9)</p> </div> <p>Value. The value of the statistic during the last sampling period. For example, if the sample method is Delta Value, this value will be the difference between the samples at the beginning and end of the period. If the sample method is Absolute Value, this value will be the sampled value at the end of the period. This is the value that is compared with the falling threshold.</p> <p>Sampling Method. The method of sampling the selected variable and calculating the value for comparison with the thresholds. Possible values are:</p> <ol style="list-style-type: none"> 1 Absolute Value. The value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. 2 Delta Value. The value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds. <p>Falling Threshold. A threshold for the sampled statistic. This trap is generated when the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was more than this threshold.</p> <p>After a falling event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches the Rising Threshold value.</p>

Trap Type	dsx3LineStatusChange
Object ID	1.3.6.1.2.1.10.30.15.0.1
Description	The value of an instance dsx3LineStatus changed.
Bit Position (Word 0)	16
Hex Value (Word 1)	1 0000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; text-align: center; margin-bottom: 10px;"> Line Status Change (line status 1, last change 4) </div> <p>DSX3 Line Status. The line status of the interface. It contains loopback, failure, received alarm, and transmitted alarm information. Valid values range from 1 to 8191.</p> <p>Last Change. The last value of MIB II's sysUpTime object at the time this DS3 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, this value is zero.</p>

Trap	dsx1LineStatusChange
Object ID	1.3.6.1.2.1.10.18.15.0.1
Description	The value of an instance dsx1LineStatus changed.
Bit Position (Word 0)	17
Hex Value (Word 1)	2 0000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; margin-bottom: 10px; text-align: center;"> Line Status Change (line status 1, last change 2) </div> <p>DSX1 Line Status. The line status of the interface. It contains loopback, failure, received alarm, and transmitted alarm information. Valid values range from 1 to 8191.</p> <p>Last Change. The last value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, this value is zero.</p>

Extended Traps

This section lists Alcatel-specific traps. These extended traps are generated specifically by Alcatel switch devices.

Trap Type	tempAlarm
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.1
Description	The temperature sensor(s) have detected a temperature in the chassis that exceeds the threshold. These sensors are physically located on the MPM module, but can detect temperature changes throughout the chassis.
Bit Position (Word 1)	0
Hex Value (Word 1)	1
Trap Text and Variable Descriptions	Temperature Sensor has changed state to Over Threshold

Trap Type	moduleChange		
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.2		
Description	A module was either inserted or removed from the chassis. In some cases, this trap may also be generated when a module is reset.		
Bit Position (Word 1)	1		
Hex Value (Word 1)	2		
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p align="center">Module was inserted or removed from chassis (slot 4, subunit 1, type 10)</p> </div> <p>Slot Number. The slot number on the front of the chassis where this module was inserted or removed.</p> <p>Submodule Type. Indicates the submodule that was inserted or removed. Typically this value will be 1, meaning the base module was inserted or removed. If this value is 2, then HSM module 1 was moved. If this value is 3, then HSM module 2 was moved.</p> <p>Module Type. Indicates the module type that was inserted or removed. The following integers are valid values:</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; vertical-align: top;"> <ul style="list-style-type: none"> 4 HSM 5 MPM 6 ESM 8-port 10BASE-T 7 ESM 16-port 8 TSM 6-port UTP/STP 9 FSM FDDI module 10 FSM CDDI module 11 ESM 4-port 12 ASM .5 MB multi-mode 13 ESM 12-port 10BASE-T 14 ESM 6-port universal module 15 MPM version II 16 ATM DS-3 17 FSM FDDI single mode 18 ASM .5 MB single mode 19 ASM UTP 20 ESM 8-port fiber </td> <td style="width: 50%; vertical-align: top;"> <ul style="list-style-type: none"> 21 ESM 12-port Telco 22 TSM fiber 23 ASM 2 MB multi-mode 24 ASM 2 MB single mode 25 WSM 26 WSM BRI 27 HSM2 base slot type 28 PizzaSwitch reserved 29 TSM CD-6 30 ASM 2 MB single mode 33 10Meg Ether Universal 34 ATM E3 (European) 35 Ether 100 FX Sngl Full Dup 36 Ether 100 FX Multi Full Dup 37 Ether 100 TX CU Full Dup 39 PizzaPort (repeater) </td> </tr> </table>	<ul style="list-style-type: none"> 4 HSM 5 MPM 6 ESM 8-port 10BASE-T 7 ESM 16-port 8 TSM 6-port UTP/STP 9 FSM FDDI module 10 FSM CDDI module 11 ESM 4-port 12 ASM .5 MB multi-mode 13 ESM 12-port 10BASE-T 14 ESM 6-port universal module 15 MPM version II 16 ATM DS-3 17 FSM FDDI single mode 18 ASM .5 MB single mode 19 ASM UTP 20 ESM 8-port fiber 	<ul style="list-style-type: none"> 21 ESM 12-port Telco 22 TSM fiber 23 ASM 2 MB multi-mode 24 ASM 2 MB single mode 25 WSM 26 WSM BRI 27 HSM2 base slot type 28 PizzaSwitch reserved 29 TSM CD-6 30 ASM 2 MB single mode 33 10Meg Ether Universal 34 ATM E3 (European) 35 Ether 100 FX Sngl Full Dup 36 Ether 100 FX Multi Full Dup 37 Ether 100 TX CU Full Dup 39 PizzaPort (repeater)
<ul style="list-style-type: none"> 4 HSM 5 MPM 6 ESM 8-port 10BASE-T 7 ESM 16-port 8 TSM 6-port UTP/STP 9 FSM FDDI module 10 FSM CDDI module 11 ESM 4-port 12 ASM .5 MB multi-mode 13 ESM 12-port 10BASE-T 14 ESM 6-port universal module 15 MPM version II 16 ATM DS-3 17 FSM FDDI single mode 18 ASM .5 MB single mode 19 ASM UTP 20 ESM 8-port fiber 	<ul style="list-style-type: none"> 21 ESM 12-port Telco 22 TSM fiber 23 ASM 2 MB multi-mode 24 ASM 2 MB single mode 25 WSM 26 WSM BRI 27 HSM2 base slot type 28 PizzaSwitch reserved 29 TSM CD-6 30 ASM 2 MB single mode 33 10Meg Ether Universal 34 ATM E3 (European) 35 Ether 100 FX Sngl Full Dup 36 Ether 100 FX Multi Full Dup 37 Ether 100 TX CU Full Dup 39 PizzaPort (repeater) 		

Trap Type	powerEvent
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.3
Description	A power supply was either inserted or removed from the chassis, or there is a problem with the power supply. This trap is also generated when a power supply is switched on or off.
Bit Position (Word 1)	2
Hex Value (Word 1)	4
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p style="text-align: center;">Power Supply was inserted or removed from chassis or has a problem (ps1 3, ps2 2)</p> </div> <p>Power Supply Status. The current state of power supply 1 (ps1) and power supply 2 (ps2). The following integers are valid values:</p> <ul style="list-style-type: none"> 1 Unknown. 2 No power supply present. 3 Power supply okay. 4 Power supply bad.

Trap Type	controllerEvent
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.4
Description	A chassis controller (MPM) lost or gained the state of the master.
Bit Position (Word 1)	3
Hex Value (Word 1)	8
Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; margin-bottom: 10px; display: inline-block;"> Chassis controller (MPM) lost or gained master control (slot 1, state 3) </div> <p>Slot. The slot number of the MPM that has lost or gained master control. Valid values are:</p> <ul style="list-style-type: none"> 1 Slot Number 1 2 Slot Number 2 <p>State. The current state of the MPM in the slot. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 Unknown 2 Invalid 3 Master 4 Slave

Trap Type	loginViolation
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.5
Description	A login attempt for the User Interface (UI) failed due to an incorrect login ID or an invalid password. Three (3) consecutive unsuccessful attempts will trigger this alarm.
Bit Position (Word 1)	4
Hex Value (Word 1)	10
Trap Text and Variable Descriptions	Login Attempt failed due to invalid ID or password.

Trap Type	macVlanViolation
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.6
Description	Data from a MAC address that previously came from one a port with a VLAN-ID different from the VLAN where the frame had been previously received.
Bit Position (Word 1)	5
Hex Value (Word 1)	20
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; display: inline-block; margin-bottom: 10px;"> Receiving Port VLAN ID has changed (bridge address 0036589adf01) </div> <p>MAC Address. The MAC address from which data has come from two different ports in two different groups.</p>

Trap Tables

Trap Type	macDuplicatePort
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.7
Description	Data from a MAC address that previously came from a source port different from the port where the frame previously was received although they both ports belong to the same VLAN.
Bit Position (Word 1)	6
Hex Value (Word 1)	40
Trap Text and Variable Descriptions	<div data-bbox="425 709 1258 783" style="border: 1px solid black; padding: 5px; text-align: center;">VLAN Receiving Port has changed (bridge address 00145221cd02)</div> <p>MAC Address. The MAC address from which data has come from two different ports in the same group.</p>

Trap Type	portLinkUpEvent																																												
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.8																																												
Description	A physical, logical, or virtual port was enabled. These ports may be enabled through the UI or Switch Manager. Note that if you enable a physical port, any associated logical and virtual ports will also be enabled. And if you enable a logical port, such as an ATM service, associated virtual ports will be enabled.																																												
Bit Position (Word 1)	7																																												
Hex Value (Word 1)	80																																												
Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; text-align: center;">Physical, logical or virtual port was enabled (slot 2 IF 2 type 203 instance 1)</div> <p>Slot Number. The slot number for the module that contains this port.</p> <p>Port Number. The port number on this module that was enabled.</p> <p>Port Type. The physical type of this port. The following integers are valid values:</p> <table style="margin-left: 40px;"> <tr><td>1</td><td>Unknown</td></tr> <tr><td>2</td><td>Other</td></tr> <tr><td>3</td><td>Router</td></tr> <tr><td>4</td><td>Bridge</td></tr> <tr><td>5</td><td>Trunk</td></tr> <tr><td>6</td><td>ATM trunk port</td></tr> <tr><td>7</td><td>ATM LAN Emulation port</td></tr> <tr><td>8</td><td>Classical IP</td></tr> <tr><td>9</td><td>ATM MUX</td></tr> <tr><td>203</td><td>Ethernet 10BASE-T</td></tr> <tr><td>204</td><td>Ethernet 100BASE-T</td></tr> <tr><td>205</td><td>Token Ring 4 mbs</td></tr> <tr><td>206</td><td>Token Ring 16 mbs</td></tr> <tr><td>207</td><td>FDDI</td></tr> <tr><td>208</td><td>CDDI</td></tr> <tr><td>209</td><td>ATM 25 mbs</td></tr> <tr><td>210</td><td>ATM 50 mbs</td></tr> <tr><td>211</td><td>DS-1</td></tr> <tr><td>212</td><td>DS-3</td></tr> <tr><td>213</td><td>OC-3</td></tr> <tr><td>214</td><td>OC-12</td></tr> <tr><td>215</td><td>OC-48</td></tr> </table> <p>Physical Instance. The specific instance of this slot/port/type. In most cases this value will be 1 (only one instance of the port), but an ATM port may have multiple instances. Possible values range from 1 to 254.</p>	1	Unknown	2	Other	3	Router	4	Bridge	5	Trunk	6	ATM trunk port	7	ATM LAN Emulation port	8	Classical IP	9	ATM MUX	203	Ethernet 10BASE-T	204	Ethernet 100BASE-T	205	Token Ring 4 mbs	206	Token Ring 16 mbs	207	FDDI	208	CDDI	209	ATM 25 mbs	210	ATM 50 mbs	211	DS-1	212	DS-3	213	OC-3	214	OC-12	215	OC-48
1	Unknown																																												
2	Other																																												
3	Router																																												
4	Bridge																																												
5	Trunk																																												
6	ATM trunk port																																												
7	ATM LAN Emulation port																																												
8	Classical IP																																												
9	ATM MUX																																												
203	Ethernet 10BASE-T																																												
204	Ethernet 100BASE-T																																												
205	Token Ring 4 mbs																																												
206	Token Ring 16 mbs																																												
207	FDDI																																												
208	CDDI																																												
209	ATM 25 mbs																																												
210	ATM 50 mbs																																												
211	DS-1																																												
212	DS-3																																												
213	OC-3																																												
214	OC-12																																												
215	OC-48																																												

Trap Type	portLinkDownEvent																																												
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.9																																												
Description	A physical, logical, or virtual port was disabled. These ports may be disabled through the UI or Switch Manager. Note that if you disable a physical port, any associated logical and virtual ports will also be disabled. And if you disable a logical port, such as an ATM service, associated virtual ports will also be disabled.																																												
Bit Position (Word 1)	8																																												
Hex Value (Word 1)	100																																												
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Physical, logical or virtual port was disabled (slot 2 IF 2 type 203 instance 1) </div> <p>Slot Number. The slot number for the module that contains this port.</p> <p>Port Number. The port number on this module that was disabled.</p> <p>Port Type. The physical type of this port. The following integers are valid values:</p> <table style="margin-left: 40px;"> <tr><td>1</td><td>Unknown</td></tr> <tr><td>2</td><td>Other</td></tr> <tr><td>3</td><td>Router</td></tr> <tr><td>4</td><td>Bridge</td></tr> <tr><td>5</td><td>Trunk</td></tr> <tr><td>6</td><td>ATM trunk port</td></tr> <tr><td>7</td><td>ATM LAN Emulation port</td></tr> <tr><td>8</td><td>Classical IP</td></tr> <tr><td>9</td><td>ATM MUX</td></tr> <tr><td>203</td><td>Ethernet 10BASE-T</td></tr> <tr><td>204</td><td>Ethernet 100BASE-T</td></tr> <tr><td>205</td><td>Token Ring 4 mbs</td></tr> <tr><td>206</td><td>Token Ring 16 mbs</td></tr> <tr><td>207</td><td>FDDI</td></tr> <tr><td>208</td><td>CDDI</td></tr> <tr><td>209</td><td>ATM 25 mbs</td></tr> <tr><td>210</td><td>ATM 50 mbs</td></tr> <tr><td>211</td><td>DS-1</td></tr> <tr><td>212</td><td>DS-3</td></tr> <tr><td>213</td><td>OC-3</td></tr> <tr><td>214</td><td>OC-12</td></tr> <tr><td>215</td><td>OC-48</td></tr> </table> <p>Physical Instance. The specific instance of this slot/port/type. In most cases this value will be 1 (only one instance of the port), but an ATM port may have multiple instances. Possible values range from 1 to 254.</p>	1	Unknown	2	Other	3	Router	4	Bridge	5	Trunk	6	ATM trunk port	7	ATM LAN Emulation port	8	Classical IP	9	ATM MUX	203	Ethernet 10BASE-T	204	Ethernet 100BASE-T	205	Token Ring 4 mbs	206	Token Ring 16 mbs	207	FDDI	208	CDDI	209	ATM 25 mbs	210	ATM 50 mbs	211	DS-1	212	DS-3	213	OC-3	214	OC-12	215	OC-48
1	Unknown																																												
2	Other																																												
3	Router																																												
4	Bridge																																												
5	Trunk																																												
6	ATM trunk port																																												
7	ATM LAN Emulation port																																												
8	Classical IP																																												
9	ATM MUX																																												
203	Ethernet 10BASE-T																																												
204	Ethernet 100BASE-T																																												
205	Token Ring 4 mbs																																												
206	Token Ring 16 mbs																																												
207	FDDI																																												
208	CDDI																																												
209	ATM 25 mbs																																												
210	ATM 50 mbs																																												
211	DS-1																																												
212	DS-3																																												
213	OC-3																																												
214	OC-12																																												
215	OC-48																																												

Trap Type	portPartitioned
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.10
Description	The physical port detected jabber (i.e., the port has transitioned through enable/disable states more than 50 times in the past 200 ms). Jabber may be produced by a bad port connection, such as a faulty cable.
Bit Position (Word 1)	9
Hex Value (Word 1)	200
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p style="text-align: center;">Port jabber detected (enabled/disabled faster than 50 times in 200 ms) (slot 2, IF 2, type 203, instance 1)</p> </div> <p>Slot Number. The slot number for the module that contains this port.</p> <p>Port Number. The port number on this module that detected jabber.</p> <p>Physical Instance. The specific instance of this slot/port/type. In most cases this value will be 1 (only one instance of the port), but an ATM port may have multiple instances. Possible values range from 1 to 254.</p> <p>Port Type. The physical type of this port. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 Unknown 2 Other 3 Router 4 Bridge 5 Trunk 6 ATM trunk port 7 ATM LAN Emulation port 8 Classical IP 9 ATM MUX 203 Ethernet 10BASE-T 204 Ethernet 100BASE-T 205 Token Ring 4 mbs 206 Token Ring 16 mbs 207 FDDI 208 CDDI 209 ATM 25 mbs 210 ATM 50 mbs 211 DS-1 212 DS-3 213 OC-3 214 OC-12 215 OC-48

Trap Type	portRecordMismatch																																												
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.11																																												
Description	The port configuration is different from the previous configuration. Typically this trap is generated when a NIC of one type is swapped for a different type (i.e., Ethernet for FDDI, ATM for Token Ring, etc.).																																												
Bit Position (Word 1)	10																																												
Hex Value (Word 1)	400																																												
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Port configuration different than previously detected (slot 2, IF 2, type 203, instance 1)</p> </div> <p>Slot number. The slot number for the module that contains this port.</p> <p>Port number. The port number on this module that has a different configuration.</p> <p>Port Type. The physical type of this port. The following integers are valid values:</p> <table style="margin-left: 20px;"> <tr><td>1</td><td>Unknown</td></tr> <tr><td>2</td><td>Other</td></tr> <tr><td>3</td><td>Router</td></tr> <tr><td>4</td><td>Bridge</td></tr> <tr><td>5</td><td>Trunk</td></tr> <tr><td>6</td><td>ATM trunk port</td></tr> <tr><td>7</td><td>ATM LAN Emulation port</td></tr> <tr><td>8</td><td>Classical IP</td></tr> <tr><td>9</td><td>ATM MUX</td></tr> <tr><td>203</td><td>Ethernet 10BASE-T</td></tr> <tr><td>204</td><td>Ethernet 100BASE-T</td></tr> <tr><td>205</td><td>Token Ring 4 mbs</td></tr> <tr><td>206</td><td>Token Ring 16 mbs</td></tr> <tr><td>207</td><td>FDDI</td></tr> <tr><td>208</td><td>CDDI</td></tr> <tr><td>209</td><td>ATM 25 mbs</td></tr> <tr><td>210</td><td>ATM 50 mbs</td></tr> <tr><td>211</td><td>DS-1</td></tr> <tr><td>212</td><td>DS-3</td></tr> <tr><td>213</td><td>OC-3</td></tr> <tr><td>214</td><td>OC-12</td></tr> <tr><td>215</td><td>OC-48</td></tr> </table> <p>Physical Instance. The specific instance of this slot/port/type. In most cases this value will be 1 (only one instance of the port), but an ATM port may have multiple instances. Possible values range from 1 to 254.</p>	1	Unknown	2	Other	3	Router	4	Bridge	5	Trunk	6	ATM trunk port	7	ATM LAN Emulation port	8	Classical IP	9	ATM MUX	203	Ethernet 10BASE-T	204	Ethernet 100BASE-T	205	Token Ring 4 mbs	206	Token Ring 16 mbs	207	FDDI	208	CDDI	209	ATM 25 mbs	210	ATM 50 mbs	211	DS-1	212	DS-3	213	OC-3	214	OC-12	215	OC-48
1	Unknown																																												
2	Other																																												
3	Router																																												
4	Bridge																																												
5	Trunk																																												
6	ATM trunk port																																												
7	ATM LAN Emulation port																																												
8	Classical IP																																												
9	ATM MUX																																												
203	Ethernet 10BASE-T																																												
204	Ethernet 100BASE-T																																												
205	Token Ring 4 mbs																																												
206	Token Ring 16 mbs																																												
207	FDDI																																												
208	CDDI																																												
209	ATM 25 mbs																																												
210	ATM 50 mbs																																												
211	DS-1																																												
212	DS-3																																												
213	OC-3																																												
214	OC-12																																												
215	OC-48																																												

Trap Type	groupChange
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.14
Description	A Group was either created or deleted through the UI or Switch Manager.
Bit Position (Word 1)	13
Hex Value (Word 1)	2000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; margin-bottom: 10px; text-align: center;"> Group created or deleted (vlan 2 admin status 4) </div> <p>Group number. The Group number that has been created or deleted.</p> <p>Administrative Status. The administrative status for this group. Possible options are:</p> <ol style="list-style-type: none"> 1 Disabled. All ports in this Group are disabled. 2 Enabled. All ports in this Group are enabled. 3 Deleted. This Group was deleted, and all attached virtual ports and routers are detached and deleted. 4 Created. This Group has been created. 5 Modify. This Group has been modified.

Trap Type	vlanChange
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.15
Description	A VLAN was either created or deleted through the UI or Switch Manager.
Bit Position (Word 1)	14
Hex Value (Word 1)	4000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; margin-bottom: 10px; text-align: center;"> VLAN Change created or deleted (group 2, admin status 4) </div> <p>Group number. The Group number to which this VLAN belongs.</p> <p>Administrative status. The administrative status for this VLAN. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 Enabled. 2 Disabled. 3 Deleted. This VLAN was deleted. 4 Created. This Group has been created. 5 Modify. This Group has been modified.

Trap Type	portMove																																												
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.16																																												
Description	The specified port has moved from a Group or has had its configuration changed.																																												
Bit Position (Word 1)	15																																												
Hex Value (Word 1)	8000																																												
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Port VLAN, group or configuration change (slot 2, IF 8, type 4, instance 1) </div> <p>Slot number. The slot number for the module that contains this port.</p> <p>Port number. The port number on this module that was changed.</p> <p>Port Type. The physical type of this port. The following integers are valid values:</p> <table style="margin-left: 40px;"> <tr><td>1</td><td>Unknown</td></tr> <tr><td>2</td><td>Other</td></tr> <tr><td>3</td><td>Router</td></tr> <tr><td>4</td><td>Bridge</td></tr> <tr><td>5</td><td>Trunk</td></tr> <tr><td>6</td><td>ATM trunk port</td></tr> <tr><td>7</td><td>ATM LAN Emulation port</td></tr> <tr><td>8</td><td>Classical IP</td></tr> <tr><td>9</td><td>ATM MUX</td></tr> <tr><td>203</td><td>Ethernet 10BASE-T</td></tr> <tr><td>204</td><td>Ethernet 100BASE-T</td></tr> <tr><td>205</td><td>Token Ring 4 mbs</td></tr> <tr><td>206</td><td>Token Ring 16 mbs</td></tr> <tr><td>207</td><td>FDDI</td></tr> <tr><td>208</td><td>CDDI</td></tr> <tr><td>209</td><td>ATM 25 mbs</td></tr> <tr><td>210</td><td>ATM 50 mbs</td></tr> <tr><td>211</td><td>DS-1</td></tr> <tr><td>212</td><td>DS-3</td></tr> <tr><td>213</td><td>OC-3</td></tr> <tr><td>214</td><td>OC-12</td></tr> <tr><td>215</td><td>OC-48</td></tr> </table> <p>Physical Instance. The specific instance of this slot/port/type. In most cases this value will be 1 (only one instance of the port), but an ATM port may have multiple instances. Possible values range from 1 to 254.</p>	1	Unknown	2	Other	3	Router	4	Bridge	5	Trunk	6	ATM trunk port	7	ATM LAN Emulation port	8	Classical IP	9	ATM MUX	203	Ethernet 10BASE-T	204	Ethernet 100BASE-T	205	Token Ring 4 mbs	206	Token Ring 16 mbs	207	FDDI	208	CDDI	209	ATM 25 mbs	210	ATM 50 mbs	211	DS-1	212	DS-3	213	OC-3	214	OC-12	215	OC-48
1	Unknown																																												
2	Other																																												
3	Router																																												
4	Bridge																																												
5	Trunk																																												
6	ATM trunk port																																												
7	ATM LAN Emulation port																																												
8	Classical IP																																												
9	ATM MUX																																												
203	Ethernet 10BASE-T																																												
204	Ethernet 100BASE-T																																												
205	Token Ring 4 mbs																																												
206	Token Ring 16 mbs																																												
207	FDDI																																												
208	CDDI																																												
209	ATM 25 mbs																																												
210	ATM 50 mbs																																												
211	DS-1																																												
212	DS-3																																												
213	OC-3																																												
214	OC-12																																												
215	OC-48																																												

Trap	moduleResetReload																								
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.17																								
Description	The specified module has been either reset or reloaded. A reload may occur during a firmware download.																								
Bit Position (Word 1)	16																								
Hex Value (Word 1)	1 0000																								
Trap Text and Variable Descriptions	<p>Submodule Type. Indicates the submodule that was reset or reloaded. Typically this value will be 1, meaning the base module was reset or reloaded. If this value is 2, then HSM module 1 was affected. If this value is 3, then HSM module 2 was affected.</p> <p>.Slot number. The slot number of the module that was reset or reloaded.</p> <div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; text-align: center;"> Module reset or reloaded by chassis manager (slot 4 subunit 1 type 6 status 3) </div> <p>Module Type. Indicates the module type that was reset or reloaded. The following integers are valid values:</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">4 HSM</td> <td style="width: 50%;">13 ESM 12-port 10BASE-T</td> </tr> <tr> <td>5 MPM</td> <td>14 ESM 6-port universal module</td> </tr> <tr> <td>6 ESM 8-port 10BASE-T</td> <td>15 MPM version II</td> </tr> <tr> <td>7 ESM 16-port</td> <td>16 ATM DS-3</td> </tr> <tr> <td>8 TSM 6-port UTP/STP</td> <td>17 FSM FDDI single mode</td> </tr> <tr> <td>9 FSM FDDI module</td> <td>18 ASM .5 MB single mode</td> </tr> <tr> <td>10 FSM CDDI module</td> <td>19 ASM UTP</td> </tr> <tr> <td>11 ESM 4-port</td> <td>20 ESM 8-port fiber</td> </tr> <tr> <td>12 ASM .5 MB multi-mode</td> <td>21 ESM 12-port Telco</td> </tr> <tr> <td></td> <td>22 TSM fiber</td> </tr> <tr> <td></td> <td>23 ASM 2 MB multi-mode</td> </tr> <tr> <td></td> <td>24 ASM 2 MB single mode</td> </tr> </table> <p>Operational State. Indicates the current state of the module that was reset or reloaded. The following integers are valid values:</p> <ol style="list-style-type: none"> 1 Unknown state. The module may have failed low-level self-test. 2 Invalid. The module may exist, by the chassis does not have control of it. 3 Operational. The module is running fine with no errors. 4 Disabled. The module has been set to disable through the UI or SNMP. 5 Reset. The module has been reset. 6 Loading. The module is in the middle of loading. 7 Testing. The module is in self-test. 8 Warning. A warning was detected during operation. 9 Non-fatal error. A non-fatal error was detected during operation. 10 Fatal error. A fatal error occurred during operation. The module may or may not be functional. 	4 HSM	13 ESM 12-port 10BASE-T	5 MPM	14 ESM 6-port universal module	6 ESM 8-port 10BASE-T	15 MPM version II	7 ESM 16-port	16 ATM DS-3	8 TSM 6-port UTP/STP	17 FSM FDDI single mode	9 FSM FDDI module	18 ASM .5 MB single mode	10 FSM CDDI module	19 ASM UTP	11 ESM 4-port	20 ESM 8-port fiber	12 ASM .5 MB multi-mode	21 ESM 12-port Telco		22 TSM fiber		23 ASM 2 MB multi-mode		24 ASM 2 MB single mode
4 HSM	13 ESM 12-port 10BASE-T																								
5 MPM	14 ESM 6-port universal module																								
6 ESM 8-port 10BASE-T	15 MPM version II																								
7 ESM 16-port	16 ATM DS-3																								
8 TSM 6-port UTP/STP	17 FSM FDDI single mode																								
9 FSM FDDI module	18 ASM .5 MB single mode																								
10 FSM CDDI module	19 ASM UTP																								
11 ESM 4-port	20 ESM 8-port fiber																								
12 ASM .5 MB multi-mode	21 ESM 12-port Telco																								
	22 TSM fiber																								
	23 ASM 2 MB multi-mode																								
	24 ASM 2 MB single mode																								

Trap Type	systemEvent
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.18
Description	A potentially fatal error occurred in the system.
Bit Position (Word 1)	17
Hex Value (Word 1)	2 0000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; width: fit-content; margin: 0 auto;">Potentially fatal error occurred (trap 10)</div> <p>Event Trap Type. A number that identifies the specific error that occurred in the system. The following integers are valid values:</p> <ul style="list-style-type: none"> 10 Unspecified Log Event 11 Log file full 12 Log file erased 20 Unspecified memory event 21 Memory shortage 30 Unspecified CPU event 31 Long term CPU overload 32 Short term CPU overload 40 Unspecified ffs event 41 Attempt to write to full ffs 42 System/user directed purge 43 Removed imgs/cfgs 44 Exec file removed 45 Config file removed 46 Exec file updated 47 Config file updated 50 Unspecified chassis event 51 Module failed to init 52 Module failed to load 53 Module startup failed 54 Module failed 55 Driver failed

Trap Tables

Trap Type	vlanRouteTableFull
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.19
Description	The IP or IPX route table is full.
Bit Position (Word 1)	18
Hex Value (Word 1)	4 0000
Trap Text and Variable Descriptions	IP or IPX route table is full on insertion.

Trap Type	sapTableFull
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.20
Description	The SAP table is full upon insertion.
Bit Position (Word 1)	19
Hex Value (Word 1)	8 0000
Trap Text and Variable Descriptions	SAP table full on insertion.

Trap Type	atmSSCOPstate
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.21
Description	A specified port changed.
Bit Position (Word 1)	20
Hex Value (Word 1)	10 0000
Trap Text and Variable Descriptions	<div style="text-align: center; border: 1px solid black; padding: 5px; width: fit-content; margin: 0 auto;"> Signalling state changed (slot 3 port 1) </div> <p>Slot number. The slot number where this ASM module is located.</p> <p>Port number. The port number on this ASM module where the signalling state has changed.</p>

Trap Type	ilmiState
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.22
Description	The ILMI state for the specified port changed. This change of state indicates whether address registration was successful, and whether the switch knows the network prefix provided by the external ATM switch.
Bit Position (Word 1)	21
Hex Value (Word 1)	20 0000
Trap Text and Variable Descriptions	<div style="text-align: center; border: 1px solid black; padding: 5px; width: fit-content; margin: 0 auto;"> ILMI state changed (slot 3 port 1) </div> <p>Slot number. The slot number where this ASM module is located.</p> <p>Port number. The port number on this ASM module where the ILMI state has changed.</p>

Trap Type	atmConnection
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.23
Description	The specified ATM VCC was created or deleted.
Bit Position (Word 1)	22
Hex Value (Word 1)	40 0000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> ATM VCC created or deleted (slot 3, port 1, Vpi 0, Vci 100, admin status 2) </div> <p>Slot Number. The slot number where this ASM module is located.</p> <p>Port Number. The port number on the ASM module where this VCC was created or deleted.</p> <p>VPI Number. The virtual path identifier for this virtual connec-</p> <p>VCI Number. The virtual channel identifier for this virtual connection.</p> <p>Admin Status. Indicates the current status of this ATM VCC. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 Disabled. This VCC was disabled. 2 Enabled. This VCC was enabled. 3 Deleted. This VCC was deleted.

Trap Type	atmService
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.24
Description	The specified ATM service (Port-to-Port Bridging, Trunking, LAN Emulation, etc.) was created or deleted.
Bit Position (Word 1)	23
Hex Value (Word 1)	80 0000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> ATM service created or deleted (slot 3, port 1, service 2, admin status 2) </div> <p>Slot Number. The slot number where this ASM module is located.</p> <p>Port Number. The port number on the ASM module where the service was created or deleted.</p> <p>Service Number. The ATM service number assigned to this service when it was set up.</p> <p>Admin Status. The current status of this ATM VCC. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 Disabled. This VCC has disabled. 2 Enabled. This VCC was enabled. 3 Deleted. This VCC was deleted.

Trap Type	dlciNew
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.27
Description	Frame Relay DLCI was created.
Bit Position (Word 1)	26
Hex Value (Word 1)	400 0000
Trap Text and Variable Descriptions	<div style="text-align: center; border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> Frame Relay DLCI created (slot 3 port 1 DLCI Number 100) </div> <p>Slot number. The slot number where this Frame Relay module is located.</p> <p>Port number. The port number on this Frame Relay module where the DLCI was created.</p> <p>DLCI Number. The number of the DLCI that was created.</p>

Trap Type	dlciDel
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.28
Description	Frame Relay DLCI was deleted.
Bit Position (Word 1)	27
Hex Value (Word 1)	800 0000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; text-align: center; margin-bottom: 10px;"> Frame Relay DLCI deleted (slot 3 port 1 DLCI Number 100) </div> <p>Slot number. The slot number where this Frame Relay module is located.</p> <p>Port number. The port number on this Frame Relay module where the DLCI was deleted.</p> <p>DLCI number. The number of the DLCI that was just deleted.</p>

Trap Tables

Trap Type	dlciUp
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.29
Description	Frame Relay DLCI changed to active state.
Bit Position (Word 1)	28
Hex Value (Word 1)	1000 0000
Trap Text and Variable Descriptions	<div data-bbox="396 646 1284 703" style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; text-align: center;">Frame Relay DLCI Changed to Active (slot 3 port 1 DLCI Number 100)</div> <p style="text-align: center;">Slot Number. The slot number where this Frame Relay module is located.</p> <p style="text-align: center;">Port Number. The port number on this Frame Relay module where the DLCI was activated.</p> <p style="text-align: center;">DLCI Number. The number of the DLCI that was just activated.</p>

Trap Type	dlciDn
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.30
Description	Frame Relay DLCI changed to inactive state.
Bit Position (Word 1)	29
Hex Value (Word 1)	2000 0000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; margin-bottom: 10px;"> <p style="text-align: center;">Frame Relay DLCI Changed to Inactive (slot 3 port 1 DLCI Number 100)</p> </div> <p style="text-align: center;">Slot Number. The slot number where this Frame Relay module is located.</p> <p style="text-align: center;">Port Number. The port number on this Frame Relay module where the DLCI was de-activated.</p> <p style="text-align: center;">DLCI Number. The number of the DLCI that was just de-activated.</p>

Trap Type	portManualForwardingMode
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.31
Description	The specified port was placed into manual mode forwarding as its default setting.
Bit Position (Word 1)	30
Hex Value (Word 1)	4000 0000
Trap Text and Variable Descriptions	<p style="text-align: center;"> Slot Number. The slot number where this port is located. </p> <p style="text-align: center;"> Port number. The port number on the module. </p> <div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; text-align: center; margin: 10px auto; width: fit-content;"> Port placed into manual mode forwarding (slot 3, port 1, type 1, instance 1) </div> <p style="text-align: center;"> Port Type. The physical type of this port. The following integers are valid values: </p> <ul style="list-style-type: none"> 1 Unknown 2 Other 3 Router 4 Bridge 5 Trunk 6 ATM trunk port 7 ATM LAN Emulation port 8 Classical IP 9 ATM MUX 203 Ethernet 10BASE-T 204 Ethernet 100BASE-T 205 Token Ring 4 mbs 206 Token Ring 16 mbs 207 FDDI 208 CDDI 209 ATM 25 mbs 210 ATM 50 mbs 211 DS-1 212 DS-3 213 OC-3 214 OC-12 215 OC-48 <p style="text-align: center;"> Physical Instance. The specific instance of this slot/port/type. In most cases this value will be 1 (only one instance of the port), but an ATM port may have multiple instances. Possible values range from 1 to 254. </p>

Trap Type	fddiCFStateChange
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.32
Description	The specified FDDI physical port changed from wrap configuration state.
Bit Position (Word 1)	31
Hex Value (Word 1)	8000 0000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; margin-bottom: 10px;"> FDDI physical port changes from wrap configuration state (index 1, state 2) </div> <p>SMT Index. A unique value for each SMT (Station Management Station). The value for each SMT must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.</p> <p>SMT State. The attachment configuration for the station or concentrator. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 isolated 2 local_a 3 local_b 4 local_ab 5 local_s 6 wrap_a 7 wrap_b 8 wrap_ab 9 wrap_s 10 c_wrap_a 11 c_wrap_b 12 c_wrap_s 13 thru

Trap Tables

Trap Type	duplicateIPaddress
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.35
Description	The switch detected a duplicate IP address.
Bit Position (Word 2)	2
Hex Value (Word 2)	4
Trap Text and Variable Descriptions	<p>IP Address. The IP address of the station that reported the duplicate IP address.</p> <p>MAC Address. The MAC address of the station that reported the duplicate IP address.</p> <p style="text-align: center;">Duplicate IP address detected (IP addr 192.168.10.1, Mac 0036589adf01, slot 3, IF 4, dup Mac 00145221cd02, dup slot 1, dup IF 3)</p> <p>Port Number. The port on the module of the reporting station from which the trap was sent.</p> <p>Duplicate Slot. The slot number on the reporting station where the duplicate address was discovered.</p> <p>Duplicate Port. The port on the module of the reporting station where the duplicate address was discovered.</p> <p>Slot Number. The slot number of the reporting station from which the trap was sent.</p> <p>Duplicate MAC. The MAC address associated with the duplicated IP address.</p>

Trap Type	duplicateMACAddress
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.36
Description	The switch detected a duplicate MAC address of one of its own router ports.
Bit Position (Word 2)	3
Hex Value (Word 2)	8
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Duplicate MAC address detected (Mac 00145221cd02, slot 2, IF 3, time 4</p> </div> <p>MAC Address. The router port's MAC address for which the last duplicate MAC address was detected.</p> <p>Slot. The slot number where the duplicate MAC address was last received.</p> <p>Interface. The interface number where the duplicate MAC address was last received.</p> <p>Time. The time, in seconds, when the duplicate MAC was detected.</p>

Trap Tables

Trap Type	healthThresholdRising
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.37
Description	At least one of the user-specified thresholds was exceeded.
Bit Position (Word 2)	4
Hex Value (Word 2)	10
Trap Text and Variable Descriptions	Thresh-hold rising trap

Trap Type	healthThresholdFalling
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.38
Description	At least one of the user-specified thresholds was exceeded during the previous cycle and none of them are exceeded in the current cycle.
Bit Position (Word 2)	5
Hex Value (Word 2)	20
Trap Text and Variable Descriptions	Thresh-hold falling trap

Trap Type	healthThresholdDevice
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.39
Description	At least one of the device-level threshold crossing was detected.
Bit Position (Word 2)	6
Hex Value (Word 2)	40
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Device-level threshold crossing is detected (Data 0a 09 0d 53 00 00 00 00 00 00 00 00 00 00) </div> <p>Data. An octet string that represents the contents of device-level rising/falling threshold trap.</p>

Trap Type	healthThresholdModule
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.40
Description	At least one module-level threshold crossing was detected.
Bit Position (Word 2)	7
Hex Value (Word 2)	80
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Module-level threshold crossing is detected (count 2, data 0a 09 0d 53 00 00 00 00 00 00 00 00 00 00) </div> <p>Count. The number of modules with threshold crossing data in module-level rising/falling threshold traps.</p> <p>Data. An octet string that represents the contents of device-level rising/falling threshold trap.</p>

Trap Type	xylanXIPXMAPPortStatusChange
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.41
Description	An XMAP turned on or off.
Bit Position (Word 2)	8
Hex Value (Word 2)	100
Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; margin-bottom: 10px;"> <p>The status of an XMAP-tracked virtual port has changed (port 1, reason 2)</p> </div> <p style="text-align: center;">Port Number. The virtual port number of the port that most recently changed.</p> <p style="text-align: center;">Reason. The reason for the last port status change. The following integers are valid values:</p> <ul style="list-style-type: none"> 0 No trap was sent. 1 A port was added. 2 A change of information on an existing port. 3 A port was deleted.

Trap Type	xylanXIPXMAPPortStateChange
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.42
Description	An XMAP turned on or off.
Bit Position (Word 2)	9
Hex Value (Word 2)	200
Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; margin-bottom: 10px;"> <p>The state of the XMAP agent has changed to (state 1)</p> </div> <p>Operating State. The XMAP's operating state. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 inactive 2 active

Trap Type	aviAuthAttempt
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.43
Description	Indicates the last authenticated VLAN attempt.
Bit Position (Word 2)	16
Hex Value (Word 2)	1 0000
Trap Text and Variable Descriptions	<p style="text-align: center;">User. The last user who made an authentication attempt.</p> <div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; text-align: center; margin: 10px auto; width: fit-content;"> <p>The last VLAN authentication attempt was: (user 1, event 2, MAC 0036589adf01, port 4, slot 5)</p> </div> <p>MAC Address. The last MAC address to make an authentication attempt.</p> <p>Port. The last port number from which the authentication attempt originated.</p> <p>Event Type. The last authorization attempt type. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 Successful login 2 Failed Login Attempt 3 Logout/Drop <p>Slot. The last slot number from which the authentication attempt originated.</p>

Trap Type	xylanXIPGMAPFailedUpdate
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.44
Description	GMAP is unable to update the forwarding database to reflect information in its internal database.
Bit Position (Word 2)	11
Hex Value (Word 2)	800
Trap Text and Variable Descriptions	<p>Reason. The reason for the last GMAP update was not applied. The following integers are valid values:</p> <ol style="list-style-type: none"> 1 The target group is an authenticated group. 2 The update would conflict with a binding rule. 3 The update would create two different group entries for the same protocol. 4 The update would create two different protocol entries for the same group. 5) The target group is not mobile. <div style="border: 1px solid black; padding: 5px; margin: 10px 0; text-align: center;"> GMAP is unable to update the forwarding database (reason 1, port 2, Mac 0036589adf01, protocol 4, group 5) </div> <p>MAC Address. The last MAC address for which a GMAP change was not applied.</p> <p>Group. The group identifier of the last GMAP change that was not applied.</p> <p>Port. The virtual port number of the last port on which the GMAP change was not applied.</p> <p>Protocol. The protocol identifier of the last GMAP change that was not applied.</p>

Trap Tables

Trap Type	clkBusLineStateChange								
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.45								
Description	Either the bus line's status changed (active or inactive) or clock switching occurred.								
Bit Position (Word 2)	10								
Hex Value (Word 2)	400								
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Bus Line's status changed (bus line 1, operating state 1) or clock switching has occurred.</p> </div> <p>Bus Line. The specific bus line where the status change occurred. The following integers are valid values:</p> <table style="margin-left: 20px;"> <tr> <td>1</td> <td>8 khz</td> </tr> <tr> <td>2</td> <td>19 mhz</td> </tr> </table> <p>Operating State. The bus line's operating state. The following integers are valid values:</p> <table style="margin-left: 20px;"> <tr> <td>1</td> <td>inactive</td> </tr> <tr> <td>2</td> <td>active</td> </tr> </table>	1	8 khz	2	19 mhz	1	inactive	2	active
1	8 khz								
2	19 mhz								
1	inactive								
2	active								

Trap Type	bind-violation
Object ID	1.3.6.1.4.1.800.3.1.1.1.0.46
Description	A configured binding rule was violated.
Bit Position (Word 2)	23
Hex Value (Word 2)	80 0000
Trap Text and Variable Descriptions	<p style="text-align: right;">IP Address. The IP address for which this binding is configured.</p> <p style="text-align: center;">VLAN ID. The VLAN ID for which this rule is configured.</p> <p style="text-align: center;">Group ID. The group ID of the VLAN for which this rule is configured.</p> <div style="border: 1px solid black; padding: 5px; text-align: center; margin: 10px auto; width: fit-content;"> <p>A binding rule has been violated (groupId 1, vlanId 2, IP 192.168.10.1 3, Mac 0036589adf01, protocol 5, port 6, rule 4, index 8)</p> </div> <p style="text-align: center;">Protocol. The protocol for which this binding is configured.</p> <p style="text-align: center;">Port. The port for which this binding is configured.</p> <p style="text-align: center;">MAC Address. The MAC address for which this binding is configured.</p> <p style="text-align: center;">Rule. The rule for which this binding is configured.</p> <p style="text-align: right;">Rule Index. The index which uniquely defines the rule for this VLAN.</p>

Trap Tables

Trap Type	mpcStatisticsOverflow
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.47
Description	An entry in the mpcStatisticsTable reached the threshold value.
Bit Position (Word 2)	18
Hex Value (Word 2)	4 0000
Trap Text and Variable Descriptions	<div data-bbox="386 636 1317 737" style="border: 1px solid black; background-color: #e0e0e0; padding: 5px;">MPC: Statistics threshold value reached (MpcIndex, Insufficient resources replies.)</div> <p>MPC Index. A unique number that identifies a conceptual row in the mpcConfig-Table.</p> <p>Insufficient resources replies. The reply from the MPC Statistics Table came back as insufficient resources.</p>

Trap Type	fddiLerFlagChange				
Object ID	1.3.6.1.4.1.800.3.1.1.1.0.65				
Description	The LER (Link Error Rate) flag on a port changed from CLEAR to SET.				
Bit Position (Word 3)	0				
Hex Value (Word 3)	1				
Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; text-align: center; margin-bottom: 10px;"> FDDI: Link Error Rate on a port is set (SMTIndex 1, port 2, LerFlag 3) </div> <p>SMT Index. A unique value for each SMT (Station Management). The value for each SMT must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.</p> <p>Port index. A unique value for each port with in a given SMT, which is the same as the corresponding resource index in SMT. The value for each port must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.</p> <p>LER Flag. The condition becomes active when the value of the fddiPRTLerEstimate is less than or equal to fddimibPORTLerEstimate. The following integers are valid values:</p> <table style="margin-left: 40px;"> <tr> <td>1</td> <td>True</td> </tr> <tr> <td>2</td> <td>False</td> </tr> </table>	1	True	2	False
1	True				
2	False				

Trap Type	fddiLCTFailCntIncr
Object ID	1.3.6.1.4.1.800.3.1.1.1.0.66
Description	The LCT (Link Confidence Test) flag on a port incremented.
Bit Position (Word 3)	1
Hex Value (Word 3)	2
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Fddi: Link Confidence Test flag on a port incremented (SMTIndex 1, port index 2, failure counts 3</p> </div> <p>Port Index . A unique value for each port within a given SMT, which is the same as the corresponding resource index in SMT. The value for each port must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.</p> <p>Failure Counts. The count of the consecutive times the link confidence test (LCT) failed during connection management.</p> <p>SMT Index. A unique value for each SMT. The value for each SMT must remain constant at least from one re-unitization of the entity's network management system to the next re-initialization.</p>

Trap Type	mpcStatisticsOverflow
Object ID	1.3.6.1.4.1.800.3.1.1.1.0.67
Description	The statisticsNum value of the mpcStatisticsTable reached the threshold value.
Bit Position (Word 2)	18
Hex Value (Word 2)	4 0000
Variables	mpcIndex mpcStatRxMpoaResolveReplyInsufECResources
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>GMAP is unable to update the forwarding database (index 1, MPOA replies 3)</p> </div> <p>MPC Index. A unique number that identifies a conceptual row in the mpcConfigTable.</p> <p>MPOA Resolution Replies. The number of MPOA Resolution Replies received with an MPOA CIE Code of 0x81.</p>

Trap Type	mpcShortCut
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.68
Description	The established shortcut path either closed or failed to complete the path.
Bit Position (Word 2)	19
Hex Value (Word 2)	8 0000
Variables	mpcRowStatus lecControlDirectVci mpcFlowDetectProtocol mpcIngressCacheDestAddr, mpcIngressCacheDestAtmAddr mpcIndex mpcMpsIndex
Trap Text and Variable Descriptions	<p style="text-align: center;">Row Status. This object allows creation and deletion of MPOA clients.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">GMAP is unable to update the forwarding database (rowStatus 1, control direct Vci 2, protocol 4, dest addr 192.168.40.12, dest ATM addr 3903488001bc900001020000090020da00000900, index 1, mps index 2)</p> </div> <p>Control Direct VCI. The VCI that identifies the VCC at the point where it connects to a LANE client. If the Control Direct VCC does not exist, this value is zero.</p> <p>Protocol. The protocol on which flow detection is performed.</p> <p>Destination ATM Address. The destination ATM address received in the MPOA Resolution Reply.</p> <p>Destination Address. The destination internet-work layer address.</p> <p>MPC Index. A unique number that identifies a conceptual row in the mpcConfig-Table.</p> <p>MPC MPS Index. The MPS's index that is used to identify a row in the mpcConig Table.</p>

Trap Type	mpcIngressRetryTimeOut
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.69
Description	The retry time exceeded the MPC-p5 time.
Bit Position (Word 2)	20
Hex Value (Word 2)	10 0000
Variables	mpcIndex mpcRetryTimeMaximum mpcIngressCacheDestAddr mpcIngressCacheDestAtmAddr mpcFlowDetectProtocol mpcMpsIndex
Trap Text and Variable Descriptions	<p>MPC Index. A unique number that identifies a conceptual row in the mpcConfig-Table.</p> <p>Maximum Retry Time. The MPC-p5 cumulative maximum value for retry time.</p> <p>Destination Address. The destination internet-network layer address.</p> <p>Destination ATM Address. The destination ATM address received in the MPOA Resolution Reply.</p> <p>Detect Protocol. The protocol on which flow detection is performed.</p> <p>GMAP is unable to update the forwarding database (index 1, max time 5, dest addr 192.168.40.12, ATM addr 3903488001bc900001020000090020da00000900, protocol 1)</p>

Trap Tables

Trap Type	vrrpTrapNewMaster
Object ID	1.3.6.1.2.1.46.1.3.1.0.3
Description	The sending agent has transitioned from “Backup” state to “Master” state.
Bit Position (Word 2)	21
Hex Value (Word 2)	20 0000
Trap Text and Variable Descriptions	<div data-bbox="404 638 1263 720" style="border: 1px solid black; background-color: #e0e0e0; padding: 5px;">Agent has transitioned from Backup to Master state (If index 1, vrid 2)</div> <p style="text-align: center;">Interface Index Number. A unique value that identifies the sending agent.</p> <p style="text-align: center;">Virtual Router ID. The number that identifies the virtual router on this VRRP. Possible values range from 1 to 255.</p>

Trap Type	vrrpAuthFailure
Object ID	1.3.6.1.2.1.46.1.3.1.0.4
Description	A packet was received from a router whose authentication key or authentication type conflicts with this router's authentication key or type.
Bit Position (Word 2)	22
Hex Value (Word 2)	40 0000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>A packet with a wrong authentication key or type is received (If index 1, vrid 2, source 192.168.10.1, error type 3)</p> </div> <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>Packet Source IP. The IP address of an inbound VRRP packet.</p> </div> <div style="text-align: center;"> <p>Interface Index Number. A unique value that identifies the sending agent.</p> </div> </div> <div style="display: flex; justify-content: space-around; margin-top: 20px;"> <div style="text-align: center;"> <p>Virtual Router ID. The number that identifies the virtual router on this VRRP. Possible values range from 1 to 255.</p> </div> <div style="text-align: center;"> <p>Error Type. The type of configuration conflict. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 Invalid authentication type 2 Mismatched authentication 3 Authentication Failure </div> </div>

Trap Tables

Trap Type	oamVCAIS
Object ID	1.3.6.1.4.1.800.3.1.1.1.0.71
Description	The specified connection is in the VC-AIS state.
Bit Position (Word 3)	10
Hex Value (Word 3)	400
Variables	xylanOamF5VCSlotIndex xylanOamF5VCPortIndex xylanOamF5VCVpiIndex xylanOamF5VCVciIndex
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 10px; margin-bottom: 10px;"> <p>The specified connection is in VC-AIS state. (Slot 1, Port 2, VPI 2, VCI 1)</p> </div> <p>Slot Number. The slot number for the specified connection.</p> <p>Port Number. The port number for the specified connection.</p> <p>VPI. The virtual path identifier for the specified connection.</p> <p>VCI. The virtual circuit identifier for the specified connection.</p>

Trap Type	oamVCRDI
Object ID	1.3.6.1.4.1.800.3.1.1.1.0.72
Description	The specified connection is in the VC-RDI state.
Bit Position (Word 3)	11
Hex Value (Word 3)	800
Variables	xylanOamF5VCSlotIndex xylanOamF5VCPortIndex xylanOamF5VCVpiIndex xylanOamF5VCVciIndex
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>The specified connection is in VC-RDI state. (Slot 1, Port 2, VPI 2, VCI 1)</p> </div> <p>Slot Number. The slot number for the specified connection.</p> <p>Port Number. The port number for the specified connection.</p> <p>VPI. The virtual path identifier for the specified connection.</p> <p>VCI. The virtual circuit identifier for the specified connection.</p>

Trap Type	oamVCLOC
Object ID	1.3.6.1.4.1.800.3.1.1.1.0.73
Description	The specified connection is in the VC-LOC state.
Bit Position (Word 3)	12
Hex Value (Word 3)	1000
Variables	xylanOamF5VCSlotIndex xylanOamF5VCPortIndex xylanOamF5VCVpiIndex xylanOamF5VCVciIndex
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>The specified connection is in VC-LOC state. (Slot 1, Port 2, VPI 2, VCI 1)</p> </div> <p>Slot Number. The slot number for the specified connection.</p> <p>Port Number. The port number for the specified connection.</p> <p>VPI. The virtual path identifier for the specified connection.</p> <p>VCI. The virtual circuit identifier for the specified connection.</p>

Trap Type	oamVCUnsuccessLoop
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.74
Description	The specified connection is in the Unsuccessful Loopback state.
Bit Position (Word 3)	13
Hex Value (Word 3)	2000
Variables	xylanOamF5VCSlotIndex xylanOamF5VCPortIndex xylanOamF5VCVpiIndex xylanOamF5VCVciIndex
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>The specified connection is in VC-UnsuccessLoop state. (Slot 1, Port 2, VPI 2, VCI 1)</p> </div> <p>VPI. The virtual path identifier for the specified connection.</p> <p>VCI. The virtual circuit identifier for the specified connection.</p> <p>Port Number. The port number for the specified connection.</p> <p>Slot Number. The slot number for the specified connection.</p>

Trap Type	oamVPAIS
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.75
Description	The specified VP connection is in the VP-AIS state.
Bit Position (Word 3)	14
Hex Value (Word 3)	4000
Variables	xylanOamF5VCSlotIndex xylanOamF5VCPortIndex xylanOamF5VCVpiIndex
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 10px; margin-bottom: 10px;"> <p>The specified connection is in VP-AIS state. (Slot 1, Port 2, VPI 2, VCI 1)</p> </div> <p>Slot Number. The slot number for the specified connection.</p> <p>Port Number. The port number for the specified connection.</p> <p>VPI. The virtual path identifier for the specified connection.</p> <p>VCI. The virtual circuit identifier for the specified connection.</p>

Trap Type	oamVPRDI
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.76
Description	The specified VP connection is in the VP-RDI state.
Bit Position (Word 3)	15
Hex Value (Word 3)	8000
Variables	xylanOamF5VCSlotIndex xylanOamF5VCPortIndex xylanOamF5VCVpiIndex
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>The specified connection is in VP-LOC state. (Slot 1, Port 2, VPI 2, VCI 1)</p> </div> <p>Slot Number. The slot number for the specified connection.</p> <p>Port Number. The port number for the specified connection.</p> <p>VPI. The virtual path identifier for the specified connection.</p> <p>VCI. The virtual circuit identifier for the specified connection.</p>

Trap Type	oamVPLOC
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.77
Description	The specified VP connection is in the VP-LOC state.
Bit Position (Word 3)	16
Hex Value (Word 3)	1 0000
Variables	xylanOamF5VCSlotIndex xylanOamF5VCPortIndex xylanOamF5VCVpiIndex
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>The specified connection is in VPUnsuccessLoop state. (Slot 1, Port 2, VPI 2, VCI 1)</p> </div> <p>VCI. The virtual circuit identifier for the specified connection.</p> <p>Slot Number. The slot number for the specified connection.</p> <p>Port Number. The port number for the specified connection.</p> <p>VPI. The virtual path identifier for the specified connection.</p>

Trap Type	oamVPUnsuccessLoop
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.78
Description	The specified VP connection is in the unsuccessful loopback state.
Bit Position (Word 3)	17
Hex Value (Word 3)	2 0000
Variables	xylanOamF5VCSlotIndex xylanOamF5VCPortIndex xylanOamF5VCVpiIndex
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>The specified connection is in VP-RDI state. (Slot 1, Port 2, VPI 2, VCI 1)</p> </div> <p>Slot Number. The slot number for the specified connection.</p> <p>Port Number. The port number for the specified connection.</p> <p>VPI. The virtual path identifier for the specified connection.</p> <p>VCI. The virtual circuit identifier for the specified connection.</p>

Trap Tables

Trap	accountEvent
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.86
Description	An account event is generated to signal that a new accounting file is available on the switch
Bit Position (Word 3)	21
Hex Value (Word 3)	20 0000
Variable Description	chasAccountName - Path name of the most recently terminated accounting file. chasAccountFileCount - The number of terminated accounting files awaiting collection and removal by an external accounting collection agent.

Trap	Over1Alarm
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.87
Description	This alarm is generated when the filling level exceeds the first threshold. It signals that the switch changes over to the alternate collection device.
Bit Position (Word 3)	22
Hex Value (Word 3)	40 0000
Variable Description	chasAccountFilingLevel - The amount of buffer taken up by accounting data. Value shown as a percentage of the buffer size. chasAccountThreshold1 - The first filling level of the intermediate storage area for accounting data. Crossing this threshold generates a warning. Value shown as a percentage of the buffer size. chasAccountDeviceInUse - The IP address of the collection device with which a TCP connection was most recently established.

Trap Type	Under1Event
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.88
Description	This event is generated when the filling level goes below the first threshold. This event is for information only.
Bit Position (Word 3)	23
Hex Value (Word 3)	80 0000
Variable Description	chasAccountFilingLevel - The amount of buffer taken up by accounting data. Value shown as a percentage of the buffer size. chasAccountThreshold1 - The first filling level of the intermediate storage area for accounting data. Crossing this threshold generates a warning. Value shown as a percentage of the buffer size.

Trap	Over2Alarm
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.89
Description	This alarm is generated when the filling level exceeds the second threshold. It signals that the switch changes over to the alternate collection device.
Bit Position (Word 3)	24
Hex Value (Word 3)	100 0000
Variable Description	chasAccountFilingLevel - The amount of buffer taken up by accounting data. Value shown as a percentage of the buffer size. chasAccountThreshold2 - The second filling level of the intermediate storage area for accounting data. Crossing this threshold generates a warning. Value shown as a percentage of the buffer size. chasAccountDeviceInUse - The IP address of the collection device with which a TCP connection was most recently established.

Trap	Under2Event
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.90
Description	This event is generated when the filling level is lowered below the second threshold.
Bit Position (Word 3)	25
Hex Value (Word 3)	200 0000
Variable Description	chasAccountFilingLevel - The amount of buffer taken up by accounting data. Value shown as a percentage of the buffer size. chasAccountThreshold2 - The second filling level of the intermediate storage area for accounting data. Crossing this threshold generates a warning. Value shown as a percentage of the buffer size.

Trap	Over3Alarm
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.91
Description	This event is generated when the filling level exceeds the third threshold. It signals that the switch is now in congestion.
Bit Position (Word 3)	26
Hex Value (Word 3)	400 0000
Variable Description	chasAccountFilingLevel - The amount of buffer taken up by accounting data. Value shown as a percentage of the buffer size. chasAccountThreshold3 - The third filling level of the intermediate storage area for accounting data. Crossing this threshold generates a warning. Value shown as a percentage of the buffer size. chasAccountDeviceInUse - The IP address of the collection device with which a TCP connection was most recently established.

Trap	Under3Event
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.92
Description	This event is generated when the filling level goes below the third threshold.
Bit Position (Word 3)	27
Hex Value (Word 3)	8000 0000
Variable Description	chasAccountFilingLevel - The amount of buffer taken up by accounting data. Value shown as a percentage of the buffer size. chasAccountThreshold3 - The third filling level of the intermediate storage area for accounting data. Crossing this threshold generates a warning. Value shown as a percentage of the buffer size.

Trap Type	NoDeviceAlarm
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.93
Description	This alarm is generated when the TCP connection establishment fails with both the primary and the secondary collection devices.
Bit Position (Word 3)	28
Hex Value (Word 3)	1000 0000
Variable Description	chasAccountDevicePrimary - The IP address of the primary collection device. chasAccountDeviceSecondary - The IP address of the secondary collection device.

Trap Tables

Trap	FileAlarm
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.94
Description	This alarm is generated when too many files are awaiting collection.
Bit Position (Word 3)	29
Hex Value (Word 3)	2000 0000
Variable Description	chasAccountFileCount - The number of terminated accounting files awaiting collection and removal by an external accounting collection agent.

Trap Type	fantrayEvent
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.1
Description	A fantrayEvent trap occurs when a problem condition is recognized on a chassis fan tray.
Bit Position (Word 3)	30
Hex Value (Word 3)	4000 0000
Variable Description	fantray1State - Status of fan tray 1. chasAccountDeviceSecondary - Status of fan tray 2.

Trap Type	lecStateChangeEvent
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.96
Description	A trap message is sent to a network manager when a LEC status changes.
Bit Position (Word 2)	26
Hex Value (Word 3)	40 00000
Variables	lecID lecActualLanName lecAtmAddress, xylanLecSlotNumber xylanLecPortNumber xylanLecServiceNumber lecInterfaceState xylanReasonOfChange

<p>Trap Text and Variable Descriptions</p>	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>ELAN Name. The name of the ELAN whose status changed to generate this trap.</p> </div> <div style="width: 45%;"> <p>Service Instance. The specific instance of this service. In most cases this value will be 1 but an ATM port may have multiple instances</p> </div> </div> <div style="text-align: center; margin: 10px 0;"> <div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; display: inline-block;"> LEC Status Change (ELAN Name, Service Instance, New state, previous state). </div> </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>New State. The new, current status of the LEC that changed to generate this trap. Displayed as an integer as shown below in the State List.</p> </div> <div style="width: 45%;"> <p>Previous State. The previous status of the LEC that changed to generate this trap. Displayed as an integer as shown below in the State List.</p> </div> </div> <div style="margin-top: 20px;"> <p>State List</p> <ol style="list-style-type: none"> 1. none 2. timeout 3. undefined error 4. version not supported 5. invalid request parameters 6. duplicate LAN destination 7. duplicate ATM address 8. insufficient resources 9. access denied 10. invalid requester id 11. invalid LAN destination 12. invalid ATM address 13. no configuration 14. leconfigureError 15. insufficient information </div>
---	--

18 DNS Resolver and RMON

Introduction

This chapter describes commands related to the Domain Name Server (DNS) resolver and remote network monitoring (RMON) feature in the switch. This chapter also describes how to configure router port MAC addresses with the **chngmac** command.

The commands for these features are available from the Networking submenu, which is described in Chapter 30, "IP Routing."

Configuring the DNS Resolver

The Names Submenu

The **Names** command takes you to the Names submenu. The one command in this menu, **res**, is used to view and to configure the Domain Name Server (DNS) resolver. You can configure up to three Domain Name Servers. The switch searches all three servers until it resolves the name to an IP address or until it fails to find the name.

To display the **Names** submenu, enter the following command:

```
names
```

A screen similar to the following displays:

```
Command      Resolver Configuration Menu
-----
res          View/Configure the DNS resolver

Main   File   Summary  VLAN   Networking
Interface Security System  Services Help
```

To configure one or more Domain Name Servers, enter the following command:

```
res
```

If the resolver function has not been enabled, a screen similar to the following displays:

```
DNS Resolver Configuration

1) Resolver Enabled : No

Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw) :
```

Configuring the DNS Resolver

To enable the resolver function, enter **1=y**. A screen similar to the following then displays:

DNS Resolver Configuration

```
1) Resolver Enabled      : Yes
2) Domain                : UNSET
3) Server Address 1     : UNSET
4) Server Address 2     : UNSET
5) Server Address 3     : UNSET
```

Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw) :

The prompts allow you to enter a Domain Name and up to three Domain Name Servers (identified by their IP addresses).

- To change a value, enter the number corresponding to that value, an (=), then the new value. For example, to set a Domain Name to Company.Com, enter **2=Company.Com**.
- To clear an entry, specify the value as (.) as in **2=.**
- To save all your modifications, enter **save**
- To cancel all your modifications, enter **quit**
- To view the parameters currently configured, enter **?**

Remote Network Monitoring (RMON)

Remote Network Monitoring (RMON) allows you to set up remote monitoring within your OmniSwitch. RMON consists of “probes” and “events.” There are two commands in the Networking menu, **probes** and **events**, which you can use to monitor, activate and inactivate probes and events. Be aware that you cannot create probes from within the switch’s User Interface; to do so requires a network application such as HP ProbeView.

Probes and Events

A **probe** is a task that runs in the switch. By using probes instead of sending repetitive inquiries to the switch, network traffic is significantly reduced.

There are three different kinds of probes: Ethernet, History, and Alarm.

A network management station (NMS) can configure either History or Alarm probes (a maximum of 16 is allowed). The status of a probe can be one of the following:

- Creating - The probe is under creation.
- Active - The probe is active.
- Inactive - The probe is inactive.

An **event** is an action that takes place based on an alarm condition detected by a probe. The event can take the form of an SNMP trap message and/or a log entry describing the alarm.

Ethernet Probes

An Ethernet probe monitors a selected Ethernet interface (port) and tracks Ethernet statistics. An Ethernet probe is automatically created on each Ethernet interface that is enabled. If the interface becomes disabled, that Ethernet probe is deleted.

History Probes

A History probe keeps a running history of all the statistics it has collected. When you set up a history probe you assign a sampling interval and a total number of samples to be taken. It keeps this information in a set of rotating buffers, so that it always retains the most recent samples.

The sampling rate is configurable from 1 second to 3600 seconds (1 hour). The total number of samples is configurable, however, it is limited by system resources (memory) available. The more samples you request, the more system resources needed. You may request as many samples as you want but the system will only grant as many as it has available.

Alarm Probes

An Alarm probe generates an alarm if the variable you are monitoring exceeds a set limit.

To set up an Alarm probe you need to select a variable (Ethernet statistic) that you want to monitor. You set an upper and lower threshold that you will allow this variable to reach. If it crosses the threshold, an event is triggered which results in the sending of an SNMP trap and/or the logging of the alarm.

There are two ways an Alarm probe monitors variables. One is by absolute value. For example, if you set an upper limit of 100, an alarm will be generated if the variable exceeds 100. The other is a delta value where you can set the amount of change allowable; for example, you could set the delta range to 10. If the current sample differs from the previous sample by more than 10, an alarm will be generated.

The Alarm probe attempts to prevent a flood of alarms from being generated by fluctuating values. It does so by continuously comparing the upper and lower limits. What this means is that the first time either an upper or lower limit is exceeded, an alarm will be generated. However, if the variable moves back inside the limit, then out again, another alarm will not be generated unless the opposite limit is exceeded. For example, consider a situation where an upper limit of 75 and a lower limit of 25 is set. The variable goes to 76. An alarm is generated. If it drops to 74 then goes back up to 76, no alarm will be generated. Only when the variable drops below 25 will another alarm be generated. If it goes back up to 76 then another alarm will be generated, etc. This procedure prevents a flood of alarms from being generated if the value fluctuates between 74 and 76.

Monitoring Probes

The **probes** command is used to monitor, activate, and inactivate existing probes (remember, you cannot create probes in the switch's UI). You can do three things with the command:

1. View all the current probes.
2. View a specific probe.
3. Activate or inactivate a History or Alarm Probe. (You can only do this with the "admin" login.)

The **probes** command has three optional parameters. The format is:

probes [active | inactive] [n]

where:

active - activates an existing probe

inactive - inactivates an existing probe

n - is the entry number of the probe to view

If you enter the **probes** command without parameters, it displays all the current probes.

RMON Probe Summary

Entry	Slot/Port	Flavor	Status	Time	System Resources
1	2/ 1	Ethernet	Active	0 hrs 39 mins	312 bytes
2	2/ 1	History	Active	0 hrs 4 mins	3656 bytes
3	2/ 1	Alarm	Active	0 hrs 0 mins	1336 bytes

Entry

The entry number in the list of probes (1-16).

Slot/Port

The slot port number (interface) that this probe is monitoring.

Flavor

Ethernet, History, or Alarm.

Status

Creating, Active, or Inactive.

Time

Time since the last change in status.

System Resources

Amount of memory that has been allocated to this probe.

To see the detail for each of the probes enter the **probes** command followed by the entry number as shown below.

```
/Networking % probes 1
```

RMON Probe Summary

Entry	Slot/Port	Flavor	Status	Time	System Resources
1	2/ 1	Ethernet	Active	0 hrs 39 mins	312 bytes

Probe's Owner: OmniSwitch Ethernet probe on slot 2 port 1

```
/Networking % probes 2
```

RMON Probe Summary

Entry	Slot/Port	Flavor	Status	Time	System Resources
2	2/ 1	History	Active	0 hrs 4 mins	3656 bytes

Probe's Owner: andy

- History Control Buckets Requested = 60
- History Control Buckets Granted = 60
- History Control Interval = 60 seconds
- History Sample Index = 6

```
/Networking % probes 3
```

RMON Probe Summary

Entry	Slot/Port	Flavor	Status	Time	System Resources
3	2/ 1	Alarm	Active	0 hrs 0 mins	1336 bytes

Probe's Owner: andy

- Alarm Rising Threshold = 3000
- Alarm Falling Threshold = 3000
- Alarm Rising Event Index = 1
- Alarm Falling Event Index = 3
- Alarm Interval = 30 seconds
- Alarm Sample Type = delta value
- Alarm Startup Alarm = rising or falling alarm
- Alarm Variable = ethernet octets received

Monitoring Events

The **events** command has one optional parameter. The format is:

```
events [clear]
```

where:

clear - clears the event log. (You can only do this with the "admin" login.)

RMON Logged Events Summary

Entry	Time	Description
1	0 hrs 26 mins	Rising threshold alarm for etherStatsOctets on slot 2 port 1
2	0 hrs 27 mins	Rising threshold alarm for etherStatsOctets on slot 2 port 1

Configuring Router Port MAC Addresses

You can use the **chnghmac** command if you want to configure a locally administered address (LAA) for a group that has an IP router port, IPX router port, or both. To use this command, enter **chnghmac** followed by the number of the group you want to modify (the default group number is **1**).

◆ Important Note ◆

You must add **chnghmacFlag=1** to the end of the **mpm.cmd** file and then reboot the switch to use the **chnghmac** command. See Chapter 11, “Managing Files,” for information on editing system files.

For example, if you want to modify a MAC address in Group 2, you would enter:

```
chnghmac 2
```

at the system prompt. Something similar to the following would then be displayed:

```
Current MAC address is factory default
Enter Router Port's MAC address ([XYZZ:AABBCC]) :
```

Enter the router port MAC address. (It cannot be a multicast address.) If you enter an incorrect address, the following will be displayed:

```
Invalid input format -- usage [XYZZ:AABBCC].
```

and the **chnghmac** command will terminate. If you enter a correct address, the following would then be displayed:

```
Is MAC address in Canonical or Non-Canonical (C or N) [C] :
```

Enter **C** if the address is canonical or **N** if it is non-canonical (the default is canonical). Note that if you execute the **chnghmac** command again it will display the user-defined instead of “factory default.”

Restoring Router Port Mac Addresses

If you want to restore the MAC address to the factory default, enter **chnghmac** followed by the group number. When the system asks for the MAC address, enter **000000:000000**. For example, to restore router port configured MAC address 003030:000001 in Group 2 to the factory default, enter

```
chnghmac 2
```

at the system prompt. The following would then be displayed:

```
Configured MAC Address: Canonical    Non-Canonical
                        003030:000001 000c0c:000080
{Address 000000:000000 requests use of factory default}
Enter Router Port's MAC address ([XYZZ:AABBCC]) :
```

Note that the **chnghmac** command displayed the user-defined instead of “factory default.” Enter **000000:000000** at the prompt.

19 Managing Ethernet Modules

Overview of OmniSwitch and Omni Switch/Router Ethernet Modules

This chapter describes User Interface commands for Ethernet, Fast Ethernet, and Gigabit Ethernet modules. Most commands are used with Fast Ethernet, 10/100, and high-density modules. With the release of 3.1, a new generation of Ethernet modules were used in the OmniSwitch. These modules include auto-sensing 10/100 Ethernet and high-density Ethernet modules. With the release of 3.4, Gigabit Ethernet modules became available.

This chapter documents User Interface (UI) commands to manage OmniSwitch and Omni Switch/Router Ethernet modules. For documentation on Command Line Interface (CLI) commands to manage Ethernet modules, see the *Text-Based Configuration CLI Reference Guide*.

◆ Important Note ◆

In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. See Chapter 8, “The User Interface,” for documentation on changing from CLI mode to UI mode.

Port Mirroring and Port Monitoring

Port Mirroring and Port Monitoring can be used on all Ethernet modules. Both Port Mirroring and Port Monitoring are described at the end of Chapter 24, “Managing Groups and Ports.”

Fast Ethernet Backbones

Fast Ethernet ports can be used as backbone links. The switch has two features that can improve the performance and flexibility of Ethernet backbones. OmniChannel aggregates the bandwidth of up to four (4) Fast Ethernet ports. This feature allows you to scale Fast Ethernet links from 100 Mbps to 800 Mbps in 100 Mbps increments. OmniChannel is described in *OmniChannel* on page 19-11. Fast Ethernet ports also support the 802.1Q tagging mechanism, enhancing the compatibility of ports with other vendors’ equipment. 802.1Q is described in Chapter 20, “Managing 802.1Q Groups.”

Gigabit Ethernet Modules

Gigabit Ethernet modules can be used as backbone links and used to support high-speed servers. Most Gigabit Ethernet modules support 802.1Q hardware tagging. In addition, all Gigabit Ethernet modules support an Alcatel version of 802.1Q called X802.1Q. See Chapter 20, “Managing 802.1Q Groups,” for more information on 802.1Q and X802.1Q hardware tagging for Gigabit Ethernet Modules.

◆ Note ◆

For Kodiak-based 10/100 Ethernet modules, 802.1Q is supported over OmniChannel. See Chapter 20, “Managing 802.1Q Groups” for more information.

Variety of Connector Options

Ethernet and Fast Ethernet modules are available in a variety of connector types. On the OmniSwitch, Fast Ethernet modules use copper RJ-45 and fiber SC connectors. On the Omni Switch/Router, 10/100 Ethernet modules use copper RJ-45 connectors and the ESX-100FM/FS-12W Fast Ethernet module uses fiber MT-RJ connectors.

On the OmniSwitch, Ethernet 10 Mbps modules are available with copper RJ-45, fiber SC, Telco (RJ-21), BNC, and AUI connectors. On the Omni Switch/Router, the 10 Mbps ESX-FM-24W uses fiber VF-45 connectors.

Gigabit Ethernet modules on the OmniSwitch and Omni Switch/Router use fiber SC connectors. Refer to Chapter 7, “OmniSwitch Switching Modules,” for more detailed information on OmniSwitch Ethernet hardware and Chapter 3, “Omni Switch/Router Switching Modules,” for information on Omni Switch/Router Ethernet hardware.

Three Generations of Modules

Ethernet modules in Release 3.1 and later contain advanced chip technology referred to as “Mammoth.” This new technology boosts the port density of modules, increasing the port count available in each chassis. The Mammoth technology also includes ports with 10/100 autosensing capability. This new generation of Ethernet modules also uses a different set of software commands to configure and monitor ports.

Ethernet modules in Release 4.3 and later contain another chip technology referred to as “Kodiak.” The new Kodiak-based modules combine several features of the Mammoth and early Ethernet modules. They support priority VLANs with 4 separate levels of priority; in addition, ESX-K Series Kodiak-based Ethernet modules support the addition of a server version of the OmniChannel. For information on priority VLANs, see Chapter 24, “Managing Groups and Ports.” For information on OmniChannel and Server Channel features, see *OmniChannel* on page 19-11.

The following tables outline the three generations of Ethernet modules and some of their differences.

Early Generation OmniSwitch Ethernet Modules

Ethernet Module	Speed Supported (per port)	Software Configurable?	Commands Available
ESM-C-8	10 Mbs	No	n/a
ESM-C-12	10 Mbs	No	n/a
ESM-F-8	10 Mbs	No	n/a
ESM-T-12	10 Mbs	No	n/a
ESM-U	10 Mbs	No	n/a
ESM-100C	100 Mbs	Yes	eth100cfg eth100vc
ESM-100C-FD	100 Mbs	Yes	eth100cfg eth100vc
ESM-100F-FD	100 Mbs	Yes	eth100cfg eth100vc
ESM-100C-5	100 Mbs	Yes	eth100cfg eth100vc
ESM-100CF-5	100 Mbs	Yes	eth100cfg eth100vc

High-Density, 10/100, and Gigabit Ethernet (Mammoth) Modules

Ethernet Module (Chassis Type)	Speed Supported (per port)	Software Configurable?	Commands Available	OmniChannel Supported?
ESM-C-16 (OmniSwitch)	10 Mbs	Yes	10/100cfg 10/100vc	No
ESM-C-32 (OmniSwitch)	10 Mbs	Yes	10/100cfg 10/100vc	No
ESM-FM-16W (OmniSwitch)	10 Mbs	Yes	10/100cfg 10/100vc	No
ESM-100C-12 (OmniSwitch)	10/100 Mbs	Yes	10/100cfg 10/100vc	Yes (at 100 Mbps)
ESM-100FM-8 (OmniSwitch)	100 Mbs	Yes	10/100cfg 10/100vc	Yes
ESM-100C-32W (OmniSwitch)	10/100 Mbs	Yes	10/100cfg 10/100vc	No
ESM-T-24W (OmniSwitch)	10 Mbs	Yes	10/100cfg 10/100vc	No
ESX-100C-12W (Omni Switch/Router)	10/100 Mbs	Yes	10/100cfg 10/100vc	Yes (at 100 Mbps)
ESX-100C-32W (Omni Switch/Router)	10/100 Mbs	Yes	10/100cfg 10/100vc	No
ESX-100FM/FS-12W (Omni Switch/Router)	100 Mbs	Yes	10/100cfg 10/100vc	Yes
ESX-FM-24W (Omni Switch/Router)	10 Mbs	Yes	10/100cfg 10/100vc	No
GSM-FM/FS-2W (OmniSwitch)	1000 Mbps	Yes	10/100cfg 10/100vc	No
GSX-FM/FS-2W (Omni Switch/Router)	1000 Mbps	Yes	10/100cfg 10/100vc	No
GSX-FM/FS-4W (Omni Switch/Router)	1000 Mbps	Yes	10/100cfg 10/100vc	No

When the OmniSwitch modules in this table are used with an MPM-1G, the MPM-1G should be at least revision level A9.

Kodiak Ethernet Modules

Ethernet Module (Chassis Type)	Speed Supported (per port)	Software Configurable?	Commands Available	OmniChannel Supported?
ESX-K-100C-32W (Omni Switch/Router)	10/100 Mbs	Yes	10/100cfg 10/100vc	Yes
ESX-K-100FM/FS-16W (Omni Switch/Router)	100 Mbs	Yes	10/100cfg 10/100vc	Yes
GSX-K-FM/FS-2W (Omni Switch/Router)	1000 Mbs	Yes	10/100cfg 10/100vc	No

ESM/ESX-K Series Modules and Optimized Ports

The ESM-100C-12, ESM-100FM-8, ESM-100C-32W, ESM-C-32, ESX-K-100C-32W, and ESX-K-100FM/FS-16W Mammoth-based and Kodiak-based modules will flood packets with unknown destination addresses on ports configured for optimized device mode. To prevent this condition, the following command can be entered into the **mpm.cmd**, **mpm3.cmd** or **mpx.cmd** file:

MamOptSwitchPorts=1

If the port is set to optimized and has not learned a MAC address, it will flood these packets out regardless if the above condition is used. If the above flag is set, the port will not flood multicast packets.

◆ Note ◆

For information on editing the **mpm.cmd**, **mpm3.cmd** or **mpx.cmd** text files, see Chapter 11, “Managing Files.”

Port Partitioning

Ethernet10BaseT, 10/100BaseT and 100BaseF boards can detect certain cabling errors and/or physical media misconfigurations which could lead to multiple retries or reception of multiple spurious frames, affecting performance of attached devices. In this event, the system will partition the affected port, which will be marked in the **vi** menu with Inactive (**Inactv**) operational status. (See Chapter 24, “Managing Groups and Ports,” for information about the **vi** command.) If a cable drop is detected, the system will remove the partitioned state, bringing the port back into a normal state once the link is detected.

If the original cabling problem has not been corrected, the link may become partitioned again. In this event, normal operation will be enabled when the problem has been corrected.

The Ethernet Management Menus

The **eth100** and **10/100** sub-menus are described in this chapter. These sub-menus are part of the physical interface sub-menu, which appears similar to the following display:

Command	Physical Interface Menu
slipc	Configure SLIP (Serial Line IP) on a TTY Port
atm	Enter the ATM Management sub-menu
eth100	Enter the 100BaseT sub-menu
10/100	Enter the 10/100BaseT sub-menu
tok	Enter the Token Ring Management sub-menu
Main File Summary VLAN Networking Interface Security System Services Help	

The **eth100** sub-menu contains commands for early generation Fast Ethernet modules. The **10/100** sub-menu has commands for high-density and 10/100 (Mammoth generation) Ethernet modules.

When you enter **eth100** at a system prompt, you enter the early generation Fast Ethernet sub-menu. This sub-menu displays as follows:

Command	100BaseT Menu
eth100vc	View 100BaseT Port Configuration Table
eth100cfg	Configure 100BaseT Port Parameters
Main File Summary VLAN Networking Interface Security System Services Help	

Descriptions for these commands begin on page 19-18.

When you enter **10/100** at a system prompt, you enter the High-Density—10/100 Ethernet configuration sub-menu. This sub-menu displays as follows:

Command	10/100 Menu
10/100vc	View 10/100 Port Configuration Table
10/100cfg	Configure 10/100 Port Parameters
crechnl	Create a Fast Ethernet Channel
delechnl	Delete a Fast Ethernet Channel
addprtchnl	Add port/s to a fast Ethernet Channel
delprtchnl	Delete port/s from a fast Ethernet Channel
chnlinfo	Display channel configuration parameters
Main File Summary VLAN Networking Interface Security System Services Help	

Descriptions for these commands begin on page 19-7. The commands in this sub-menu below **crechnl** are used to configure OmniChannel; documentation for OmniChannel begins on page 19-11.

Configuring 10/100 Auto-Sensing Ports (High-Density 10/100 Modules)

The **10/100cfg** command allows you to enable auto-negotiation, as well as configure link speed (10 or 100 Mbps) and the link mode (full or half-duplex) on 10/100 Ethernet ports on the ESM-100C-12 and ESM-100C-32W modules on the OmniSwitch and the ESX-100C-12W, ESX-K-100C-32W, and ESX-100C-32W modules on the Omni Switch/Router.

◆ **Note** ◆

The **10/100cfg** command can only be used with newer Ethernet modules included in Release 3.1 and later. It cannot be used with 1 and 2 port Fast Ethernet modules, such as the ESM-100F-2.

Follow these steps to configure a 10/100 port:

1. Enter **10/100cfg** at the system prompt and press **<Enter>**.
2. The system displays a prompt asking for the slot and port number:

Enter Slot/Interface :

Enter the slot number, a slash (/), and the port number of the Ethernet port that you want to configure. Press **<Enter>**.

3. The system prompts you to enable or disable auto-sensing:

Autonegotiate [y,n, or quit] (Currently enabled (y)) :

Enter **y** to enable auto-negotiation or **n** to disable auto-negotiation. Auto-negotiation can be used to determine the link speed *and* the link mode (full or half) of the connection.

If you choose **y** to enable auto-negotiation, the system will automatically detect whether the connection speed of the attached device is 10 Mbps or 100 Mbps. It can also determine whether the link mode of the connection is half- or full-duplex.

◆ **Note** ◆

Auto-negotiated ports on GSX modules display inactive ports as 1000 Mbps/full duplex.

If you enable auto-negotiation, continue with Step 6.

If you choose **n** to disable auto-negotiation, then you will be prompted for the Line Speed. Continue on with the next step.

4. If you chose to disable auto-sensing, then the following prompt displays showing the current line speed:

Line Speed [100 or 10] (Currently 100) :

Select whether you want the port to operate at 10 Mbps or 100 Mbps. The port will operate at this speed until you change it through the **10/100cfg** command later. Press **<Enter>** after you enter the Line Speed. The new line speed will take effect; no reboot is required. Continue with the next step.

5. The following prompt displays, showing the current link mode:

Link Mode [Full, Half] (Currently (H)alf Duplex) :

Enter **F** to set the port to full-duplex mode or **H** to set the port to half-duplex mode. In full-duplex mode, the full 100 or 10 Mbps of bandwidth is used for data traveling on each direction of the cable. Press **<Enter>** after you enter the Mode. The new mode will take effect; no reboot is required. You have completed the configuration of this port.

6. Since you have enabled auto-negotiation, the port will automatically sense the line speed of the connection. You can also further enable auto-negotiation for the link mode. When the following prompt displays:

Link Mode [Half or Auto] (Currently (H)alf Duplex) :

select whether you want the port to auto-sense the duplex mode (**Auto**) or whether you want the port to default to half-duplex mode (**Half**). Enter an **A** for auto-sensing or enter an **H** for half-duplex.

If you set the mode to half-duplex, then the port will always run in half-duplex. If you set the mode to **Auto**, then the port will automatically detect whether the connection is half- or full-duplex and then operate in that mode. You have completed the configuration of this port.

Connecting High-Density 10/100 Modules to Non-Auto-Negotiating Links

The ESM-100C-12, ESM-100C-32W, ESX-100C-12W, and ESX-100C-32W can auto-negotiate link speed. However, if you hard-configure (auto-negotiation disabled) a high-density 10/100 module port for 10 Mbps, then you should not connect that port to a non-auto-negotiating 100 Mbps port or device.

Configuring High-Density Ethernet Ports (10 Mbps and Fast Ethernet Modules)

The **10/100cfg** command allows you to configure the link mode (full or half-duplex) for ports on newer high-density Ethernet modules.

This procedure describes how to configure ports on the ESM-100FM-8, ESM-FM-16W, ESM-C-16, ESM-C-32, and ESM-T-24W modules on the OmniSwitch and Ethernet modules on the Omni Switch/Router.

◆ Note ◆

The **10/100cfg** command can only be used with newer Ethernet modules included in Release 3.1 and later. It cannot be used with 1 and 2 port Fast Ethernet modules, such as the ESM-100F-2.

Follow these steps to configure a high-density Ethernet port:

1. Enter **10/100cfg** at the system prompt and press **<Enter>**.
2. The system displays a prompt asking for the slot and port number:

Enter Slot/Interface :

Enter the slot number, a slash (/), and the port number of the Ethernet port that you want to configure. Press **<Enter>**.

3. The following prompt displays, showing the current link mode:

Link Mode [Full, Half] (Currently (H)alf Duplex) :

Enter **F** to set the port to full-duplex mode or **H** to set the port to half-duplex mode. In full-duplex mode, the full 100 or 10 Mbps of bandwidth is used for data traveling on each direction of the cable. Press **<Enter>** after you enter the Mode. The new mode will take effect; no reboot is required.

High-Density Modules With 10 Mbps Ports

The ESM-FM-16W, ESM-C-16, ESM-C-32, ESM-T-24W, and ESX-FM-24W modules contain only 10 Mbps ports. You should not plug 100 Mbps non-auto-negotiating links into ports on these modules.

Viewing Configurations for High-Density and 10/100 Ethernet Modules

The **10/100vc** command allows you to view the current status of newer Ethernet modules (see *High-Density, 10/100, and Gigabit Ethernet (Mammoth) Modules* on page 19-4). These modules are part of Release 3.1 or later and they support 10 Mbps, 100 Mbps, or 1000 Mbps Ethernet. Ethernet 10/100 ports (e.g., *ESM-100C-12*) can auto-sense the connection speed of the attached device.

Entering **10/100vc** displays information similar to the following:

10/100 Configure Values for all slots

Slot/ Intf	Auto- negotiate	DETECTED		SET	
		Line Speed	Duplex Mode	Line Speed	Duplex Mode
5/ 1	enabled	?	?	auto	half-d
5/ 2	enabled	10	HALF-D	auto	half-d
5/ 3	enabled	100	HALF-D	auto	half-d
5/ 4	enabled	100	HALF-D	auto	half-d
5/ 5	enabled	?	?	auto	half-d
5/ 6	enabled	10	HALF-D	auto	half-d
5/ 7	enabled	100	HALF-D	auto	half-d
5/ 8	enabled	?	?	auto	half-d

Slot/Intf. The slot and port number (Intf) where this Ethernet port is located.

Auto-negotiate. Indicates whether auto-negotiation is enabled on a 10/100 port. If enabled, the port will automatically sense whether the attached device operates at 10 Mbps or 100 Mbps and adjust accordingly. If disabled, the port does not automatically detect the connection speed and instead uses the line speed you configure through the **10/100cfg** command. You enable or disable auto-negotiation through **10/100cfg**. A value of **n/a** in this column means the port does not support auto-sensing and the line speed defaults to either 10 or 100 Mbps.

The next set of columns are divided into DETECTED and SET. The columns under DETECTED are the current operational **Line Speed** or **Duplex Mode**. The columns under SET are the configured values; these configured values will either be defaults or the values configured through **10/100cfg**.

Line Speed. Indicates the speed (in Mbps) at which the port is currently operating (DETECTED) or configured to operate (SET).

DETECTED values will be **10** (Mbps), **100** (Mbps), or a question mark (?). A question mark (?) in this column indicates the port is not connected to a device.

SET values will be **auto**, **10** (Mbps,) or **100** (Mbps). The **auto** setting means auto-sensing is enabled and the Line Speed will equal the speed for which the attached device is configured.

Duplex Mode. Indicates whether the port is operating (DETECTED) or configured (SET) for half- or full-duplex mode.

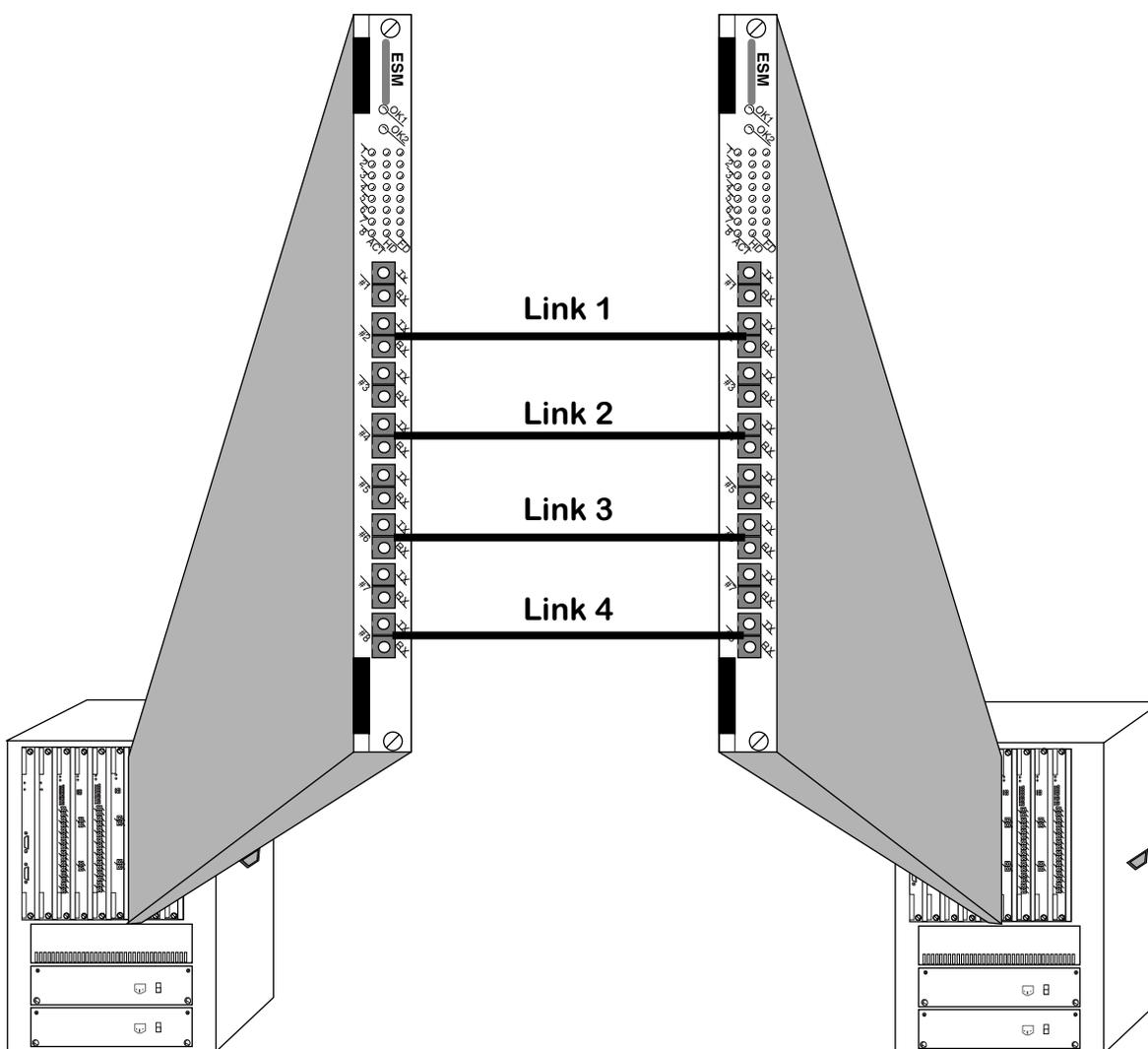
DETECTED values will be half-duplex (**HALF-D**), full-duplex (**FULL-D**), or a question mark (?). A question mark (?) in this column indicates the port is not connected to a device.

SET values will be auto-sensing (**auto**), half-duplex (**half-d**), or full-duplex (full-d). If this value is **auto**, then the switch automatically sets the duplex mode to the network device's setting. If this value is **half-d**, then the port will always run in half-duplex mode. If this value is **full-d**, then the port will always run in full-duplex mode. You configure the duplex mode through the **10/100cfg** command. Note that you can only configure a 10/100 port for full-duplex if you disable auto-sensing.

OmniChannel

OmniChannel allows you to increase the bandwidth of Fast backbones by combining the capacity of up to four (4) Fast Ethernet ports into one channel. The combined channel operates within Spanning Tree as one virtual port, and can provide up to 800 Mbps (in full-duplex mode) of bandwidth. (In full-duplex mode, 400 Mbps is supported in each direction of the OmniChannel.) This feature is useful for Ethernet-intensive networks that need to increase bandwidth capacity without setting up ATM backbones using OC-3 or OC-12 connections.

The OmniChannel feature operates only on 10/100 and Fast Ethernet ports employing Mammoth chip technology, such as those modules listed in the table, *High-Density, 10/100, and Gigabit Ethernet (Mammoth) Modules* on page 19-4. OmniChannel is also supported on ESX-K series Kodiak-based Ethernet modules listed in the table on page 19-5. OmniChannel does not operate on 10 Mbps ports or on early-generation Fast Ethernet ports, such as those listed in the table, *Early Generation OmniSwitch Ethernet Modules* on page 19-3.



Up to Four 100 Mbps Links May Comprise an OmniChannel Backbone

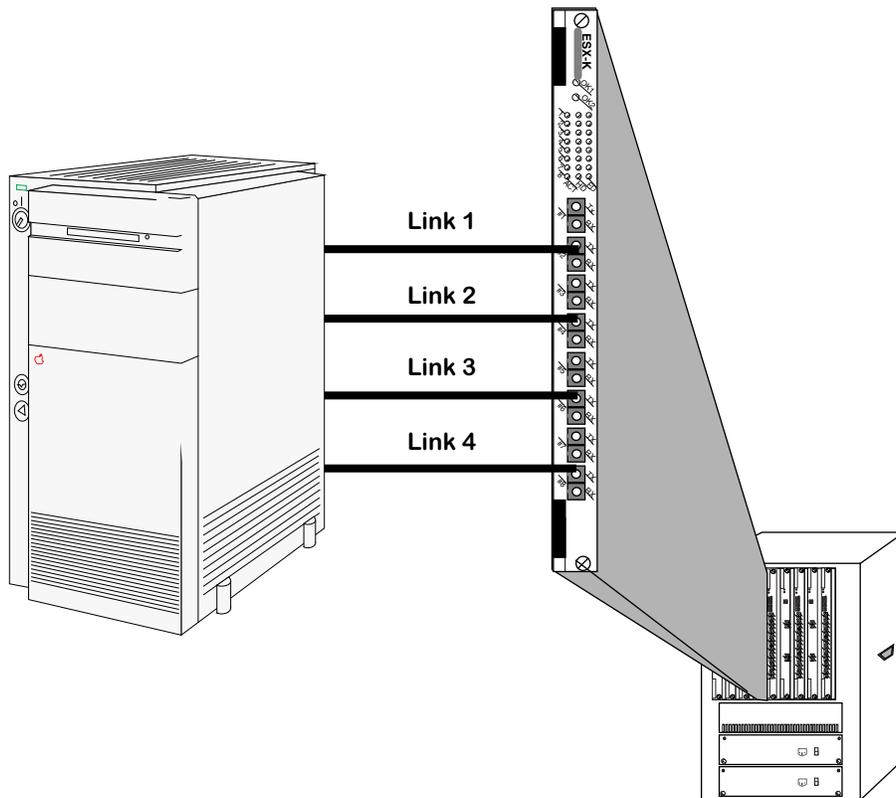
◆ Note ◆

For Kodiak-based 10/100 Ethernet modules, 802.1Q is supported over OmniChannel. See Chapter 20, “Managing 802.1Q Groups” for more information.

OmniChannel balances the traffic load among links by MAC address. MAC addresses are assigned to physical links in the OmniChannel in a round-robin fashion. The first MAC address learned will transmit and receive data on the first link. The second MAC address learned will transmit and receive over the second link, and so on regardless of the bandwidth requirements of each MAC address.

The Server Channel Feature

For ESX-K Series Kodiak-based Ethernet boards, you can create an OmniChannel that connects to a server instead of another OmniSwitch. The intention of the Server Channel is to give the user the option to increase the bandwidth between a server and Omni Switch/Router for more client request support. This functionality is especially useful for internet servers such as B2C and B2B servers.



Up to Four 100 Mbps Links May Comprise a Server Channel backbone

Server Channel Limitations

The following are limitations to creating a server channel on the Omni Switch/Router:

- The maximum number of Server Channels in the whole box is not fixed; however, it is suggested that no more than 16 be created on the same switch.
- Each Server Channel can support up to 4 ports.
- Within one Server Channel, all of channel ports must be on the same slot.
- Within one Server Channel, all of channel ports must be in one VLAN.
- A port cannot be configured as Server Channel and Omni Channel port at the same time.
- Currently, Server Channel cannot be used with 802.1Q.

Creating an OmniChannel

You use the **crechnl** command to create an OmniChannel. Follow these steps:

1. Enter **crechnl**.
2. The following prompt displays:

Channel Number (2):

Enter the identification number you want to assign to this OmniChannel. By default, the software lists the next available channel number in parentheses. (In this example, the next available channel number is **2**.) If you want to select the default, simply press **<Enter>**. Otherwise, enter the desired channel number and press **<Enter>**.

3. The following prompt displays:

Channel type (1) omni_chnl (2) server_chnl

If the far end of the link is another OmniSwitch or Switch/Router, you need to create an OmniChannel. Select **1** and proceed to the next step. If the far end of the link is a server, select **2** to create a Server Channel.

4. The following prompt displays:

To select a port, use the convention - Slot/Physical Port.

For eg. 2/1 is used to select Physical Port 1 on Slot 2

Primary Slot/Port:

Enter the slot and port that the switch will initially use as the Spanning Tree virtual port for this channel. Each OmniChannel is considered a single virtual port within the network, so only one physical port will participate in Spanning Tree.

◆ Note ◆

After a reboot or after a loss of a connection, the first port in an OmniChannel that the switch brings up will become the primary port. Therefore, one of the ports you choose as the secondary port (explained in Step 5 below) could become the primary port and thus participate in Spanning Tree.

If the port you enter is already part of another OmniChannel, then it cannot be used in a second OmniChannel. The following message displays for those ports that are already part of another OmniChannel:

Primary port in use

5. The following prompt displays:

To select a port, use the convention - Slot/Physical Port.

For eg. 2/1 is used to select Physical Port 1 on Slot 2

Secondary Slot/Port:

Enter the other ports that will be used in this OmniChannel. Up to four (4) Fast Ethernet Ports may participate in an OmniChannel. Therefore, you can specify up to three (3) additional ports which will initially become secondary ports. These secondary ports must be on the same module as the primary port. Secondary ports do not participate in the Spanning Tree algorithm; they are used for data transmission only.

◆ Note ◆

As explained in Step 4 above, a port that you initially configure as a secondary port can become a primary port.

Specifying a Range of Ports. To specify a range of ports, enter the slot number, a slash (/), the port number for the first secondary port, a dash (-), and the port number for the last secondary port. For example, to specify ports 3, 4, and 5 on the Fast Ethernet module in slot 2 as secondary ports in an OmniChannel, you would enter:

2/3-5

Specifying Multiple Ports. To specify multiple ports (on the same module) that are not physically contiguous, enter the slot number, a slash (/), the port number for the first secondary port, a comma (,), and then the slot and port for the next secondary port. For example, to specify ports 3 and 5 on the Fast Ethernet module in slot 2, you would enter:

2/3, 2/5

The order in which you specify secondary ports is important. In the event of a failure on the primary port, the first secondary port specified will become the primary port in the OmniChannel and participate in Spanning Tree.

Messages will display, informing you that secondary ports were saved in flash memory:

Successfully saved sec port in flash

Successfully saved sec port in flash

Adding Ports to an OmniChannel

After you create an OmniChannel with the **crechnl** command, you can add more secondary ports to the same channel as long as the channel contains less than 4 ports. You use the **addprtchnl** command to add ports to an OmniChannel. Follow these steps:

1. Enter **addprtchnl**.
2. The following prompt displays:

Channel Number :

Enter the channel number to which you want to add secondary ports. You can check the current port assignments for a given OmniChannel by using the **chnlinfo** command, which is described in *Viewing OmniChannel Parameters* on page 19-16.

3. The following prompt displays:

**To select a port, the convention - Slot/Physical Port or Slot/Phy.
Port Range. For eg. 2/1 is used to select Physical Port 1 on Slot
2 and 2/2-4 selects physical ports 2,3 and 4 on Slot 2
Slot/Port(s):**

Enter the additional ports that will be part of this OmniChannel. All the ports you enter will initially be secondary ports (i.e., they do not participate in the Spanning Tree algorithm and are used for data transmission only). You can specify up to 4 ports on an OmniChannel; only 3 of the ports can be secondary ports.

Specifying a Range of Ports. To specify a range of ports, enter the slot number, a slash (/), the port number for the first secondary port, a dash (-), and the port number for the last secondary port. For example, to specify ports 3, 4, and 5 on the Fast Ethernet module in slot 2 as secondary ports in an OmniChannel, you would enter:

2/3-5

Specifying Multiple Ports. To specify multiple ports (on the same module) that are not physically contiguous, enter the slot number, a slash (/), the port number for the first secondary port, a comma (,), and the slot and port for the next secondary port. For example, to specify ports 3 and 5 on the Fast Ethernet module in slot 2, you would enter:

2/3, 2/5

Messages will display, informing you that secondary ports were saved in flash memory:

**Successfully saved sec port in flash
Successfully saved sec port in flash**

Deleting an OmniChannel

You can delete any existing OmniChannel through the **delchnl** command. Follow these steps:

1. Enter **delechnl**.
2. The following prompt displays:

Channel to be deleted:

Enter the channel number that you want to delete. You can obtain information on a channel through the **chnlinfo** command, which is described in *Viewing OmniChannel Parameters* on page 19-16. Press **<Enter>** and the channel, along with all port assignments, will be deleted.

Deleting Ports from an OmniChannel

You can delete ports from an OmniChannel using the **delprtchnl** command. Follow these steps:

1. Enter **delprtchnl**.
2. The following prompt displays:

Channel Number :

Enter the channel number on which you want to delete ports. You can check the current port assignments for a given OmniChannel by using the **chnlinfo** command, which is described in *Viewing OmniChannel Parameters* on page 19-16.

3. The following prompt displays:

**To select a port, the convention - Slot/Physical Port or Slot/Phy.
Port Range. For eg. 2/1 is used to select Physical Port 1 on Slot
2 and 2/2-4 selects physical ports 2,3 and 4 on Slot 2
Slot/Port(s):**

Enter the port(s) that you want to delete from this OmniChannel.

Important Note

If you delete the primary port a secondary port will become the new primary port. The secondary port that will take over this role is the first secondary port specified through the **crechnl** command.

Deleting a Range of Ports. To delete a range of ports, enter the slot number, a slash (/), the port number for the first port, a dash (-), and the port number for the last port. For example, to delete ports 3, 4, and 5 on the Fast Ethernet module in slot 2, you would enter:

2/3-5

Deleting Multiple Ports. To delete multiple ports (on the same module) that are not physically contiguous, enter the slot number, a slash (/), the port number for the first port, a comma (,), and the slot and port for the next port. For example, to delete ports 3 and 5 on the Fast Ethernet module in slot 2, you would enter:

2/3, 2/5

Viewing OmniChannel Parameters

You can view the current configuration parameters and port assignments for an OmniChannel by using the **chnlinfo** command. Follow these steps:

1. Enter **chnlinfo**.
2. The following prompt displays:

Enter channel number for which information is required:

Enter the channel number for which you want to view information. If you want to view information on all OmniChannels in the switch, simply press **<Enter>**.

3. A screen similar to the following displays:

Displaying channel 2			
Channel Id	Phy. Port	Port Status	Mac Count
2	5/6	Inactive	0
	5/7	Inactive	0
3	5/3	Active	35
	5/4	Active	34
	5/5	Active	34

The following sections describe the variables in this table.

Channel Id. The identification number assigned to this OmniChannel during the **crechnl** configuration procedure.

Phy. Port. The physical slot and port number for all ports included in the OmniChannel. The slot number is listed first, then a slash (/), and the port number on the Ethernet module.

Port Status. The current operational status of this physical port. If the port is **Active**, then a cable is connected and data is capable of passing to and from the port. If the port is **Inactive**, then a cable may not be attached or the port is inoperational for hardware or software reasons.

Mac Count. The current number of MAC addresses that have been learned on this port. A separate MAC count is given for each physical port in the OmniChannel.

Configuring Older Fast Ethernet Ports

The **eth100cfg** command allows you to alter the Link Mode of some Fast Ethernet modules. The Link Mode may be set to half-duplex or full-duplex. The **eth100cfg** command can only be used with the following modules:

- ESM-100C-FD
- ESM-100FM-FD
- ESM-100FS-FD
- ESM-100C-5
- ESM-100FM-5
- ESM-100FS-5

It cannot be used with the ESM-100C shared-port module or the high-density and 10/100 Ethernet modules.

Follow these steps to configure the Link Mode on a Fast Ethernet port:

1. Enter **eth100cfg** at the system prompt and press **<Enter>**.
2. The system displays a prompt, asking for the slot and port number:

Enter Slot/Interface :

Enter the slot number, a slash (/), and the port number of the Fast Ethernet port that you want to configure. Press **<Enter>**.

3. The system displays the current Link Mode and prompts you for the mode to which you want to configure this port:

Link Mode [F or H] (Current Mode is Full Duplex (F)) :

Enter **F** to set the port to full-duplex mode or **H** to set the port to half-duplex mode. In full-duplex mode, the full 100 Mbps of bandwidth is used for data traveling on each direction of the cable. Press **<Enter>** after you enter the Mode. The new mode will take effect; no reset is required.

Viewing Fast Ethernet Configurations

The **eth100vc** command allows you to view the current status of Fast Ethernet ports in the switch. Entering **eth100vc** displays information similar to the following:

100BaseT Port Status Table for all slots

Slot/ Intf	Port Type	Link Mode	Link Type
2/ 1	100BaseTx (4 port)	Half Duplex	Copper
3/ 1	100BaseTx	Full Duplex	Copper
3/ 2	100BaseTx	Full Duplex	Copper
4/ 1	100BaseFx	Full Duplex	Single Mode Fiber
4/ 2	100BaseFx	Full Duplex	Multi Mode Fiber

Slot/Intf. The slot and port number (Intf) where this Fast Ethernet port is located.

Port Type. Indicates whether this is a 100BaseTx port or a 100BaseFx (fiber) port. Some 100BaseTx ports are actually shared among four RJ-45 connectors. In such cases, these ports are identified as **100BaseTx (4 port)** in the table. An example of such a port is shown in the first row of the table above.

Link Mode. Indicates whether the port is currently operating in half-duplex or full-duplex mode. The 4-port shared 100BaseTx modules operate only in half-duplex mode. However, other Fast Ethernet modules may be configured to operate in either half- or full-duplex mode. You can configure the mode through the **eth100cfg** command, which is described in the next section.

Link Type. Describe the physical interface of the port. The ports will either be copper (100BaseTx) or fiber (100BaseFx). In addition, fiber ports may be either single-mode or multi-mode—this column also indicates the mode of the fiber.

Selecting the Aggressive Ethernet Back-Off Algorithm

The OmniSwitch supports two Ethernet back-off algorithms. The default is the standard back-off algorithm that complies with IEEE 802.3. The second algorithm is more aggressive. It gives the OmniSwitch priority to transmit onto Ethernet media and lessen the possibility that the switch will drop a packet when the Ethernet media experiences high traffic.

◆ **Note** ◆

This algorithm selection feature is not available on high-density and 10/100 (Mammoth) Ethernet ports.

You can select the aggressive back-off algorithm through a command line within the **mpm.cmd** initialization file. To use the aggressive algorithm, edit the **mpm.cmd** file to add the following line:

```
esmDoMBA=1
```

Make sure you enter this line before the line, **cmInit**. (Refer to Chapter 11, “Managing Files,” for instructions on how to edit the **mpm.cmd** file.) After adding this line, you must reboot the switch for the change to take effect.

You can also go back to the default IEEE 802.3 back-off algorithm by deleting the **esmDoMBA** line, or by changing the line’s value to **0**, as follows:

```
esmDoMBA=0
```

20 Managing 802.1Q Groups

This chapter documents User Interface (UI) commands to manage 802.1Q groups. For documentation on Command Line Interface (CLI) commands to manage 802.1Q groups, see the *Text-Based Configuration CLI Reference Guide*.

◆ Important Note ◆

In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. See Chapter 8, “The User Interface,” for documentation on changing from CLI mode to UI mode.

802.1Q is an IEEE standard for sending frames through the network tagged with VLAN identification. Alcatel has developed its own implementation of VLANs that closely follows the IEEE standard (and enhances it). However, Alcatel VLANs and 802.1Q VLANs cannot interoperate without special configuration.

If your network uses 802.1Q tagging, you will need to create 802.1Q groups and specify ports that will handle 802.1Q traffic. This can be done for 10/100, Fast Ethernet and Gigabit Ethernet Mammoth and Kodiak ASIC-based modules. Up to 64 groups can be supported using multiple spanning tree on an 802.1Q link for Kodiak ASIC-based Fast Ethernet and Gigabit Ethernet modules.

For Release 4.4 and later, Kodiak ASIC-based 10/100 Ethernet modules support 802.1Q traffic over OmniChannel in multiple spanning tree mode. However, you must first create an OmniChannel before creating 802.1Q groups. See Chapter 19, “Managing Ethernet Modules” for information about OmniChannel. See *Single vs. Multiple Spanning Tree* on page 20-4 for information on single and multiple spanning tree.

Support for 802.1Q in the OmniSwitch allows you to set up port-based groups that interoperate with 802.1Q-compliant equipment from other networking vendors.

On Mammoth ASIC-based Gigabit Ethernet modules only, a proprietary version of 802.1Q called X802.1Q is also supported. See *X802.1Q vs. IEEE 802.1Q* on page 20-4 for additional information on the differences between these versions. X802.1Q is not supported on Kodiak ASIC-based Gigabit Ethernet modules.

Ports added to an 802.1Q group are done using Ethernet switch services. When using the service commands to add ports to an 802.1Q group, multiple spanning tree instances on a single port are supported. See *Single vs. Multiple Spanning Tree* on page 20-4 for additional information on the differences between single and multiple spanning tree.

The 802.1Q specification defines *trunk* and *access* ports (and links). Trunk links are LAN segments used for multiplexing VLANs between VLAN bridges. All devices that are directly connected to a trunk link must be VLAN-aware. Access links are LAN segments used to multiplex one or more VLAN-unaware devices into a port of a VLAN bridge. (This also includes a hybrid with some tagged and some untagged Groups.)

◆ Note ◆

The use of the word *trunk* in this document should not be confused with the IEEE use of *trunking* with link aggregation (such as OmniChannel and IEEE 802.3ad). The general meaning of a trunk is an inter-switch link over which different types of traffic are multiplexed.

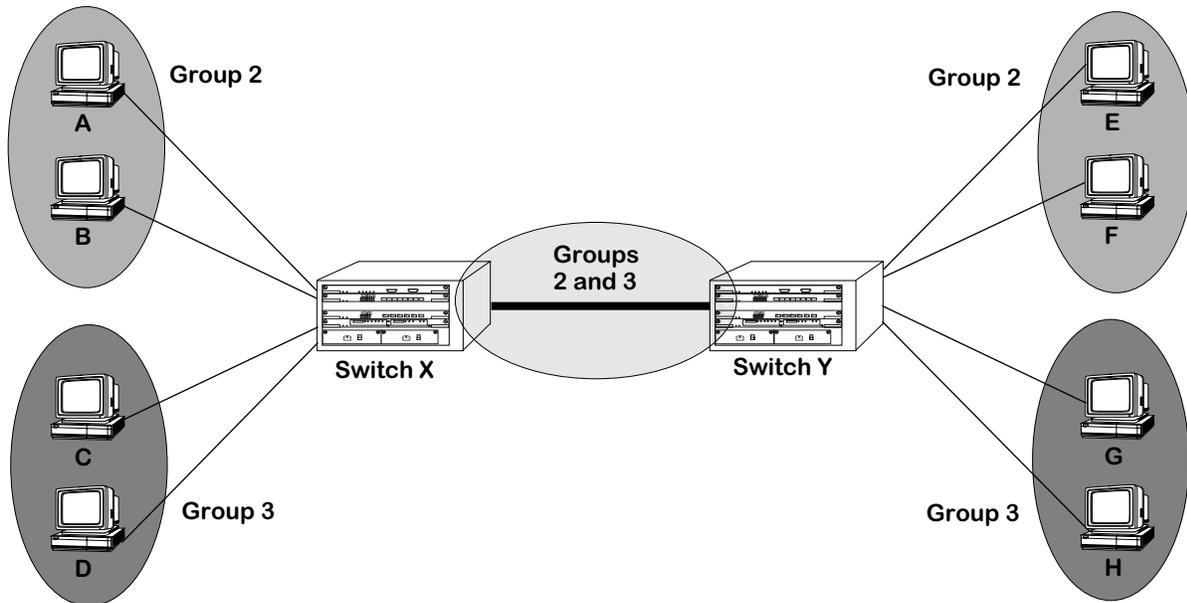
IEEE 802.1Q Sections Not Implemented

Some portions of the 802.1Q specification have not yet been implemented in the Omni Switch/Router. These include the following:

- The tunneling of non-canonical 802.5 frames is not supported, since the Alcatel Omni S/R handles such traffic by frame translations. This tunneling mode of operation involves the Token Ring Encapsulation Flag in the 802.1Q header. It is not set or interpreted in the Alcatel Omni S/R implementation.
- The Alcatel Omni S/R implementation does not support the SNAP-encoded Tag Header (which is intended for Token Ring LANs). Only the Ethernet-encoded 4-byte Tag Header is supported (and only Ethernet LANs are supported).
- Alcatel Omni S/R does not support the Generic Attribute Registration Protocol (GARP) Multicast Registration Protocol (GMRP) and GARP VLAN Registration Protocol (GVRP) that are defined in 802.1Q.

Application Example

The following diagram illustrates a simple 802.1Q application:



Simple 802.1Q Application

In the above diagram, the PC devices (endstations) need to be segmented into different 802.1Q VLANs. The switch port to which each device attaches is assigned to an 802.1Q group (Group 2 for endstations A, B, E, and F, and Group 3 for endstations C, D, G, and H).

The ports connecting Switch X and Switch Y are also added to 802.1Q groups 2 and 3. All of the switch ports that handle 802.1Q traffic are now capable of passing 802.1Q information.

Prior to Release 4.4, only Mammoth ASIC-based Ethernet, Fast Ethernet and Gigabit Ethernet modules could be part of an 802.1Q group. For Release 4.4 and later, Kodiak ASIC-based 10/100, Fast Ethernet and Gigabit Ethernet modules also support 802.1Q groups. In either configuration, existing policies for a group will not be affected by the group's support for 802.1Q.

◆ Important Note ◆

Kodiak ASIC-based 10/100 Ethernet modules support 802.1Q traffic over OmniChannel in multiple spanning tree mode. However, for 802.1Q support over OmniChannel, you must first create an OmniChannel before creating 802.1Q groups. See Chapter 19 for information about OmniChannel. For information on the differences between single and multiple spanning tree, see *Single vs. Multiple Spanning Tree* on page 20-4.

By matching switch ports with 802.1Q groups, you are statically assigning the port to the group. Once assigned, an 802.1Q port cannot be dynamically assigned to another group. However, the same switch port can be statically assigned to more than one 802.1Q group.

X802.1Q vs. IEEE 802.1Q

Alcatel's original implementation of the 802.1Q specification (prior to its official approval) was a proprietary version called X802.1Q. This proprietary version is only available on Mammoth ASIC-based Gigabit Ethernet modules. X802.1Q is not supported on Kodiak ASIC-based Gigabit Ethernet modules.

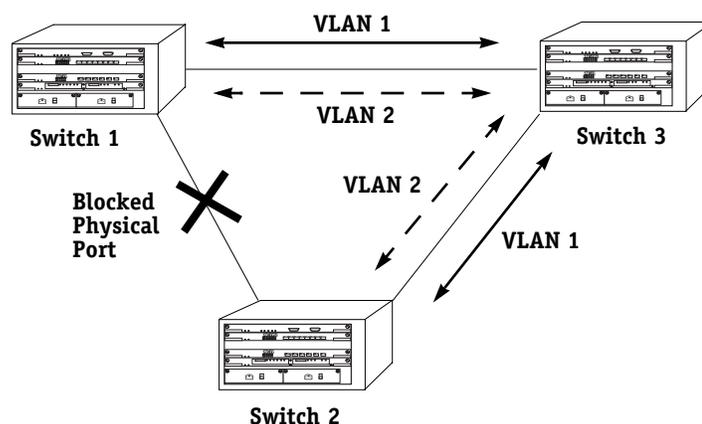
When adding an 802.1Q group to a Gigabit port, a field in the display allows you to select either the proprietary 802.1Q (X802.1Q) or IEEE 802.1Q. For more information on adding an X802.1Q group to a port, see *Configuring 802.1Q on Gigabit Ethernet Ports* on page 20-12.

When implementing X802.1Q on Gigabit Ethernet modules, use the following guidelines:

- The number of groups must be equal on both sides of the link.
- The group IDs must be the same on both sides of the link.
- You must add groups in the same order on both ends of the link. For example, if you add groups 1, 2, 3, 4, and 5 on the local switch, you must add the same five groups in the same order on the remote switch. *If groups are not added in this manner, 802.1Q packets will not be routed correctly.*
- You must delete groups in the same order on both ends of the link. For example, if you delete groups 1, 2, 3, 4, and 5 on the local switch, you must delete the same five groups in the same order on the remote switch. *If groups are not deleted in this manner, 802.1Q packets will not be routed correctly.*
- You must use Alcatel equipment on both sides of the link.

Single vs. Multiple Spanning Tree

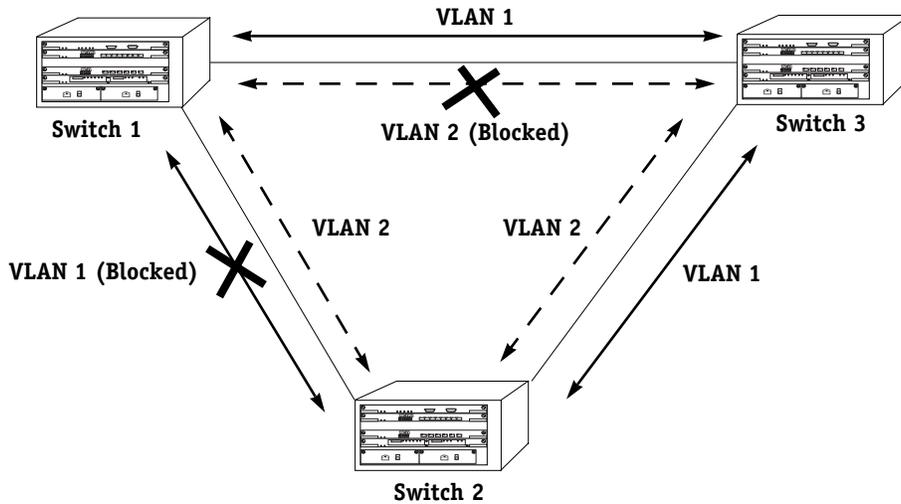
In previous releases of the OmniSwitch software (4.0 and earlier), spanning tree support was done on a per port basis. In other words, a physical port could only participate in one instance of a spanning tree on the network. If a network is passing both untagged and IEEE tagged frames, single spanning tree support could lead to packets being lost. Lost packets could occur if a port specifically assigned to handle one type of traffic (e.g., IEEE 802.1Q) is blocked by spanning tree, forcing traffic for that port to move to a port not assigned to handle IEEE 802.1Q traffic.



Port Based Spanning Tree

In the above diagram, the physical connection between Switch 1 and Switch 2 is blocked by spanning tree. No traffic can pass over the connected ports.

Release 4.1 (and later) of the Omni Switch/Router allows for multiple spanning tree instances on a single port. Put another way, a port can be part of separate spanning trees, with no impact on packet delivery. This is done by basing spanning tree configuration on groups rather than physical ports.

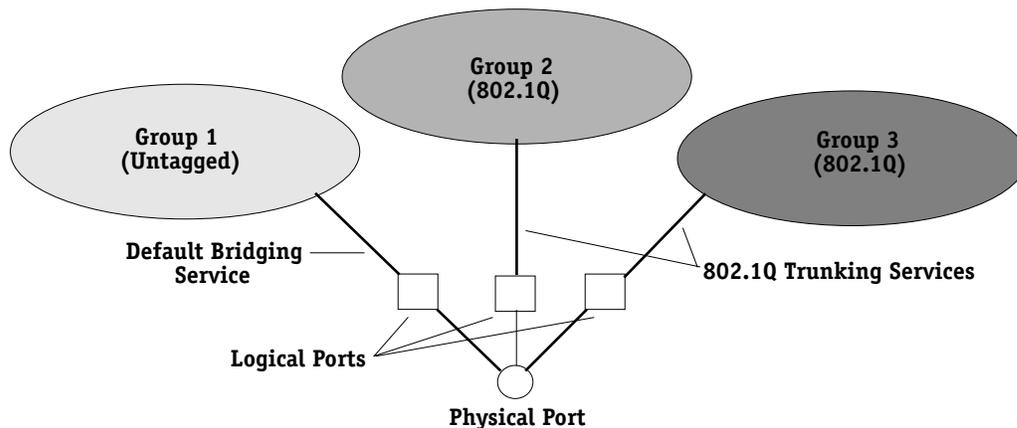


Group Based Spanning Tree

The above diagram shows how traffic on VLAN 1 is blocked between Switch 1 and Switch 2, while VLAN 2 traffic is allowed to pass. The reverse is true for Switch 1 and Switch 3 (i.e., VLAN 2 traffic is blocked, while VLAN 1 traffic is allowed to pass).

Service commands are used in Ethernet modules to assign groups to 10/100 and Gigabit ports. The **cas**, **das**, **mas**, and **vas** commands create, delete, modify, and view trunking services created to handle 802.1Q traffic over an Ethernet backbone. This trunking service, coupled with the default bridging service, allows you to pass both tagged and untagged frames over the same port.

The following diagram shows the logical structure of the trunked 802.1Q groups:



Logical Configuration of Multiple Groups on a Single Port

In the above diagram, Groups 2 and 3 have been trunked to the physical port with an 802.1Q trunking service.

Since spanning tree is group based, the physical port in the above diagram participates in three spanning tree instances: one for untagged traffic and two for 802.1Q tagged traffic. Both types of frames can now pass through the same port.

◆ **Important Notes** ◆

Since a trunk is a service, and Alcatel switches have a 16 (10/100) or 15 (Gigabit) services per port limit, only 15 or 14 802.1Q groups can be added to the same port. In both cases, a default bridge service occupies one of the service slots.

For Kodiak ASIC-based Fast Ethernet and Gigabit Ethernet modules, up to 64 groups are supported using multiple spanning tree on an 802.1Q link. To support 64 groups, the following lines should be added into the **mpx.cmd** file :

MaxEthQGroups=64
MaxGigaQGroups=64

See Chapter 11, “Managing Files,” for more information on editing text files.

Giga I and II ASIC Modules

Some early versions of the Gigabit Ethernet modules for the Omni Switch/Router use the Giga I or II ASIC. These modules do *not* support standard IEEE 802.1Q tagging.

You can use the **slot** command to determine if your Gigabit Ethernet module uses the Giga 1 or II ASIC. Use the number shown in the **Part-Number** field displayed by the **slot** command and compare it to the number in the **Part Number** columns in the table below. For example, if you have a GSX-FM-2 and the number in the **Part-Number** field shown by the **slot** command is **05023726**, then your module has a Giga 1 ASIC.

◆ **Note** ◆

See Chapter 13, “Switch-Wide Parameters,” for more information on the **slot** command

Gigabit Ethernet Modules with the Giga I or II ASIC

Module	Part Number for Giga I (Shown in Slot Command)	Part Number for Giga II (Shown in Slot Command)
GSM-FM-2	N/A	05026129
GSM-FS-2	N/A	05026130
GSX-FM-2	05023726	05023731
GSX-FM-4	05021526	05021529
GSX-FS-2	05023728	05023730
GSX-FS-4	05021528	05021530

For information on configuring 802.1Q groups for use over Gigabit ports, see *Configuring 802.1Q on Gigabit Ethernet Ports* on page 20-12.

Assigning an 802.1Q Group to a Port

Previous versions of the OmniSwitch (version 4.0 and earlier) only allowed for single spanning tree configured 802.1Q groups using the **addqgp**, **viqgp**, and **delqgp** menu commands. These commands were invalidated in the 4.1 release and replaced by the **cas**, **mas**, **vas**, and **das** service commands.

The procedure for assigning an 802.1Q group to a port is slightly different, depending on whether the port is a 10/100 or Gigabit Ethernet module port. (For additional information on Gigabit and Kodiak-based Ethernet modules, see Chapter 19, “Managing Ethernet Modules.”) Up to 64 groups can be supported using multiple spanning tree on an 802.1Q link for Kodiak ASIC-based Fast Ethernet and Gigabit Ethernet modules.

◆ Important Notes ◆

For Release 4.4 and later, Kodiak ASIC-based 10/100 Ethernet modules support 802.1Q traffic over OmniChannel in multiple spanning tree mode. However, you must first create an OmniChannel before creating 802.1Q groups. See Chapter 19, “Managing Ethernet Modules” for information about OmniChannel.

For information about the differences between single and multiple spanning tree, see *Single vs. Multiple Spanning Tree* on page 20-4.

In most of the procedures described in this section, the screens displayed vary, depending on what type of board and ASIC you are using. By viewing the front panel of your module, it should be easy to determine which procedure applies to you.

Ethernet modules are designated by either ESX or ESM. Gigabit modules are designated by either GSX or GSM. Modules with a **K** on the front panel are Kodiak ASIC-based modules. No **K** means it is a legacy board. For example, a module with designation **GSX-K** is a Gigabit module using a Kodiak ASIC.

◆ Note ◆

Remember that Gigabit modules can have different versions of the Mammoth ASIC. See *Giga I and II ASIC Modules* on page 20-7 for more information.

For information on assigning an 802.1Q group to a 10/100 port, see *Configuring 802.1Q on 10/100 Ethernet Ports* on page 20-9. For information on assigning an 802.1Q group to a Gigabit port, see *Configuring 802.1Q on Gigabit Ethernet Ports* on page 20-12.

◆ Note ◆

802.1Q OmniSwitch and Omni Switch/Router tagging does not work with OmniCore 5200 tagging unless the OmniCore software is version 3.0.19 or later.

Configuring 802.1Q on 10/100 Ethernet Ports

Use the **cas** command to assign 802.1Q groups to 10/100 ports. To use this command, follow the steps below.

1. Enter **cas** at the system prompt, as shown:

```
cas <slot>/<port>
```

where **<slot>** is the slot of the module, and **<port>** is the port number that is to be added to the group. For example, to add port 3 on slot 5, you would enter:

```
cas 5/3
```

2. If you have a legacy 10/100 board, the following screen displays:

```
Slot 3 Port 5 Ethernet 802.1Q Service
1) Description          :
2) Group ID            :
3) Tag                 :
4) Priority             :
5) Mode
   Multiple Spanning Tree (3)
   Single Spanning Tree (4) :
```

If you have a Kodiak 10/100 board, the following screen displays:

```
Slot 3 Port 5 Ethernet 802.1Q Service
1) Description          :
2) Group ID            :
3) Tag                 :
5) Mode
   Multiple Spanning Tree (3)
   Single Spanning Tree (4) :
```

You can modify the parameters by entering the line number, an equal sign, and the value for the parameter. For example, to change the **Group ID** to **5**, you would enter **2** (the line number for **Group ID**), an equal sign (=), and a **5** (the group number), as shown:

```
2=5
```

3. Remember to save your changes by entering **save** at the system prompt when you have finished with the configuration.

◆ Important Notes ◆

Because 802.1Q support over OmniChannel is supported only in **Multiple Spanning Tree** mode on Kodiak 10/100 Ethernet boards, the **Mode** screen option is not configurable for this feature.

For 802.1Q support over OmniChannel, you must first create an OmniChannel before creating 802.1Q groups. See Chapter 19, “Managing Ethernet Modules” for information about OmniChannel.

The following sections describe the parameters shown in the screen on the preceding page.

Description

A textual description (up to thirty characters) for the service created when adding the port to a group.

Group ID

The number of the group to which the port is to be added.

Tag

A simple identifier that is added to 802.1Q packets for identification. This value can be any number between 1 and 4094.

Priority/Priority Remap Values

If the module uses a Kodiak ASIC, this field is labeled either **Priority** or **Priority Remap Values**. In single spanning tree mode, it is **Priority**. In multiple spanning tree mode, it is **Priority Remap Values**. See **Mode** below for more detailed information.

◆ Important Notes ◆

ESX-K and GSX-K Kodiak ASIC-based modules support 802.1p traffic prioritization. For chassis configurations that include only ESX-K, GSX-K and/or WSX series modules, 802.1p priority bits can be carried inbound on a tagged port (configured with multiple spanning tree 802.1Q) across the backplane. This priority information is used at the egress port to queue the packet, and is sent out in the packet whether the egress port is tagged or not.

The ESX-K and GSX-K modules can also remap incoming priority on an ingress port. If priority remapping has been configured, the new priority will be carried across the backplane. The priority information is used to queue the packet, and is sent out in the packet if the egress port is tagged.

Mode

This field allows you to choose either multiple or single spanning tree. This option only appears if the module uses 10/100 Ethernet ports. Once you select a type of spanning tree for a port, the port automatically retains the spanning tree selection for any other group it is added to.

For example, suppose that Port 3/1 is assigned to be in Group 2, and to use single spanning tree. If the port were to be assigned to another group, it would automatically set itself to use single spanning tree for that group as well.

When you set the **Mode** of the service, the **cas** screen changes to accommodate the selection and allows you to set the priority of the service. If you select single spanning tree, for example, the screen changes to the following display, as shown:

```

Slot 3 Port 5 Ethernet 802.1Q Service
1) Description           :
2) Group ID             :
3) Tag                  :
4) Priority              :
5) Mode                 : 4
    
```

If you select multiple spanning tree, the screen changes to the following display, as shown:

```

Slot 2 Port 1 Ethernet 802.1Q Service
1. Description (30 chars max) :
2. Group ID                   : 0
3. Tag                         : 0
4. Priority Remap Values      :
   40. 0 - 0
   41. 1 - 1
   42. 2 - 2
   43. 3 - 3
   44. 4 - 4
   45. 5 - 5
   46. 6 - 6
   47. 7 - 7
5. Mode                       : 3
    
```

The incoming priority level of the packet can be remapped to any value between **0** and **7**, with **7** being the highest priority. To set a value of **5** for an incoming priority value of **4**, for example, you would enter **44=5**.

For more information on single vs. multiple spanning tree, see *Single vs. Multiple Spanning Tree* on page 20-4.

Configuring 802.1Q on Gigabit Ethernet Ports

Use the **cas** command to assign 802.1Q groups to Gigabit ports. To use this command, follow the steps below.

1. Enter **cas** at the system prompt, as shown:

```
cas <slot>/<port>
```

where **<slot>** is the slot of the module, and **<port>** is the port number that is to be added to the group. For example, to add port 3 on slot 5, you would enter:

```
cas 5/3
```

2. If you have a Mammoth Gigabit module, the following prompt displays:

```
Slot 3 Port 5 Ethernet 802.1Q Service
1) Description                :
2) Group ID                   :
3) Tag                        :
4) Priority                   :
5) Mode
   Proprietary Tagging (1)    :
   IEEE Standard Tagging (2) :
```

If you have a Kodiak Gigabit module, the following prompt displays:

```
Slot 3 Port 5 Ethernet 802.1Q Service
1. Description (30 chars max) :
2. Group ID                   : 0
3. Tag                        : 0
4. Priority Remap Values      :
   40. 0 - 0
   41. 1 - 1
   42. 2 - 2
   43. 3 - 3
   44. 4 - 4
   45. 5 - 5
   46. 6 - 6
   47. 7 - 7
```

You can modify the parameters by entering the line number, an equal sign, and the value for the parameter. For example, to change the **Group ID** to **5**, you would enter **2** (the line number for **Group ID**), an equal sign (=), and a **5** (the group number), as shown:

```
2=5
```

3. Remember to save your changes by typing **save** at the system prompt when you have finished with the configuration.

◆ Note ◆

X802.1Q is supported only on Mammoth ASIC-based Gigabit Ethernet modules. It is not supported on Kodiak-based modules. You must add X802.1Q groups in the same order on both ends of the link. For example, if you add groups 1, 2, 3, 4, and 5 on the local switch, you must add the same five groups in the same order on the remote switch. *If groups are not added in this manner, X802.1Q packets will not be routed correctly.*

Most of the fields are the same as described in *Configuring 802.1Q on 10/100 Ethernet Ports* on page 20-9. The Mode feature for Mammoth Gigabit modules is different, and described below.

Mode

This field allows you to choose either the proprietary 802.1Q (X802.1Q) or IEEE 802.1Q versions. Enter **1** for X802.1Q, or **2** for IEEE 802.1Q. This option only appears if the module uses Gigabit Ethernet ports. Once you select the 802.1Q type, the port automatically retains the selection for any other group it is added to.

◆ Note ◆

Tags (field number **3**) do not apply if proprietary mode is selected. Proprietary mode is only available on Mammoth Gigabit Modules.

For example, suppose that Port 3/1 is assigned to be in Group 2, and to use IEEE 802.1Q. If the port were to be assigned to another group, it would automatically set itself to use IEEE 802.1Q for that group as well.

For more information on proprietary vs. IEEE 802.1Q, see *X802.1Q vs. IEEE 802.1Q* on page 20-4.

Modifying 802.1Q Groups

802.1Q groups for both 10/100 and Gigabit Ethernet ports can be modified using the **mas** command. The procedure is slightly different in each case. The screens for the **mas** command change, depending on whether you have a legacy Ethernet board or a Kodiak ASIC-based Ethernet board.

Modifying 802.1Q Groups for 10/100 Ports

To modify the configuration of an 802.1Q group for 10/100 ports, use the **mas** command as shown:

```
mas <slot>/<port> <instance>
```

where **<slot>** is the slot number of the module on the switch, **<port>** is the port number where the service was created, and **<instance>** is the identifier for the service on this port. For example, to modify 802.1Q service instance 1 on port 5 of slot 2, enter:

```
mas 2/5 1
```

If this is a legacy Ethernet module, the screen appears as shown:

Slot 2 Port 5 Ethernet 802.1Q Service

```
1) Tag           : 3
2) Priority      : 0
```

If this is a Kodiak ASIC-based module, the screen appears as shown:

Slot 2 Port 5 Ethernet 802.1Q Service

```
1. Description (30 chars max) :
2. Tag                       : 0
3. Priority Remap Values     :
   30. 0 - 0
   31. 1 - 1
   32. 2 - 2
   33. 3 - 3
   34. 4 - 4
   35. 5 - 5
   36. 6 - 6
   37. 7 - 7
```

To change a field setting, enter the line number, an equal sign, and the new value. For example, to change the **Priority** setting to **7**, you would enter a **3** (the line number for priority), an equal sign (=), and a **37**, as shown:

```
3=37
```

◆ Important Notes ◆

ESX-K and GSX-K Kodiak ASIC-based modules support 802.1p traffic prioritization. For chassis configurations that include only ESX-K, GSX-K and/or WSX series modules, 802.1p priority bits can be carried inbound on a tagged port (configured with multiple spanning tree 802.1Q) across the backplane. This priority information is used at the egress port to queue the packet, and is sent out in the packet whether the egress port is tagged or not.

The ESX-K and GSX-K modules can also remap incoming priority on an ingress port. If priority remapping has been configured, the new priority will be carried across the backplane. The priority information is used to queue the packet, and is sent out in the packet if the egress port is tagged.

Remember to save the changes to the service by entering **save** at the system prompt when finished.

To find the instance of a port service, use the **vas** command. See *Viewing 802.1Q/X802.1Q Groups in a Port* on page 20-18 for more information.

Modifying 802.1Q Groups for Gigabit Ethernet Ports

To modify the configuration of an 802.1Q group for Gigabit ports, use the **mas** command as shown:

```
mas <slot>/<port> <instance>
```

where **<slot>** is the slot number of the module on the switch, **<port>** is the port number where the service was created, and **<instance>** is the identifier for the service on this port. For example, to modify 802.1Q service instance 1 on port 5 of slot 2, enter:

```
mas 2/5 1
```

If this is a legacy Ethernet module, the screen appears as shown:

```
Slot 2 Port 5 Ethernet 802.1Q Service
```

```
1) Tag           : 3
2) Priority      : 0
```

If this is a Kodiak ASIC-based module, the screen appears as shown:

```
Slot 2 Port 5 Ethernet 802.1Q Service
```

```
1. Description (30 chars max) :
2. Tag                       : 0
3. Priority Remap Values     :
   30. 0 - 0
   31. 1 - 1
   32. 2 - 2
   33. 3 - 3
   34. 4 - 4
   35. 5 - 5
   36. 6 - 6
   37. 7 - 7
```

To change a field setting, enter the line number, an equal sign, and the new value. For example, to change the **Priority** setting to **7**, you would enter a **3** (the line number for priority), an equal sign (=), and a **37**, as shown:

```
3=37
```

◆ Important Notes ◆

ESX-K and GSX-K Kodiak ASIC-based modules support 802.1p traffic prioritization. For chassis configurations that include only ESX-K, GSX-K and/or WSX series modules, 802.1p priority bits can be carried inbound on a tagged port (configured with multiple spanning tree 802.1Q) across the backplane. This priority information is used at the egress port to queue the packet, and is sent out in the packet whether the egress port is tagged or not.

The ESX-K and GSX-K modules can also remap incoming priority on an ingress port. If priority remapping has been configured, the new priority will be carried across the backplane. The priority information is used to queue the packet, and is sent out in the packet if the egress port is tagged.

Remember to save the changes to the service by entering **save** at the system prompt when finished.

To find the instance of a port service, use the **vas** command. See *Viewing 802.1Q/X802.1Q Groups in a Port* on page 20-18 for more information.

◆ **Note** ◆

Tags (field number **1**) do not apply if proprietary tagging is used on this port.

Viewing 802.1Q/X802.1Q Groups in a Port

To view which ports use which 802.1Q groups, enter the **vas** command at the system prompt, as shown:

```
vas <slot>/<port>
```

where **<slot>** is the slot number of the module on the switch and **<port>** is the port number where the service was created. For example, to view an 802.1Q service on port 5 of slot 2, enter:

```
vas 2/5
```

A screen similar to the following is displayed:

Slot/Port/Inst	Vport	Group	Tag	Priority or PriorityRemap	Tagging Mode	Description
2 5 1	33	2	2	4	Mult STree	

As a variation of this command, it is possible to enter **vas** without a slot or port number. This will display all services configured for the switch.

◆ Note ◆

The above screen is for Gigabit ports. The display is slightly different for 10/100 ports. See descriptions below for more details.

The following section describes the fields displayed using the **vas** command.

Slot. The slot number of the switch on which the service is located.

Port. The port number of the slot on which the service is located.

Instance. The service identifier for the 802.1Q service. This is assigned when the service is created.

Vport. The virtual port number that the service uses.

Group. The group identifier for the group attached to this service.

Tag. The tag information entered into tagged frames, as specified when creating the service.

Priority or PriorityRemap. The priority number assigned to packets from this service.

Tagging Mode. This field displays different information depending on whether the switch ports are 10/100 or Gigabit. If the ports are 10/100 or Kodiak-based Gigabit, this field shows either multiple or single spanning tree. If the ports are Mammoth-based Gigabit, this field shows either proprietary 802.1Q (X802.1Q) or IEEE 802.1Q. For 802.1Q support over OmniChannel on Kodiak 10/100 Ethernet boards, this field will display as **Mult S Tree**.

Description. A textual description used to identify the service.

For more information on single vs. multiple spanning tree, see *Single vs. Multiple Spanning Tree* on page 20-4. For more information on proprietary vs. IEEE 802.1Q, see *X802.1Q vs. IEEE 802.1Q* on page 20-4.

Viewing 802.1Q Statistics for 10/100 Ports

The **viqs** command provides a display of statistics for 802.1Q groups assigned to 10/100 ports. Enter the **viqs** command, as shown:

```
viqs <slot>/<port> <groupid>
```

where **<slot>** is the slot number of the module on the switch, **<port>** is the port number where the service was created, and **<groupid>** is the number of the group that the port belongs to. For example, to view an 802.1Q service for group 2 on port 5 of slot 2, enter:

```
viqs 2/5 2
```

A screen similar to the following displays:

Physical Port	Group Id (802.1Q)	Transmit Pkts	Received Pkts	Transmit Octets	Received Octets
2/5	2	29	0	41	0

Physical Port. The slot and port number for this port.

Group Id (802.1Q). The 802.1Q group to which this port was assigned.

Transmit/Received Pkts. The number of packets transmitted and received on this port.

Transmit/Received Octets. The number of bytes transmitted and received on this port.

Deleting 802.1Q/X802.1Q Groups from a Port

802.1Q groups for both 10/100 and Gigabit Ethernet ports can be deleted using the **das** command. The procedure is slightly different in each case.

To delete an 802.1Q group from a 10/100 port using single spanning tree, use the **das** command, as shown:

```
das <slot>/<port> <instance> <groupid>
```

where **<slot>** is the slot number of the module on the switch, **<port>** is the port number where the service was created, **<instance>** is the identifier for the service on this port, and **<groupid>** is the number of the group that the port belongs to. For example, to delete an 802.1Q service for group 2, instance 1 on port 5 of slot 2, enter:

```
das 2/5 1 2
```

To delete 802.1Q groups from a Gigabit port or 10/100 ports using multiple spanning tree, enter the **das** command, as shown:

```
das <slot>/<port> <instance>
```

where **<slot>** is the slot number of the module on the switch, **<port>** is the port number where the service was created, and **<instance>** is the identifier for the service on this port. For example, to delete 802.1Q service instance 1 on port 5 of slot 2, enter:

```
das 2/5 1
```

In either case, a message will appear, confirming the delete operation:

```
802.1Q service deleted for Group ID 3 on 3/9 (slot/Port)
```

◆ Important Notes ◆

You must delete X802.1Q groups in the same order on both ends of the link. For example, if you delete groups 1, 2, 3, 4, and 5 on the local switch, you must delete the same five groups in the same order on the remote switch. *If groups are not deleted in this manner, X802.1Q packets will not be routed correctly.*

To delete 802.1Q support over OmniChannel, you must first delete the 802.1Q service before you delete the OmniChannel.

21 Managing Token Ring Modules

This chapter describes User Interface (UI) commands for Token Ring switching modules. Beginning with Release 3.4, a new generation of Token Ring modules are used in the OmniSwitch and Omni Switch/Router. These modules have many advanced features, including full-duplex mode and auto-sensing capabilities. Token Ring Port Switching* and Ring Switching features are also supported (*Omni Switch/Router TSX-series modules only).

Two Generations of Modules

The two generation of Token Ring switching modules are described in *Bigfoot and Early-Generation Token Ring Modules* on page 21-2.

Source Routing

A basic overview of source routing on Token Ring networks is provided in *Source Routing* on page 21-4.

Virtual Rings

A basic overview of virtual Token Rings is provided in *Source Routing* on page 21-4.

User Interface Commands

Documentation for UI commands used to configure and display parameters on Token Ring modules begins on page 21-13. For documentation on Command Line Interface (CLI) commands to manage Token Ring Modules, see the *Text-Based Configuration CLI Reference Guide*.

◆ Important Notes ◆

In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. See Chapter 8, “The User Interface,” for documentation on changing from CLI mode to UI mode.

Beginning with Release 4.4, FDDI is no longer supported.

Bigfoot and Early-Generation Token Ring Modules

Alcatel's Token Ring switching modules come in two basic families: the original early-generation modules and a new generation of modules containing advanced-technology Mammoth II and Bigfoot ASICs.

The newer modules (Bigfoot modules) support new features, such as auto-sensing and full-duplex mode, which are not available in the early-generation modules. The subsections below provide additional information on the differences between the early-generation and Bigfoot modules.

Early-Generation Modules

Early-generation Token Ring modes consist of the TSM-C-6, TSM-CD-6, and TSM-F-6 for the OmniSwitch (see the table below). All of these modules support connections to Multistation Access Units (MAUs). The TSM-CD-6 and TSM-F-6 modules also support connections to desktop devices. Hardware documentation for these modules can be found in Chapter 7, "OmniSwitch Switching Modules."

Token Ring Module	Chassis Type	Configuration Commands	Port Types	Auto Sensing Supported?	Full Duplex Supported?
TSM-C-6	OmniSwitch	tpcfg	Station	No	No
TSM-CD-6	OmniSwitch	tsc, tpcfg	Station, Lobe	No	No
TSM-F-6	OmniSwitch	tsc, tpcfg	Station, Lobe, Ring Out Only, Ring In/Ring Out (RI/RO)	No	No

Bigfoot Modules

Bigfoot Token Ring modules consist of the TSX-CD-16W and TSX-C-32W for the Omni Switch/Router and the TSM-CD-16W for the OmniSwitch (see the table below). All of these modules support Station connections to desktop devices. The TSM-CD-16W and TSX-CD-16W also support Lobe connections to Multistation Access Units (MAUs).

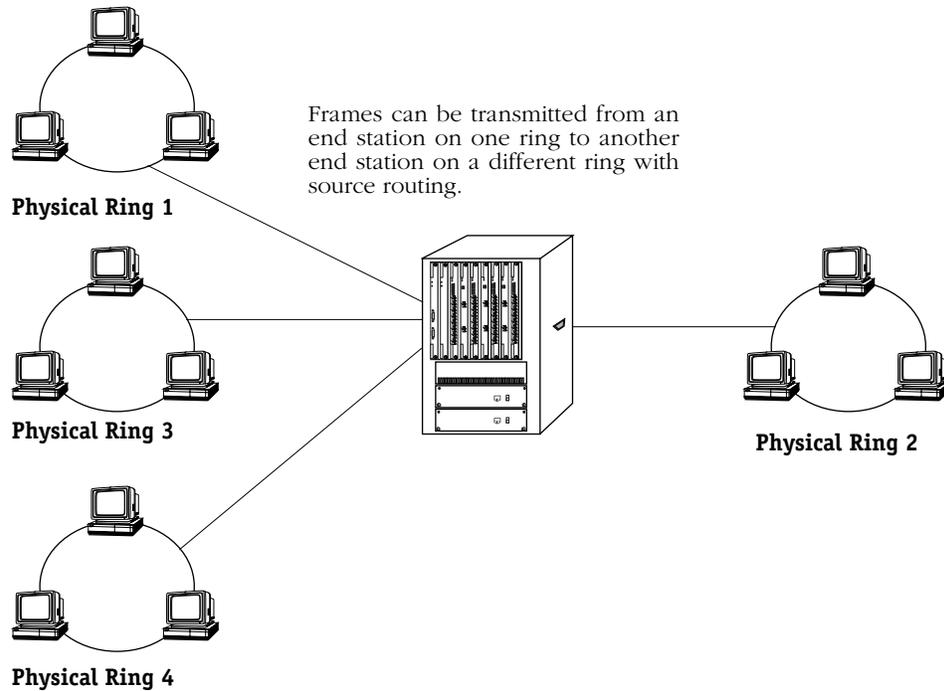
Token Ring Module	Chassis Type	Configuration Commands	Port Types	Auto Sensing Supported?	Full Duplex Supported?
TSM-CD-16W	OmniSwitch	tpcfg, tsmcfg	Station, Lobe	Yes	Yes
TSX-CD-16W	Omni Switch/Router	tpcfg, tsmcfg	Station, Lobe	Yes	Yes
TSX-C-32W	Omni Switch/Router	tpcfg, tsmcfg	Lobe	Yes	Yes

Hardware documentation for the OmniSwitch TSM-CD-16W can be found in Chapter 7, “OmniSwitch Switching Modules.” Hardware documentation on the Omni Switch/Router TSX-CD-16 and TSX-C-32W modules can be found in Chapter 3, “Omni Switch/Router Switching Modules.”

Source Routing

Traditional (Layer 2) source routing is the practice of including routing information in the packet header. This serves to supply the route that the frame should take from the source to the destination. Alcatel switches support traditional source routing on Token Ring and ATM interfaces.

In the figure below, the switch operates as a source route bridge between the four physical Token Rings. Each ring must have a unique ring number.



Source Routing on Token Ring Networks

Hop Counts

Hop counts are split into inbound and outbound hop counts. This is due to the fact that a hop count is validated when an All Routes Explorer (ARE) or Spanning Tree Explorer (STE) is received from a station. When a station starts communicating, it sends out either an STE or an ARE explorer. This packet contains a Route Information Field (RIF) without any source routing information (Null-RIF). The switch examines this explorer. If the inbound hop count is not exceeded, an STE is forwarded to all the ports that are in a forwarding state; and an ARE is forwarded to all ports.

◆ Note ◆

The TSM-CD-6 only supports a maximum of six (6) bridge hops.

The switch adds the destination bridge and ring ID to the RIF. (The first switch on the hop will also add the source ring ID.) Then, the hop count of this RIF is checked against the outbound hop count of the outbound port. If it exceeds the outbound hop count, the explorer frame is discarded. Each succeeding bridge performs the same inboard and outboard check. You should configure the inbound and outbound check to the lowest possible setting. See *Configuring Source Routing/Virtual Rings* on page 21-15 to configure the inbound and outbound hop counts. This will dramatically reduce the number of broadcasts in a network.

◆ Note ◆

Because hop counts are limited, Port Switching can be used in a split ring to ensure that an extra hop is not incurred – for example, when adding an additional switch to an established network. To learn about the Port Switching feature, see *Configuring Token Ring Port Switching* on page 21-33.

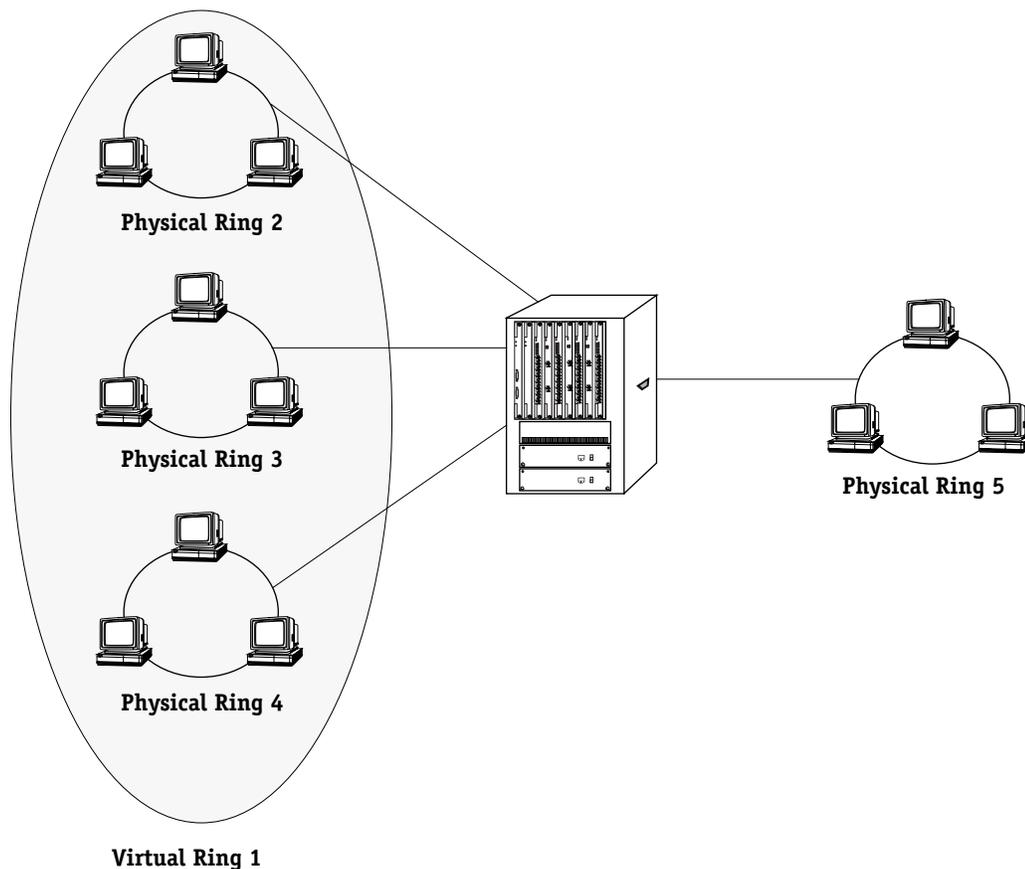
Virtual Rings

With AutoTracker, you can create virtual rings that combine multiple physical Token Ring LANs into one logical Token Ring LAN. Virtual rings allow you to maintain the same number of rings and bridges without increasing the amount of management required. They also provide high speed switching between Token Ring LANs with the same ring number while at the same time providing source route bridging of traffic between Token Rings with different ring numbers. With virtual rings, additional ring numbers are not used, devices do not have to be configured, and additional hops are conserved.

The Route Information Field (RIF) limits the number of hops you can have. This limit is costly in a switched network if a bridge forwards frames strictly according to the RIF. With AutoTracker, a virtual ring network forwards source route traffic without using RIF information, and therefore without using any hops.

Local Virtual Rings

With virtual rings, you can micro-segment an existing Token Ring network, which increases bandwidth by transparently connecting multiple physical rings into one logical Token Ring network. Traffic is switched between rings with the same ring number and source route bridged to rings with a different ring number. In the figure on the following page, all end stations attached to the three physical Token Rings identified as virtual ring Number 1 will appear to the end stations as being on the same ring. The three physical rings will be treated as one logical ring. The switch will also operate as a standard source route bridge to allow end stations on virtual Ring 1 to communicate with end stations on Ring 5.



Local Virtual Rings

Spanning Tree Leaf Rings

Any physical Token Ring that is part of a virtual ring must be a leaf of the spanning tree. The only exception is a source route bridge that is attached to a Token Ring, not participating in a virtual ring or a Token Ring that *is* participating but does not cause a loop.

Any source route bridges attached to a physical Token Ring that is part of a virtual ring, cannot create a loop back to another physical Token Ring that is part of the same virtual ring.

Setting Up Virtual Rings

First, create a group and assign multiple physical ports to it. Assign the same ring number to each physical port that you want to be in the Virtual Ring. Assign the other ports a unique ring number if standard source route bridging is required between rings. You may have one or more source route bridges as part of a virtual ring, but you must ensure that no loop is introduced into the network; any source route bridge added to the ring must not have a path through it that leads back to the ring.

Source Route Traffic Across a Backbone

If you assign a ring number to the backbone, then the backbone can be used as a single hop in the source route network. If the number of hops used is a concern, this may not be the best method for you.

Alcatel switches support standard Source Routing for Token Ring networks. In addition, a network of switches can support source routing over ATM backbones.

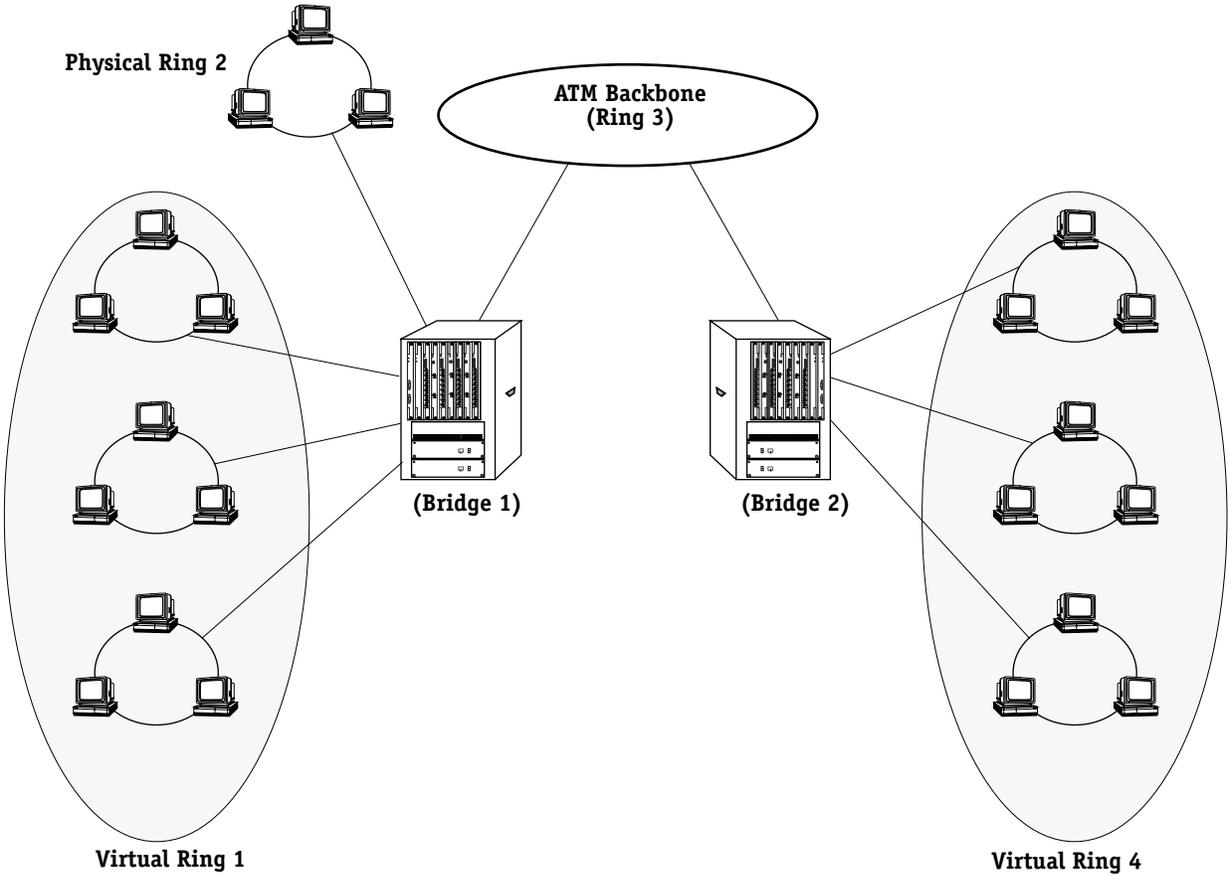
With standard source route bridging, the bridge forwards frames according to the routing information field contained within each frame. An explicit route designated by the RIF is as follows:

RIF:LAN Identifier, Bridge Number:LANIdentifier,Bridge Number:..LAN Identifier

where the LAN Identifier (Ring number) is locally administered and unique for the network.

Because the RIF contains necessary information, source route bridges do not need to examine either the source or destination MAC addresses except to monitor for their own address in the destination field for management frames. Instead, they monitor all traffic on their ports and search for the ring number, and Bridge number assigned for that port. Because the route is explicit, source routing has the advantage that it allows for routing across blocked spanning tree ports without concern for the frame replication that can occur through looping. Two switches connected by a backbone with an assigned ring number cannot have virtual rings extended across that backbone simultaneously.

In the figure on the following page, two switches are used to interconnect two logical rings. A route discovered from Ring 1 to Ring 4 would include Ring 1, Bridge 1, Ring 3, Bridge 2, and Ring 4 in the RIF.

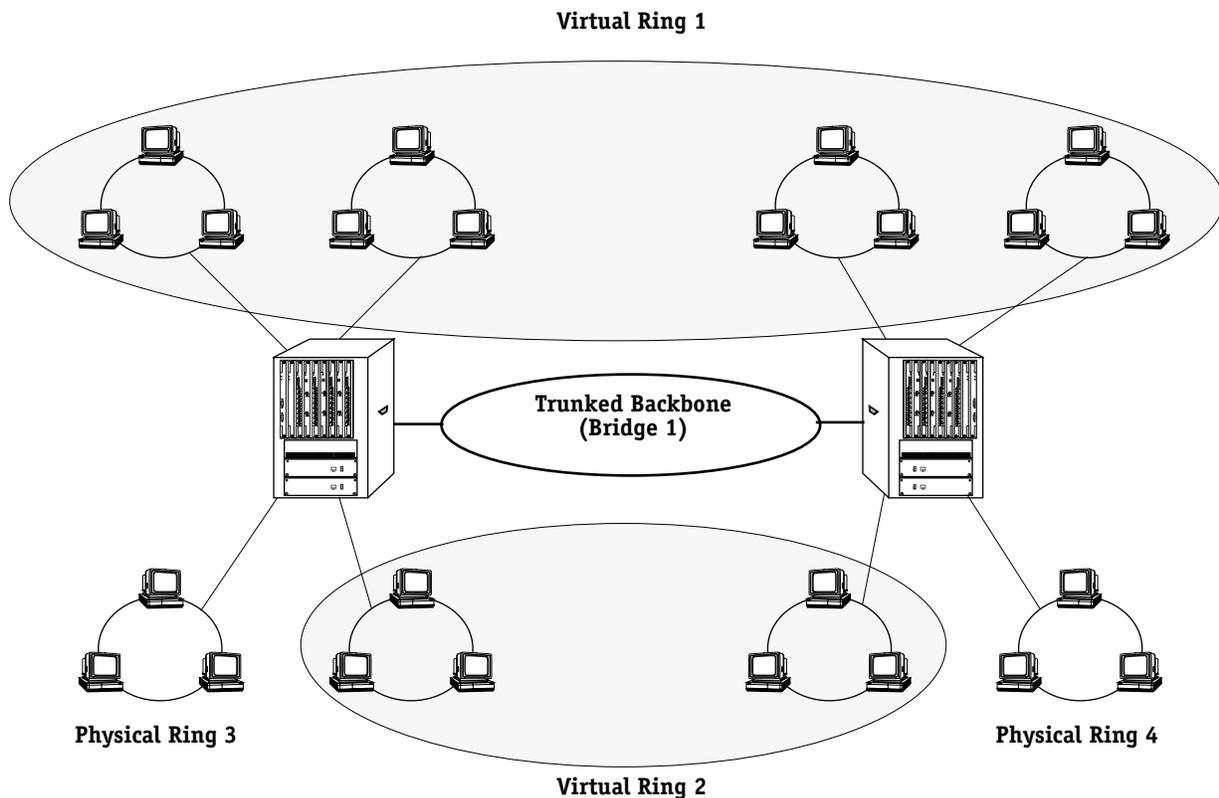


Source Routing Across a Backbone

Virtual Rings Using Trunks

Virtual rings can be extended across an ATM backbone to a remote switch or switches which are part of the same virtual LAN by assigning all switches connected to the backbone the same bridge number, and trunking that virtual ring. Any connected switches with different numbers will simply not be part of that virtual ring. Thus, two or more switches will act as a single source route bridge hop. A frame received on a Token Ring on one switch will travel across the backbone to remote Token Ring networks with the same ring number, and will be viewed by the end stations as if they were on that same physical Token Ring. If you do not assign a ring number to the backbone, it will be considered by the rest of the virtual ring to be part of it. Thus multiple virtual rings could share the same backbone transparently.

Traffic between the stations on the same logical ring would have a null RIF field and the stations would appear to each other as if on the same ring. Traffic is transparently switched within the extended switch network and between the segments within a virtual ring.



Virtual Rings Using Trunks

Token Ring Copy Bit Stamping

Token Ring frames contain a bit called Frame Copied Bit that is normally set when a frame is bridged from one ring to another. By default, the switch sets this bit for all Token Ring frames that it processes, even frames with source and destination addresses on the same ring. In some cases, when a Token Ring frame reaches its destination workstation, the adapter on that workstation generates 802.5-defined soft errors because it does not support local frames that have already had their Frame Copy Bit set.

You can configure the switch to stop setting the Frame Copy bit on Token Ring frames on a per-port basis. If you turn off Frame Copy bit stamping, then no frames received on the specified Token Ring port will be stamped.

If you are receiving soft errors on a Token Ring workstation that is attached to an switch, then you may want to consider turning off Frame Copy Bit stamping.

When Copy Bit Stamping is enabled (the default), the switch knows it has looked at a frame by looking at the Copy Bit. When you turn off Copy Bit Stamping, the switch builds a pseudo-CAM of frame addresses it has already seen. Otherwise, it will not know if it has seen a frame before. The building of this pseudo-CAM may cause some performance degradation.

To turn off Copy Bit stamping, use the **tpcfg** command, which is described in *Configuring Port Parameters for Early-Generation Token Ring Modules* on page 21-24. You will need to reset the switch for the new Copy Bit stamping status to take effect.

Source Routing to Transparent Bridging (SRTB)

Source-routed frames generated by Token Ring workstations contain a 2-byte Routing Information Field (RIF). Normally, when an Ethernet port on the switch sees a source-route frame with a RIF field, it discards that frame. The frame never reaches the Ethernet network.

In Release 4.1 and later, Source Routing to Transparent Bridging (SRTB) provides connectivity between transparently-bridged Ethernet and a source-routed Token Ring. The RIF is stripped from frames that are switched from Token Ring networks to Ethernet networks. Conversely, the RIF is added to frames that are switched from Ethernet networks to Token Ring networks. See Chapter 22, “Configuring Bridging Parameters,” for documentation on the SRTB feature.

Token Ring UI Commands

User Interface (UI) commands are available to configure and display Token Ring parameters. These commands are grouped into the Token Ring (**tok**) submenu, which is described below. In addition, UI commands are available to configure source routing and display source routing parameters on Token Ring networks. These commands are group into the bridging (**br**) submenu, which is described in *Bridging Submenu* on page 21-14.

Token Ring Submenu

The **tok** submenu contains commands to configure and display parameters for Token Ring switching modules. To enter the **tok** submenu, enter

tok

at the system prompt. Enter a question mark (?) to display the list of commands, as shown below.

Command	Token Ring Menu
tsc	View/Configure the Token Ring Interface Type
tsmvc	View Token Ring Base MAC addressed settings
tsmcfg	Configure the Token Ring Base MAC addresses
tpvc	View the Token Ring Port Configuration Table
tpcfg	Configure Token Ring Port Parameters
tperrs	View Token Ring Port Error Statistics
trsw	Token Ring Switching
tprs	View Token Ring Port Ring Status

Descriptions of the **tok** submenu commands begin on page 21-21.

Bridging Submenu

Commands for configuring and displaying source routing parameters are contained in the bridging (**br**) submenu. You create and modify source routing with the **src** command and you display source routing parameters with the **srs** command.

To enter the **br** submenu, enter

br

at the system prompt. Enter a question mark (?) to display the list of commands, as shown below.

Command	Bridge Management Menu
fls	Display Flood Limit of selected Group
flc	Configure Flood Limit on selected Group
sts	Display Spanning Tree parameters on selected Group
fstps	Display Fast Spanning Tree Port parameters on selected VLAN
actfstps	Activate Fast Spanning Tree Port parameters for a selected VLAN
stc	Configure Spanning Tree parameters on selected Group
stps	Display Spanning Tree Port parameters on selected VLAN
stpc	Configure Spanning Tree Port parameters on selected VLAN
srs	Display Source Routing parameters on selected Group
src	Configure Source Routing parameters on selected Group
srsf	Enable or disable Source Routing SAP Filter Support
srtrbcfg	View and Configure Source Route to Transparent Bridging
srtrbrif	View learned RIF from Source Route to Transparent Bridging table
srtrbclrrif	View and Clear learned RIF from Source Route to Transparent Bridging table
fwf	Display Bridge Forward table on selected VLAN
fs	Display Bridge Static Address
fc	Configure Bridge Static Address
bps	Display Bridge Port Statistics on selected VLAN
macinfo	Locate learned Bridge MAC address in this chassis
macstat	Show statistics of Bridge MAC address
macclrstat	Clear statistics of Bridge MAC address
selgp	A Group can be selected for the bridge operations or to generate MIB reports
rts	Display remote Trunking Stations discovered
dbmap	View the Domain Bridge Mapping table
+ / -	Select next / previous VLAN

The **src** command is described in *Configuring Source Routing/Virtual Rings* on page 21-15. The **srs** command is described in *Displaying Source Routing Parameters* on page 21-18. See Chapter 22, "Configuring Bridging Parameters," for documentation on all other **br** submenu commands.

Configuring Source Routing/Virtual Rings

The **src** command allows you to set the parameters for source routing. In addition, it also displays current source routing parameters for your switch. The syntax for the **src** command is as follows:

```
src <group number>
```

If you do not enter a group number, then Group No. 1 (the default group) will be entered. For example, to configure the source routing parameters on Group No. 1, enter

```
src
```

at the system prompt. A screen similar to the following is displayed.

Source Routing Parameters for Group 1 (Default GROUP (#1))

	Slot Intf	Type/ Inst/Srvc	Ring Number	Bridge Number	Largest frame	HopCnt In Out	Port Type	Block ARE
1.	2/1	Brg/ 1/ na	1 (0x001)	10 (0xA)	590	6 6	SRT	n
2.	3/1	Brg/ 1/ na (V)	2 (0x002)	10 (0xA)	4472	7 7	SRT	n
3.	3/2	Brg/ 1/ na	4 (0x004)	10 (0xA)	4472	7 7	SRT	n
4.	3/3	Brg/ 1/ na	5 (0x005)	10 (0xA)	4472	6 6	SRT	n
5.	3/4	Brg/ 1/ na	3 (0x003)	10 (0xA)	4472	7 7	SRT	n
6.	3/5	Brg/ 1/ na (V)	2 (0x002)	10 (0xA)	4472	7 7	SRT	n
7.	3/6	Brg/ 1/ na (V)	3 (0x003)	10 (0xA)	4472	7 7	SRT	n

Enter index of the entry to configure (e.g. 1) <RETURN> to exit :

The fields displayed by the **src** command are described in the subsection below. To set parameters, enter the index entry (the left-most number) in the row with the port you want to configure. See *Source Routing/Virtual Ring Configuration Steps* on page 21-16 to configure source routing and virtual Token Rings.

◆ Note ◆

The **src** command operates differently if you have turned on SAP filtering on with the **srsf** command. For documentation on using the **src** command with SAP filtering turned on, see Chapter 22, “Configuring Bridging Parameters.”

Source Routing/Virtual Ring Parameters

Slot Intf. The slot and interface (port) for this Token Ring.

Type. The type of service of this Token Ring. The type of service can be one of the following.

Brg. Indicates that bridging has been configured on this ring.

Lne. Indicates that an 802.5 LANE client service is configured on this ring.

Inst. This field is used to identify the instance of the service if there is more than one service for the **Slot/Intf** field.

Srvc. This field indicates the service number. If a port has more than one service configured on it, then each service will be identified by a different service number.

Ring Number. The ring number assigned to the Token Ring for participation in source routing. If a **(V)** appears in front of this field, then a virtual ring is configured.

Bridge Number. A unique number to identify the source routing bridge number used to participate in source routing. This number will be the same for each port on the same group.

Largest frame. The maximum size of the INFO field that this virtual port can send and receive.

Hop Cnt In. The maximum inbound hop count for Spanning Tree Explorer (STE) and All Routes Explorer (ARE) frames (the default is **7**). This value is checked on all inbound STE or ARE frames. If the hop count is exceeded, the frame will be dropped. See *Hop Counts* on page 21-4 for more information on hop counts.

Hop Cnt Out. The maximum outbound hop count for Spanning Tree Explorer (STE) and All Routes Explorer (ARE) frames (the default is **7**). This value is checked on outbound STE or ARE frames. If the hop count is exceeded, the frame will be dropped. See *Hop Counts* on page 21-4 for more information on hop counts.

Port Type. This can be either source route (**SR**) or source route transparent (**SRT**) bridge port.

Block ARE. Indicates whether the All Routes Explorer (ARE) will be treated as Spanning Tree Explorer (STE). Normally ARE does not acknowledge blocked ports the way STE does. This behavior can cause unnecessary congestion.

Source Routing/Virtual Ring Configuration Steps

Perform the steps below to configure source routing parameters.

1. At the system prompt, enter

```
src
```

A screen similar to the following displays. (See *Source Routing/Virtual Ring Parameters* on page 21-15 for descriptions of these fields.)

Source Routing Parameters for Group 1 (Default GROUP (#1))

	Slot Intf	Type/ Inst/Srvc	Ring Number	Bridge Number	Largest frame	HopCnt In Out	Port Type	Block ARE
1.	2/1	Brg/ 1/ na	1 (0x001)	10 (0xA)	590	6 6	SRT	n
2.	3/1	Brg/ 1/ na (V)	2 (0x002)	10 (0xA)	4472	7 7	SRT	n
3.	3/2	Brg/ 1/ na	4 (0x004)	10 (0xA)	4472	7 7	SRT	n
4.	3/3	Brg/ 1/ na	5 (0x005)	10 (0xA)	4472	6 6	SRT	n
5.	3/4	Brg/ 1/ na	3 (0x003)	10 (0xA)	4472	7 7	SRT	n
6.	3/5	Brg/ 1/ na (V)	2 (0x002)	10 (0xA)	4472	7 7	SRT	n
7.	3/6	Brg/ 1/ na (V)	3 (0x003)	10 (0xA)	4472	7 7	SRT	n

Enter index of the entry to configure (e.g. 1) <RETURN> to exit :

2. Enter the index entry (the left-most number) of the ring you want to configure. A screen similar to the following displays.

```
Ring Number (1 - 4095, 0 to disable) (0x004):
```

3. Enter a ring number from **1** to **4095** or enter **0** to remove the port from all rings. The current ring (in hexadecimal) is displayed in parentheses. The following screen displays.

```
Virtual Ring (y/n) (n):
```

4. Enter **y** to configure the port for a virtual Token Ring or **n** to configure the port for a physical ring. (The default is **n**.) A screen similar to the following displays.

Bridge Number (1 - 15, 0 to disable) (0xA):

5. Enter a bridge number from **1** to **15** or enter **0** to remove the port from all bridges. The current bridge (in hexadecimal) is displayed in parentheses. A screen similar to the following displays.

Max Outbound Hop Count (7):

6. Enter the maximum number of outbound hop counts, which can be from 0 to 14, for this port. (The current number is displayed in parentheses.) A screen similar to the following displays.

Max Inbound Hop Count (7):

7. Enter the maximum number of inbound hop counts, which can be from 0 to 14, for this port. (The current number is displayed in parentheses.) A screen similar to the following displays.

Largest Frame size (4472):

8. Enter the largest frame size (in bytes) allowed on this port. On early-generation modules, the largest possible value is 4472. On Bigfoot modules, the largest possible value is 17800. The following screen displays.

Turn Transparent Bridging ON (y/n) (y):

9. Enter **n** for pure source routing or **y** for source route transparent bridging (SRTB). (The default is **y**.) The following screen displays.

Block ARE on non-forward state (y/n) (n):

10. If you answer **Yes** to this option, blocked ports will be treated in a non-forwarding state by ARE. (The default is **n**.) The following screen displays.

Save the new configuration? (y/n) (n):

11. Enter **y** to save the new settings or **n** to discard them. (The default is **n**.) The following screen displays.

Enter index of the entry to configure (e.g. 1) <RETURN> to exit :

12. Enter the index entry (the left-most number) to configure another ring or press **<Return>** to exit.

Displaying Source Routing Parameters

The **srs** command displays the current parameters for source routing. To use this command, enter

srs

at the system prompt. A screen similar to the following will be displayed.

Source Routing Parameters for Group 1 (Default GROUP (#1))

	Slot Intf	Type/ Inst/Srvc	Ring Number	Bridge Number	Largest frame	HopCnt In Out	Port Type	Block ARE
1.	2/1	Brg/ 1/ na	1 (0x001)	10 (0xA)	590	6 6	SRT	n
2.	3/1	Brg/ 1/ na (V)	2 (0x002)	10 (0xA)	4472	7 7	SRT	n
3.	3/2	Brg/ 1/ na	4 (0x004)	10 (0xA)	4472	7 7	SRT	n
4.	3/3	Brg/ 1/ na	5 (0x005)	10 (0xA)	4472	6 6	SRT	n
5.	3/4	Brg/ 1/ na	3 (0x003)	10 (0xA)	4472	7 7	SRT	n
6.	3/5	Brg/ 1/ na (V)	2 (0x002)	10 (0xA)	4472	7 7	SRT	n
7.	3/6	Brg/ 1/ na (V)	3 (0x003)	10 (0xA)	4472	7 7	SRT	n

Enter index of the entry to see details (e.g. 1) <RETURN> to exit :

To display detailed information for a particular port, enter the index entry (the left-most number) of the row with the port you want to display. If you entered an index number, a screen similar to the following will be displayed.

Selected entry is attached to Group 1 (Default GROUP (#1))

Bridge Num:	0xa	Ring Num:	0x4
Hop Count In/Out:	7 / 7	Max Frame:	4472
LF Mode:	3 bits	Span Mode:	Auto-Span
SRFs In/Out:	4532/ 3048	Invalid RI field:	0
AREs In/Out:	21078/ 3262	Dup Segments:	0
STEs In/Out:	3242/ 1056		
Dup LAN IDs:	0	LAN ID Mismatches:	0
Hop Count Exceeded - Inbound/Outbound:			0/ 0

Enter index of the entry to see details (e.g. 1) <RETURN> to exit :

◆ Note ◆

The **srs** command operates differently if you have turned on SAP filtering on with the **srsf** command. For documentation on using the **srs** command with SAP filtering turned on, see Chapter 22, “Configuring Bridging Parameters.”

Enter an index number to display detailed parameters for another port or press <Return> to exit. The fields displayed by the **srs** command are described below.

Slot Intf. The slot and interface (port) for this Token Ring.

Type. The type of service of this Token Ring. The type of service can be one of the following.

Brg. Indicates that bridging has been configured on this ring.

Lne. Indicates that an 802.5 LANE client service is configured on this ring.

Inst. This field is used to identify the instance of the service if there is more than one service for the **Slot/Intf** field.

Srvc. This field indicates the service number. If a port has more than one service configured on it, then each service will be identified by a different service number.

Ring Number. The ring number assigned to the Token Ring for participation in source routing. If a **(V)** appears in front of this field, then a virtual ring is configured.

Bridge Number. A unique number to identify the source routing bridge number used to participate in source routing. This number will be the same for each port on the same group.

Largest frame. The maximum size of the INFO field that this virtual port can send and receive.

Hop Cnt In. The maximum inbound hop count for Spanning Tree Explorer (STE) and All Routes Explorer (ARE) frames (the default is **7**). This value is checked on all inbound STE or ARE frames. If the hop count is exceeded, the frame will be dropped. See *Hop Counts* on page 21-4 for more information on hop counts.

Hop Cnt Out. The maximum outbound hop count for Spanning Tree Explorer (STE) and All Routes Explorer (ARE) frames (the default is **7**). This value is checked on outbound STE or ARE frames. If the hop count is exceeded, the frame will be dropped. See *Hop Counts* on page 21-4 for more information on hop counts.

Port Type. This can be either source route (**SR**) or source route transparent (**SRT**) bridge port.

Block ARE. Indicates whether the All Routes Explorer (ARE) will be treated as Spanning Tree Explorer (STE). Normally ARE does not acknowledge blocked ports the way STE does. This behavior can cause unnecessary congestion.

◆ Note ◆

The fields listed below are only displayed if you selected to display detailed information for a single port.

Bridge Num. See the description for the **Bridge Number** field above.

Ring Num. See the description for the **Ring Number** field on the previous page.

Hop Count In/Out. See the description for the **Hop Cnt In** and **Hop Cnt Out** fields above

Ring Num. See the description for the **Ring Number** field on the previous page.

LF Mode. The length of the frame size negotiation field. Currently set to 3 bits.

Max Frame. See the description for the **Largest frame** field above.

Span Mode. Determines how this virtual port will handle a Spanning Tree Explorer (STE) frames. Values include the following:

Auto-span. Can only be returned by a bridge that both implements the Spanning Tree Protocol and has use of the protocol enabled on this virtual port. If the virtual port is in the forwarding state, the frame will be accepted or propagated. Otherwise it will be silently discarded. [Any others?]

SRFs In/Out. The number of Specifically Routed Frames that have been received/transmitted.

AREs In/Out. The number of All Route Explorer (ARE) frames that have been received/transmitted.

STEs In/Out. The number of Spanning Tree Explorer (STE) frames that have been received/transmitted.

Displaying Source Routing Parameters

Dup LAN IDs. The number of frames discarded due to Duplicate LAN IDs.

Invalid RI field. The number of explorer frames that have been discarded because the routing information field contained an invalid value.

Dup Segments. The number of frames that have been discarded by this virtual port because routing descriptor field contained a duplicate segment identifier.

LAN ID Mismatches. The number of ARE and STE frames that were discarded because of a LAN ID mismatch.

Hop Count Exceeded - Inbound/Outbound. The total inbound and outbound hop count for source router STE and ARE frames. See *Configuring Source Routing/Virtual Rings* on page 21-15 to configure the inbound and outbound hop counts.

Configuring the Interface Type on Early-Generation Modules

You can use the **tsc** command to modify the interface type on early-generation modules with configurable ports (i.e., the TSM-F-6 and the TSM-CD-6). You cannot use the **tsc** command to configure the TSM-C-6 or Bigfoot Token Ring modules.

◆ Note ◆

You can use the **tsc** command to display the interface type on all Token Ring modules. See *Displaying the Token Ring Interface Type* on page 21-41 for documentation on using the **tsc** command to display the interface type.

See the subsection below to configure the interface type on a TSM-F-6 and see *Configuring the Interface Type on a TSM-CD-6* on page 21-23 to configure a TSM-CD-6.

Configuring the Interface Type on a TSM-F-6

Perform the steps below to configure the interface type for a TSM-F-6.

1. Enter **tsc** at the system prompt. A screen similar to the following will be displayed.

```
Token Ring slot interface table
Slot  Interface Type
-----
3     C-RJ45
4     C-6PORT-XYLAN
Enter Slot Number [<ret> to exit] :
```

2. Enter the slot number of the TSM-F-6 module. A screen similar to the following is displayed.

```
Available Interface Types
(1) F-STATION-802.5j
(2) F-LOBE-802.5j
(3) F-RIRO-BYTEX
(4) F-RO-6PORT-BYTEX
(5) F-RIRO-SYNOPTICS
(6) F-RO-6PORT-SYNOPTICS
(7) F-RIRO-XYLAN
(8) F-6PORT-XYLAN/IBM
(9) F-OPTION-3PORT
(10) F-OPTION-6PORT
```

```
Enter interface type [<ret> to exit] :
```

3. Enter the number of the interface type you want to configure. Each of the supported configurations, 1-8, require a separate configuration file (options 9 and 10 are for future use). The default interface type is **6PORT-XYLAN/IBM**. These files are stored in the MPM in a compressed form. If a file cannot be found you will receive an error message.

◆ Note ◆

Initially all fiber configuration files are archived into the one file **tsm.pga**.

Synoptics/Bytex Hubs. If you are interfacing with a Synoptics (Bay Networks) hub, select option 5 or 6. If interfacing with a Bytex hub, select option 3 or 4.

IBM 8230 and 8272. If interfacing with an IBM 8230 or IBM 8272, select the **6PORT-XYLAN/IBM** option. Connect either the RI or the RO port on the IBM hub to one of the six ports on the TSM-F-6 — do not connect both IBM ports (RI and RO) to the same OmniSwitch. For example, you could connect the RI port on an IBM hub to a TSM-F-6 port on one OmniSwitch and connect the RO port on the same IBM hub to a TSM-F-6 port in another OmniSwitch. Both TSM-F-6 ports in the two OmniSwitches and all ports in the IBM hub form one ring.

ODS 836J. If interfacing with an ODS 836J Token Ring fiber optic transceiver, select the **6PORT-XYLAN/IBM** option. When connecting the ODS 836J to a twisted-pair MAU, set the ODS 836J switch to position 2 and connect its fiber port to the TSM-F-6. When connecting the ODS 836J to a station (twisted-wire adapter card), set the ODS 836J switch to position 0 and connect its fiber port to the TSM-F-6.

Ring In/Ring Out (RI/RO) Configurations. The RI/RO interface options provide fiber redundancy by using two fiber ports as a pair. See Chapter 7, “OmniSwitch Switching Modules,” for an explanation of the RI/RO configuration.

Token ring fiber optic RI/RO is not an IEEE standard. Different vendors provide their proprietary RI/RO interface. Options are provided for Synoptics, Bytex, and Xylan RI/RO interfaces.

After you select an interface type, the following will be displayed.

**(The new value is saved in configuration and will be activated after reboot.
Reload board with new interface now? [y/n] :**

4. Enter **y** to save your changes or press **<Return>** to cancel. If you entered **y**, the following will be displayed.

**Loading new interface...
System must now be REBOOTED.**

5. You must reboot the switch for any changes to take effect.

Configuring the Interface Type on a TSM-CD-6

Perform the steps below to configure the interface type for a TSM-CD-6.

1. Enter **tsc** at the system prompt. A screen similar to the following will be displayed.

```
Token Ring slot interface table
Slot  Interface Type
-----
3     C-RJ45
4     C-6PORT-XYLAN
Enter Slot Number [<ret> to exit] :
```

2. Enter the slot number of the TSM-CD-6 module. A screen similar to the following is displayed.

```
Port      Mode
-----
1         Lobe
2         Lobe
3         Lobe
4         Lobe
5         Lobe
6         Lobe
```

**Note: this is the configured mode. 'tpvc' displays the active mode.
Ports may be in either Lobe or Station mode.
Select port to change:**

Each port is set to either Lobe or Station mode. You toggle a port between these modes by entering the port number at this prompt. After you enter the port number, a screen similar to the following will be displayed.

**Port 6 configuration has been saved as Station mode.
Activate the configuration now? [y/n] :**

3. Enter **y** to change the interface type or press **<Return>** to cancel. Any changes to the interface type will take place immediately; you do not need to reboot the switch.

If you entered **y**, a screen similar to the following will be displayed.

Port 6 activated in Station mode.

A screen similar to the following will be displayed showing the current interface type configurations.

```
Port      Mode
-----
1         Lobe
2         Lobe
3         Lobe
4         Lobe
5         Lobe
6         Station
```

**Note: this is the configured mode. 'tpvc' displays the active mode.
Ports may be in either Lobe or Station mode.
Select port to change:**

4. Enter a slot number to configure another port or press **<Return>** to exit.

Configuring Port Parameters for Early-Generation Token Ring Modules

You can use the **tpcfg** command to set port parameters for early-generation Token Ring modules.

1. Enter **tpcfg** at the system prompt. The following screen will be displayed.

Enter Slot/Interface :

2. Enter the slot and interface that you want to configure. A screen similar to the following will be displayed.

New Ring Speed (16 or 4 mps) (current speed is 16) :

3. Enter **4** to set the ring speed to 4 Mbps or **16** to set it to 16 Mbps. A screen similar to the following will be displayed.

Active Monitor Participation (currently No) :

4. The active monitor performs certain functions (e.g., ensuring that frames do not circulate endlessly on the ring, ensuring that there is a valid token on the ring) to ensure that the ring functions properly. Enter **n** (the default) to turn off active monitor participation or **y** to turn it on. A screen similar to the following will be displayed.

Frame-Copied Bit Always Set (currently Yes):

5. Enter **yes** to disable Copy Bit stamping or **no** to disable it. (See *Token Ring Copy Bit Stamping* on page 21-11 for more information on Copy Bit stamping.) A screen similar to the following will be displayed.

**The new value is saved into configuration and will be activated on next Reset command after reboot.
New Frame-Copied Mode is saved in configuration.**

Immediate Command (Open, Reset, Close, <ret>No action) :

6. The **Ring Speed**, **Active Monitor Participation**, and **Frame-Copied Bit** settings are saved in memory until you close or reset the ring, or reboot the switch. If you want the settings to take effect immediately, enter **reset**. The system will close the ring and reopen it with the new settings.

Enter **open** to open a closed ring, enter **close** to close an open ring, or press **<Return>** to exit to take no action at this time.

Configuring Auto-Sensing Ports for Bigfoot Modules

You can use the **tpcfg** command to configure Token Ring ports on Bigfoot modules (which are described in *Bigfoot Modules* on page 21-3) that will simultaneously auto-sense ring speed (4 and 16 Mbps), duplex mode (full- and half-duplex), and port mode (Station and Lobe ports).

◆ Note ◆

The Omni Switch/Router TSX-C-32W only supports Lobe ports.

To use the **tpcfg** command to configure auto-sensing ports, follow the steps below.

1. At the system prompt, enter

```
tpcfg
```

The following prompt will be displayed.

```
Enter Slot/Interface [<ret> to exit] :
```

2. Enter the slot and port number. If you want to set Port 1 on Slot 5 to auto-configuration mode, for example, enter

```
5/1
```

at the prompt. A prompt similar to the following will be displayed.

```
Current Configuration:
```

```
OpenStat=Closed, CfgType=Auto , Speed= ? , Duplex= ? , Mode= ?
ARI/FCI= Nonlocal, ActiveMon=No
```

```
Change Port's Configuration? (Y/N) [Y] :
```

3. Enter **y** (the default) to configure this port or **n** to leave this port's configuration "as is" and proceed to Step 7. A prompt similar to the following will be displayed.

```
New Config Type ((A)uto or (F)ixed).....[currently Auto ] :
```

4. Enter **a** (the default) to set the port to auto configuration mode. (If you want to set any of these parameters individually, please see *Manually Configuring Token Ring Ports on Bigfoot Modules* on page 21-27.) A prompt similar to the following will be displayed.

```
New ARI/FCI Bit ((N)on-local, (R)epeat or (A)lways)..[currently Nonlocal] :
```

5. This field sets the control mode for handling Address Recognized Indicator (ARI)/Frame Copied Indicator (FCI) bits. There are three possible ways for handling the ARI/FCI bits:
 - **Nonlocal.** Set the ARI/FCI bits on remote LLC frames repeated by the port and for local LLC frames repeat the ARI/FCI bits just as they are received.
 - **Repeat.** The ARI/FCI bits on all LLC frames are repeated just as they are received.
 - **Always.** Set the ARI/FCI bits on all LLC frames repeated by the port.

Enter **n** to set the control method to non-local, **r** for repeat, or **a** for always. A prompt similar to the following will be displayed.

```
Active Monitor Participation? (Y/N).....[currently No ] :
```

6. The active monitor performs certain functions (e.g., ensuring that frames do not circulate endlessly on the ring, ensuring that there is a valid token on the ring) to ensure that the ring functions properly.

Enter **n** to turn off active monitor participation or **y** to turn it on.

7. All of the changes you have made will take effect when you reboot the switch or reset the module. Therefore, the **tpcfg** command gives you the option to reset the port now and displays the following prompt.

Would you like to reset the port now? (Y/N) [N] :

8. Enter **y** to reset the Token Ring port or enter **n** (the default) to skip the reset. If you answered **n**, then go to Step 9. If you answered **y**, then a confirmation prompt similar to the following will be displayed.

**Reset the Token Ring port 4/5 may cause disruption to the ring.
Are you sure you want to do this? (Y/N) [N] :**

Enter **n** (the default) to skip the reset or **y** to implement it immediately.

9. The following prompt will be displayed.

Enter Slot/Interface [<ret> to exit] :

10. Enter the slot and port number to configure another port or press the **<Return>** key to exit.

◆ Note ◆

You can confirm your changes with the **tpvc** command, which is described in *Displaying Token Ring Port Status* on page 21-44.

Manually Configuring Token Ring Ports on Bigfoot Modules

You can use the **tpcfg** command to manually configure Token Ring ports on Bigfoot modules (which are described in *Bigfoot Modules* on page 21-3) on any or all of the following parameters:

- Ring speed (4 Mbps or 16 Mbps)
- Duplex mode (full duplex, half duplex, or half/full auto-sensing)
- Port mode (Lobe, Station, and auto-sensing Lobe/Station) on the OmniSwitch TSM-CD-16W and the Omni Switch/Router TSX-CD-16W (the Omni Switch/Router TSX-C-32W only supports Lobe port mode).

To use the **tpcfg** command to manually configure Token Ring ports, follow the steps below.

1. At the system prompt, enter

```
tpcfg
```

The following prompt will be displayed.

```
Enter Slot/Interface [<ret> to exit] :
```

2. Enter the slot and port number. If you want to set Port 1 on Slot 5 to fixed-configuration mode, for example, enter

```
5/1
```

at the prompt. A prompt similar to the following will be displayed.

```
Current Configuration:
```

```
OpenStat=Closed, CfgType=Auto , Speed= ? , Duplex= ? , Mode= ?  
ARI/FCI= Nonlocal, ActiveMon=No
```

```
Change Port's Configuration? (Y/N) [Y] :
```

3. Enter **y** (the default) to configure this port or **n** to leave this port's configuration "as is" and proceed to Step 11. A prompt similar to the following will be displayed.

```
New Config Type ((A)uto or (F)ixed).....[currently Auto ] :
```

4. Enter **f** to set the port to fixed-configuration mode. (If you want to configure auto-sensing ring speed, duplex mode, and port mode simultaneously, please see *Configuring Auto-Sensing Ports for Bigfoot Modules* on page 21-25.) The following prompt will be displayed.

```
New Duplex ((H)DX or (F)DX).....[currently HDX ] :
```

5. Enter **h** to set the port's duplex mode to half duplex or **f** to set it to full duplex. A prompt similar to the following will be displayed.

```
New Ring Speed ((1)6 Mbps, (4) Mbps).....[currently 16 Mbps] :
```

6. Enter **1** to set the port's ring speed to 16 Mbps or **4** to set it to 4 Mbps. If you are configuring an Omni Switch/Router TSX-C-32W, go to Step 8 on page 21-28. Otherwise, the following prompt will be displayed.

```
New Mode ((L)obe or (S)tation).....[currently Station] :
```

7. Enter **l** to configure the port as a Lobe port or **s** to configure the port as a Station port.

8. A prompt similar to the following will be displayed.

New ARI/FCI Bit ((N)on-local, (R)epeat or (A)lways)..[currently Nonlocal] :

9. This field sets the control mode for handling Address Recognized Indicator (ARI)/Frame Copied Indicator (FCI) bits. There are three possible ways for handling the ARI/FCI bits:
- **Nonlocal.** Set the ARI/FCI bits on remote LLC frames repeated by the port and for local LLC frames repeat the ARI/FCI bits just as they are received.
 - **Repeat.** The ARI/FCI bits on all LLC frames are repeated just as they are received.
 - **Always.** Set the ARI/FCI bits on all LLC frames repeated by the port.

Enter **n** to set the control method to non-local, **r** for repeat, or **a** for always. A prompt similar to the following will be displayed.

Active Monitor Participation? (Y/N).....[currently No] :

10. The active monitor performs certain functions (e.g., ensuring that frames do not circulate endlessly on the ring, ensuring that there is a valid token on the ring) to ensure that the ring functions properly.

Enter **n** to turn off active monitor participation or **y** to turn it on.

11. All of the changes you have made will take effect when you reboot the switch or reset the module. Therefore, the **tpcfg** command gives you the option to reset the port now and displays the following prompt.

Would you like to reset the port now? (Y/N) [N] :

12. Enter **y** to reset the Token Ring port or enter **n** (the default) to skip the reset. If you answered **n**, then go to step 13. If you answered **y**, then a confirmation prompt similar to the following will be displayed.

**Reset the Token Ring port 4/5 may cause disruption to the ring.
Are you sure you want to do this ? (Y/N) [N] :**

Enter **n** (the default) to skip the reset or **y** to implement it immediately.

13. The following prompt will be displayed.

Enter Slot/Interface [<ret> to exit] :

14. Enter the slot and port number to configure another port or press the **<Return>** key to exit.

◆ **Note** ◆

You can confirm your changes with the **tpvc** command, which is described in *Displaying Token Ring Port Status* on page 21-44.

Configuring the Locally-Administered Token Ring Base MAC Address for Bigfoot Modules

You can use the **tsmcfg** command to create or modify a locally-administered (i.e., user-configured) base MAC address for Bigfoot Token Ring modules (which are described in *Bigfoot Modules* on page 21-3). You can use a locally administered MAC to uniquely-identify the Token Ring module on the network.

To use the **tsmcfg** command to configure a locally-administered MAC address f, follow the steps below.

1. At the system prompt, enter

```
tsmcfg
```

The following prompt will be displayed.

```
Enter Slot to change the Configured Base MAC Address [<ret> to exit] :
```

2. Enter the slot number of the Token Ring module you want to create or modify a locally-administered MAC address. For example, if the Token Ring module is in Slot 5, enter

```
5
```

at the prompt. The following prompt is displayed.

```
Choose entry format ((N)on-canonical or (C)anonical  
or (D)isable Locally Administered MAC Addresses) :
```

Enter **c** to use the canonical format or **n** to use the non-canonical format. (If you want to disable the locally-administered MAC address, see *Disabling the Locally-Administered Token Ring Base MAC Address for Bigfoot Modules* on page 21-30). The following prompt is displayed.

```
Enter New Base MAC Address (current value is 000000:000000) :
```

3. Enter a unique MAC address in canonical format if you answered **c** in Step 2 or non-canonical format if you answered **n** in Step 2. (The current MAC address displayed in the parentheses will be in canonical format if you answered **c** in Step 2 or non-canonical format if you answered **n** in Step 2.) A prompt similar to the following will be displayed.

```
The new value is saved in the configuration and will be  
activated on next Reset command or after reboot.  
Would you like to reset slot 5 now? (y/n) [n] :
```

4. Enter **y** to reset the Token Ring module or enter **n** (the default) to skip the reset.

◆ Note ◆

You can confirm your changes with the **tsmvc** command, which is described in *Displaying Token Ring Base MAC Addresses* on page 21-42.

Disabling the Locally-Administered Token Ring Base MAC Address for Bigfoot Modules

You can use the **tsmcfg** command to disable a locally-administered (i.e., user-configured) base MAC address for Bigfoot Token Ring modules. This will ensure that the firmware-based MAC address is used instead of a user-defined address.

To use the **tsmcfg** command to disable the locally-configured MAC address, follow the steps below.

1. At the system prompt, enter

```
tsmcfg
```

The following prompt will be displayed.

```
Enter Slot to change the Configured Base MAC Address [<ret> to exit] :
```

2. Enter the slot number of the Token Ring module you want to disable a locally-administered MAC address. For example, if the Token Ring module is in Slot 5, enter

```
5
```

at the prompt. The following prompt is displayed.

```
Choose entry format ((N)on-canonical or (C)anonical  
or (D)isable Locally Administered MAC Addresses) :
```

Enter **d** to disable the locally-administered base MAC address. (If you want to configure the locally-administered MAC address, see *Configuring the Locally-Administered Token Ring Base MAC Address for Bigfoot Modules* on page 21-29). A prompt similar to the following will be displayed.

```
Locally administered MAC address has been disabled on slot 5.  
Universally Administered MAC address will take  
effect on next Reset command or after reboot.  
Would you like to reset slot 5 now? (y/n) [n] :
```

3. Enter **y** to reset the Token Ring module or enter **n** (the default) to skip the reset.

◆ Note ◆

You can confirm your changes with the **tsmvc** command, which is described in *Displaying Token Ring Base MAC Addresses* on page 21-42.

Enabling or Disabling Token Ring Switching

To use the **trsw** command to enable or disable Token Ring Switching, enter

trsw

at the system prompt. A screen similar to the following menu will be displayed.

Token Ring Switching DISABLED Enable 1 / Disable 2 / Return nothing ?

This screen displays the feature's current status (**Enabled** or **Disabled**), options and key commands (e.g., **Enable 1**). Supporting Bigfoot and Early-Generation Token Ring Modules, the Token Ring Switching feature can be enabled to prevent Source Route traffic from using the switch's learning mechanism, optimizing availability of usable CAM space and reducing the risk of potential connectivity issues (see *Benefits and Risks* table below). By disabling this feature, Source Routing can work with the Auto Tracking or Group Mobility features, and MAC addresses will be learned and stored in CAM.

The diagram on the following page illustrates how Ring Switching can be used to optimize Source Learning for improved throughput efficiency.

Feature	Benefits and Risks	
When Ring Switching is Enabled...	MAC Address Learning is reduced	MAC Addresses are Learned for Directly Attached Rings Only
	Risk of Flooding is reduced	Trunking protocols are not supported
	Usable CAM Availability is optimized	AutoTracker & Group Mobility features are not supported

MAC addresses from workstations residing on directly-attached rings, transparently-bridged frames and frames having RIFs pointing to directly-attached rings or with 2 bytes allocated to Explorer (for route discovery) will always be learned, regardless whether Token Ring Switching is enabled or disabled.

To enable Token Ring Switching, enter **1** at the prompt. (To disable this feature, enter **2** at the prompt.) A confirmation screen similar to the following message will be displayed:

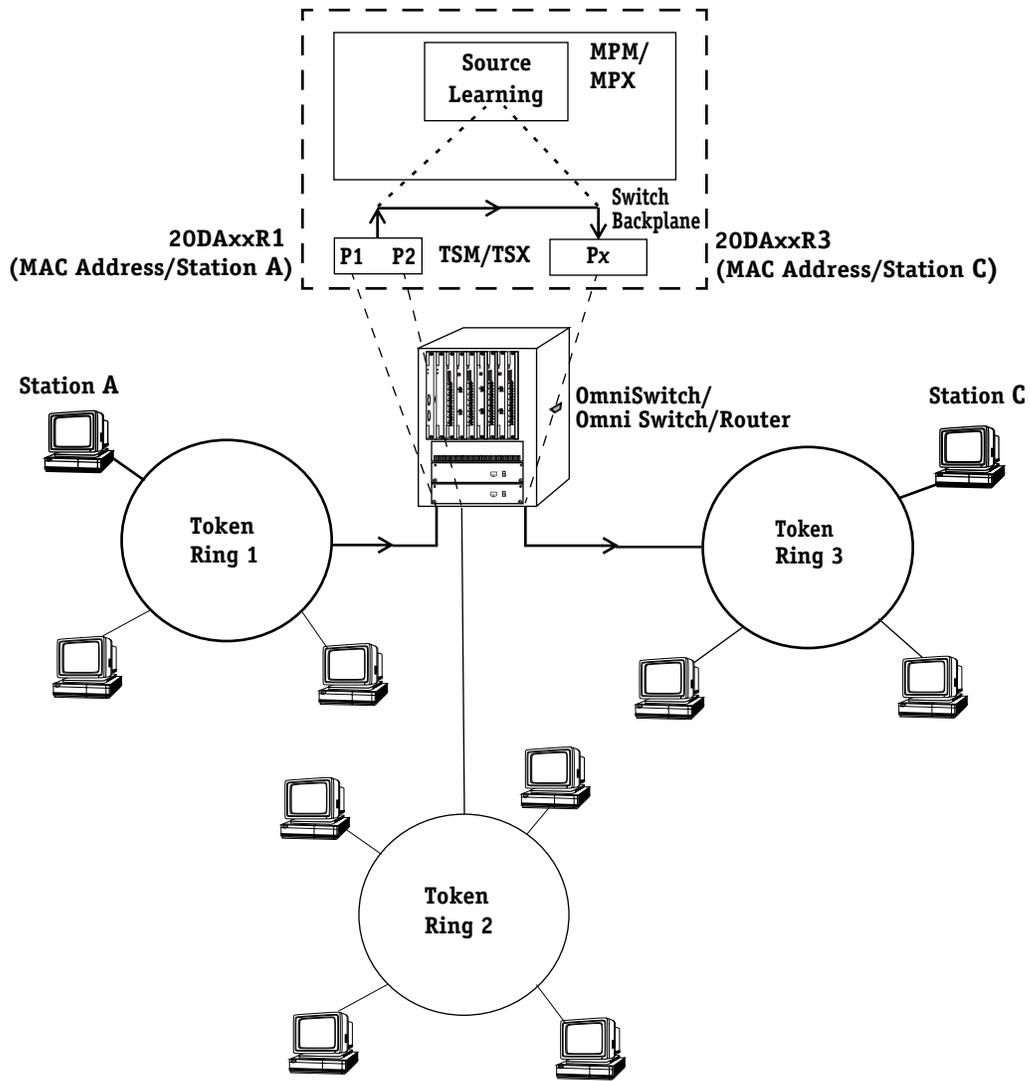
The modification of Ring Switching will be effective after the reboot of the node

Next, reboot the system to enable or disable Token Ring Switching.

◆ Note ◆

The system must be rebooted to enable or disable Token Ring Switching.

To escape without changing the current setting for this feature, don't enter a value – just press the **Enter** key at the system prompt.



Optimizing Source Learning with Ring Switching

Configuring Token Ring Port Switching

To display the Token Ring Port Switching menu, enter **trportsw** at the system prompt. Then enter a **?**. A screen similar to the following menu will be displayed.

<u>Command</u>	<u>Token Ring Port Switching Menu</u>
crtsmap	Add ports to map
dtsmap	Delete ports from map
vtsmap	View ports from map

For Omni Switch/Router TSX-series Token Ring Modules, the Token Ring Port Switching feature can be used to create a one-to-one mapping between two Token Ring virtual ports belonging to a certain group, or between a Token Ring virtual port and an ATM virtual port configured for the same group. Because hop counts are limited in a Token Ring network, Port Switching can be used in a split ring to ensure that an extra hop will not be incurred when adding an additional switch into an established network.

When Port Switching is enabled between a pair of mapped ports, no MAC addresses are learned on the ports. Traffic is switched between them without additional checking, improving system performance.

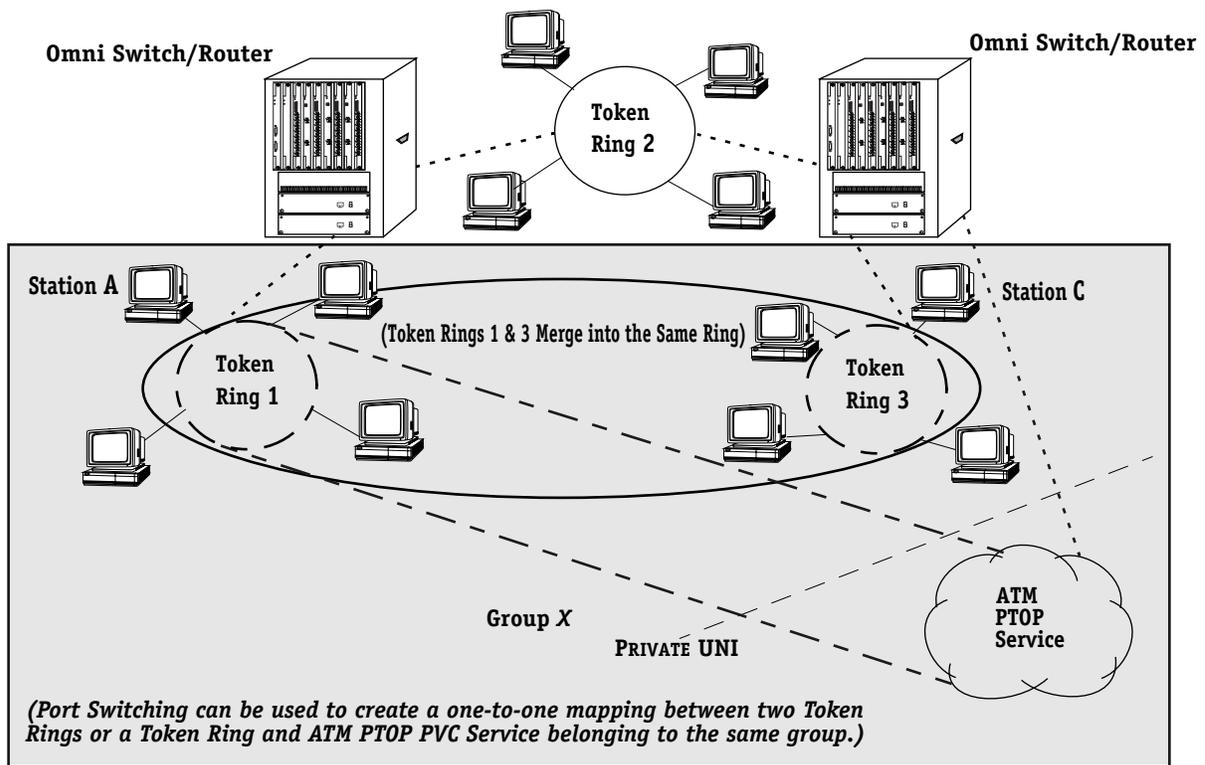
The diagram on the following page shows how Port Switching can be used to create a one-to-one mapping between two Token Ring virtual ports (or a Token Ring virtual port and an ATM virtual port) configured for the same group. (The ATM Service must be PTOPT PVC.)

◆ Important Notes ◆

Port Switching is supported only for Source Routing. It is supported on Omni Switch/Router TSX-series Token Ring Modules, but is not supported on OmniSwitch TSM-series Modules.

For optimum LAN performance, the Spanning Tree feature should be disabled *before* enabling Port Switching. To change the Spanning Tree configuration, see Chapter 22, "Configuring Bridging Parameters."

Configuring Token Ring Port Switching



Creating a One-to-One Mapping with Port Switching

Mapping Token Ring Ports

The **crtsmap** command can be used to map a Token Ring port to another Token Ring port or to an ATM PTOp PVC service. The syntax for this command is:

```
crtsmap <group_id> <TR_slot/TR_port>-{<ATM_slot/ATM_port/ATM_service>
|<TR_slot/TR_port>}
```

The fields used by the **crtsmap** command are described below:

- group_id.** The group id number for the corresponding mapped port(s).
- TR_slot.** The slot number location of the source Token Ring port.
- TR_port.** The port number location of the source Token Ring port.
- ATM_slot.** The slot number location for destination ATM PTOp PVC Service.
- ATM_port.** The port number location for destination ATM PTOp PVC Service.
- ATM_service.** The service number for destination ATM PTOp PVC Service.
- TR_slot.** The slot number location of the destination Token Ring port.
- TR_port.** The port number location of the destination Token Ring port.

◆ **Note** ◆

Port Switching supports both Token Ring and ATM PTOp PVC service.

To map to a Token Ring Port, see *Mapping a Token Ring Port to Another Token Ring Port* on page 21-36. To map to an ATM PTOp PVC Service, see *Mapping a Token Ring Port to an ATM PTOp PVC Service* on page 21-36.

Mapping a Token Ring Port to Another Token Ring Port

To create a mapping between two Token Ring ports belonging to the same group, enter **crtsmap** at the system prompt, followed by the Group I.D. Number, Slot and Port locations for both Token Ring ports at the system prompt. For example, to create a mapping between Token Ring Port 7 in Group 5, Slot 6 and Token Ring Port 1 in Group 5, Slot 7, the following command would be entered:

```
crtsmap 5 6/7 7/1
```

At this point, a map would be created between both Token Ring ports, as indicated by the following confirmation screen:

```
Created a map for group 5 between Token Ring 6/7 and Token Ring 7/1
```

Mapping a Token Ring Port to an ATM PTOp PVC Service

To create a mapping between a Token Ring port and an ATM PTOp PVC Service belonging to the same group, enter **crtsmap** followed by the Group I.D. Number, Slot and Port locations for the Token Ring port and ATM Service (include the **atm service number**) at the system prompt. For example, to create a mapping between Token Ring Port 7 in Group 5, Slot 6 and ATM PTOp Service 2 in Group 5, Slot 8, Port 1, the following command would be entered:

```
crtsmap 5 6/7 8/1/2
```

At this point, a map would be created between the Token Ring port and the ATM Service, as indicated by the following confirmation screen:

```
Created a map for group 5 between Token Ring 6/7 and ATM 8/1/2
```

◆ **Note** ◆

Port Switching supports both Token Ring and ATM PTOp PVC service.

Viewing Mapped Ports Configured Within the System

Enter **vtsmmap** at the system prompt to view all mapped ports configured within the system. A screen similar to either of the following displays will appear.

With a Token Ring connection:

MapNumber	Group	TOKEN RING Slot/Port/Vport			ATM or TOKEN RING Slot/Port/Vport		
		Slot	Port	Vport	Slot	Port	Vport
1	5	6/	7/	15	7/	1/	16

With an ATM connection:

MapNumber	Group	TOKEN RING Slot/Port/Vport			ATM or TOKEN RING Slot/Port/Vport		
		Slot	Port	Vport	Slot	Port	Vport
2	5	6/	7/	15	8/	1/	36

The fields used by the **vtsmmap** command are described below.

MapNumber. The label identifying the corresponding mapped ports.

Group. The Group I.D. Number for the corresponding mapped ports.

TOKEN RING Slot. The slot number location of the mapped source Token Ring port.

TOKEN RING Port. The physical port number location of the mapped source Token Ring port.

TOKEN RING Vport. The virtual port number location of the mapped source Token Ring port.

ATM or TOKEN RING Slot. The slot number location for the destination ATM PTOp PVC Service or Token Ring port.

ATM or TOKEN RING Port. The physical port number location for the destination ATM PTOp PVC Service or Token Ring port.

ATM or TOKEN RING Vport. The virtual port number location for the destination ATM PTOp PVC Service or Token Ring port.

Deleting Mapped Ports

The **dtsmap** command deletes a specific Token Ring map (mapped ports and associated MapNumber) from the Map table. To delete mapped ports from the Map table, enter:

dtsmap <MapNumber>

at the system prompt, where **<MapNumber>** indicates the MapNumber of the mapped ports to be deleted. (The MapNumber can be identified by using the **vtsmmap** command described on the previous page.)

To delete MapNumber 2, for example, enter:

dtsmap 2

(No additional confirmation screen will appear.)

To confirm that the specified Token Ring map has been deleted, enter **vtsmmap** at the system prompt to view any remaining mapped ports configured within the system.

Displaying the Status Table for Token Ring Modules

You can use the **tprs** command to display the status of every Token Ring port in your switch. This command is supported on Bigfoot and early-generation Token Ring modules. To use this command, enter

tprs

at the system prompt. A screen similar to the following will be displayed.

Token Ring Status Table for all slots											
Slot/ Intf	Signal Loss	Hard Error	Soft Error	Trans Beacon	LobeWir Fault	Auto Remove	Remove Receve	Cntr Ovflow	Single Statn	Ring Recov	FDX Error
5/ 1	0	0	0	0	0	0	0	0	0	0	0
5/ 2	0	0	0	0	0	0	0	0	0	0	0
5/ 3	0	0	0	0	0	0	0	0	0	0	0
5/ 4	0	0	0	0	0	0	0	0	0	0	0
5/ 5	0	0	0	0	0	0	0	0	0	0	0
5/ 6	0	0	0	0	0	0	0	0	0	0	0
5/ 7	0	0	0	0	0	0	0	0	0	0	0
5/ 8	0	0	0	0	0	0	0	0	0	0	0
5/ 9	0	0	0	0	0	0	0	0	0	0	0
5/10	0	0	0	0	0	0	0	0	0	0	0
5/11	0	0	0	0	0	0	0	0	0	0	0
5/12	0	0	0	0	0	0	0	0	1	1	0
5/13	0	0	0	0	0	0	0	0	0	0	0
5/14	0	0	0	0	0	0	0	0	0	0	0
5/15	0	0	0	0	0	0	0	0	0	0	0
5/16	0	0	0	0	0	0	0	0	0	0	0

◆ Note ◆

The **FDX Error** column will not be displayed for early-generation (e.g., TSM-CD-6, TSM-F-6) Token Ring modules because they do not support full-duplex Token Ring mode.

The fields displayed by the **tprs** command are described below.

Slot/Intf. The slot and port number of the Token Ring port.

Signal Loss. The number of times this port has detected a loss of signal from the ring.

Hard Error. The number of hard errors detected by this port and the number of times this port has transmitted or received a beacon MAC frame.

Soft Error. The number of soft errors detected by this port and the number of times this port has transmitted or received a report error MAC frame.

Trans Beacon. The number of times this port has transmitted a beacon frame.

LobeWir Fault. The number of times this port has detected an open or short circuit in the lobe data path.

Auto Remove. The number of times an auto remove process has taken place on this port.

Remove Receve. The number of times this port has received a Remove Ring Station MAC frame request.

Cntr Ovflow. The number of times a counter overflow has taken place on this port.

Single Statn. The number of times that this port has it is the only station on the ring.

Displaying the Status Table for Token Ring Modules

Ring Recov. The number of times the ring has been purged and brought back to an operating state.

FDX Error. The number of times a full-duplex protocol error has been detected by this port. This field will not be displayed on early-generation Token Ring modules.

Displaying the Token Ring Interface Type

You can display the interface types for all Token Ring modules in a chassis with the **tsc** command. You can use the **tsc** command in display mode on early-generation and Bigfoot modules. To use this command to display the interface type, follow the steps below.

◆ Note ◆

See *Configuring the Interface Type on Early-Generation Modules* on page 21-21 for documentation on using the **tsc** command to configure the interface type on certain (e.g., TSM-CD-6 or TSM-F-6) early-generation Token Ring modules.

1. At the system prompt, enter

```
tsc
```

A screen similar to the following will be displayed.

```
Token Ring slot interface table
Slot  Interface Type
-----
3     C32-RJ45
5     C16-RJ45 DUAL MODE
Enter Slot Number [<ret> to exit] :
```

2. Press the **<Return>** key to exit. An error message will be displayed if you enter the slot number of a Bigfoot Token Ring module or a TSM-C-6.

The fields displayed by the **tsc** command (when used to display the interface type) are described below.

Slot. The slot number of the Token Ring module.

Interface Type. The port type on the Token Ring module. The words **DUAL MODE** in this field indicates the module supports dual Station/Lobe mode.

Displaying Token Ring Base MAC Addresses

You can display the locally-administered (i.e., user-configured) and the firmware-based base MAC addresses in canonical and non-canonical formats for Bigfoot Token Ring modules with the **tsmvc** command. (The locally-administered MAC address can be created and modified with the **tsmcfg** command, which is described in *Configuring Auto-Sensing Ports for Bigfoot Modules* on page 21-25.) See the subsection below for information on using the **tsmvc** command with Bigfoot modules.

For early-generation Token Ring modules, the **tsmvc** displays the firmware-based MAC address in canonical and non-canonical format only since you cannot configure a locally-administered MAC address on these modules. See *Displaying the Base MAC Address for Early-Generation Modules* on page 21-43 for information on using the **tsmvc** command with early-generation modules.

Displaying Base MAC Addresses for Bigfoot Modules

To use the **tsmvc** command with Bigfoot Token Ring modules, enter

```
tsmvc
```

at the system prompt. A screen similar to the following will be displayed.

The Token Ring Base MAC Address for all slots				
Slot	Local MAC Address (Canonical)	Local MAC Address (Non-canonical)	Universal MAC Address (Canonical)	Universal MAC Address (Non-canonical)
5	000000:000000	000000:000000	0020DA:B07D50	00045B:0DBE0A

The fields displayed by the **tsmvc** command for Bigfoot modules are described below.

Slot. The chassis slot number of the Token Ring module.

Local MAC Address (Canonical). The locally-administered MAC address of the Token Ring module in canonical format.

Local MAC Address (Non-canonical). The locally-administered MAC address of the Token Ring module in non-canonical format.

Universal MAC Address (Canonical). The firmware-based MAC address of the Token Ring module in canonical format.

Universal MAC Address (Non-canonical). The firmware-based MAC address of the Token Ring module in non-canonical format.

Displaying the Base MAC Address for Early-Generation Modules

To use the **tsmvc** command with early-generation Token Ring modules, enter

tsmvc

at the system prompt. A screen similar to the following will be displayed.

The Token Ring Base MAC Address for all slots				
Slot	Local MAC Address (Canonical)	Local MAC Address (Non-canonical)	Universal MAC Address (Canonical)	Universal MAC Address (Non-canonical)
3	** Function not supported **		0020DA:022F50 0020DA:06A490	00045B:40F40A 00045B:602509

The fields displayed by the **tsmvc** command for early-generation modules are described in *Displaying Base MAC Addresses for Bigfoot Modules* on page 21-42. Please note that the **Local MAC Address (Canonical)** and **Local MAC Address (Non-canonical)** fields will always display **** Function not supported **** since you cannot configure a locally-administered MAC address on these modules.

Displaying Token Ring Port Status

You can use the **tpvc** command to display the status for all Token Ring ports in a switch. This command is supported on Bigfoot and early-generation Token Ring modules. To use this command, enter

```
tpvc
```

at the system prompt. A screen similar to the following will be displayed.

The Token Ring Port Status Table for all slots

Slot/ Intf	Open Status	Cfg Type	Ring Speed	Duplex Mode	Port Mode	ARI/FCI Bit Set	Active Monitor	Up Stream Neighbor
3/ 1	Open	Auto	16 M	FDX	Station	Nonlocal	No	00045B:0D3E09
3/ 2	Open	Auto	16 M	HDX	Lobe	Repeat	No	00045B:0D3E89
3/ 3	Open	Auto	4 M	HDX	Station	Always	Yes	00045B:0D3E49
3/ 4	Open	Fixed	16 M	HDX	Lobe	Nonlocal	No	0000F6:8889BD
3/ 5	-----	Fixed	16 M	FDX	Station	Repeat	No	000000:000000
3/ 6	-----	Fixed	4 M	HDX	Lobe	Always	No	000000:000000
3/ 7	-----	Auto	?	?	?	Nonlocal	No	000000:000000
3/ 8	-----	Auto	?	?	?	Nonlocal	No	000000:000000
3/ 9	-----	Auto	?	?	?	Nonlocal	No	000000:000000
3/10	-----	Auto	?	?	?	Nonlocal	No	000000:000000
3/11	-----	Auto	?	?	?	Nonlocal	No	000000:000000
3/12	-----	Auto	?	?	?	Nonlocal	No	000000:000000
3/13	-----	Auto	?	?	?	Nonlocal	No	000000:000000
3/14	-----	Auto	?	?	?	Nonlocal	No	000000:000000
3/15	-----	Auto	?	?	?	Nonlocal	No	000000:000000
3/16	-----	Auto	?	?	?	Nonlocal	No	000000:000000

The fields displayed by the **tpvc** command are described below. The display format for the **tpvc** command is the same for early-generation Token Ring modules and Bigfoot modules, although some fields (e.g., **Duplex Mode**) are only meaningful for Bigfoot modules.

Slot/Intf. The slot and port number of the Token Ring port.

Open Status. The result of the last attempt to enter the ring. Possible values include **Open**, (the default), **noOpen**, **badParam**, **Lobe Fail**, **signalLoss**, **insertion Timeout**, **ringFailed**, **beaconing**, **duplicateMAC**, **requestFailed** and **Down**. Dashes will be displayed if this port is on a Bigfoot Token Ring module and the configuration type has not been sensed yet.

Cfg Type. This field displays if the port is auto-sensing (**Auto**) or has a fixed configuration (**Fixed**). Early-generation Token Ring modules will always display **Fixed** since auto-sensing is not available on those modules.

Ring Speed. This field displays the ring speed (4 or 16 Mbps) of the port. A question mark (?) will be displayed if this port is on a Bigfoot Token Ring module and the ring speed has not been sensed yet.

Duplex Mode. This field displays the duplex mode, which can be full duplex (**FDX**) or half duplex (**HDX**) on Bigfoot Token Ring modules and half duplex (**HDX**) only on early-generation Token Ring modules. A question mark (?) will be displayed if this port is on a Bigfoot Token Ring module and the duplex mode has not been sensed yet.

Port Mode. The field displays the port mode, which can be Station or Lobe on dual-mode modules (e.g., the Omni Switch/Router TSX-CD-16W and the OmniSwitch TSM-CD-16W) or Lobe only on single-mode Omni Switch/Router TSX-C-32W and Station only on the single-mode OmniSwitch TSM-C-6.

ARI/FCI Bit Set. This field shows the control mode for handling ARI/FCI bits. (The default is **Nonlocal**.) The following are possible values.

Nonlocal. Set the ARI/FCI bits on remote LLC frames repeated by the port and for local LLC frames repeat the ARI/FCI bits just as they are received.

Repeat. The ARI/FCI bits on all LLC frames are repeated just as they are received.

Always. Set the ARI/FCI bits on all LLC frames repeated by the port.

Active Monitor. This field shows if the port participates in the active monitor selection.

Upstream Neighbor. The MAC address of the upstream neighbor (i.e., next port on the ring) for this port.

Displaying Token Ring Port Error Statistics

You can use the **tperrs** command to display error statistics for all the Token Ring ports in your switch. This command is supported on Bigfoot and early-generation Token Ring modules. To use this command, enter

```
tperrs
```

A screen similar to the following will be displayed.

Token Ring Error Statistics Table for all slots									
Slot/ Intf	Line Error	Burst Error	ARI/FCI Error	Lost_Fm Error	Rcv_Cng Error	Token Error	DMA_Bus Error	DMA_Par Error	
5/1	0	0	0	0	0	0	0	0	0
5/2	0	0	0	0	0	0	0	0	0
5/3	0	0	0	0	0	0	0	0	0
5/4	0	0	0	0	0	0	0	0	0
5/5	0	0	0	0	0	0	0	0	0
5/6	0	0	0	0	0	0	0	0	0
5/7	0	0	0	0	0	0	0	0	0
5/8	0	0	0	0	0	0	0	0	0
5/9	0	0	0	0	0	0	0	0	0
5/10	0	0	0	0	0	0	0	0	0
5/11	0	0	0	0	0	0	0	0	0
5/12	0	0	0	0	0	0	0	0	0
5/13	0	0	0	0	0	0	0	0	0
5/14	0	0	0	0	0	0	0	0	0
5/15	0	0	0	0	0	0	0	0	0
5/16	0	0	0	0	0	0	0	0	0

The fields displayed by the **tperrs** command are described below. The display format is the same for early-generation modules and Bigfoot modules.

Slot/Intf. The slot and port number of the Token Ring port.

Line Error. The number of times a frame or token with an error has been copied or repeated by this port.

Burst Error. The number of times this port has detected an absence of transitions for five (5) half-bit times (burst-five error).

ARI/FCI Error. The number of times this port has received an AMP or SMP frame with improperly-set AC bits.

Lost_Fm Error. Lost Frame Error. The number of times this port failed to receive an end of its transmit frame.

Rcv_Cng Error. Receive Congestions. The number of times this port received a frame but no buffer space was available.

Token Error. The number times this port, when acting as the active monitor, recognized an error in the token protocol.

DMA_Bus Error. The number of DMA bus errors on this port that did not exceed the abort threshold.

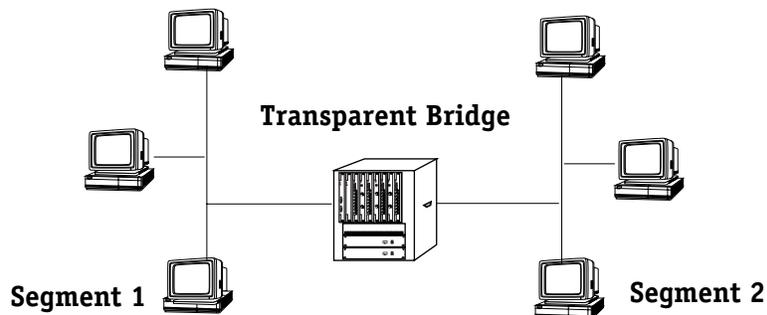
DMA_Par Error. The number of DMA bus errors on this port that did not exceed the abort threshold.

22 Configuring Bridging Parameters

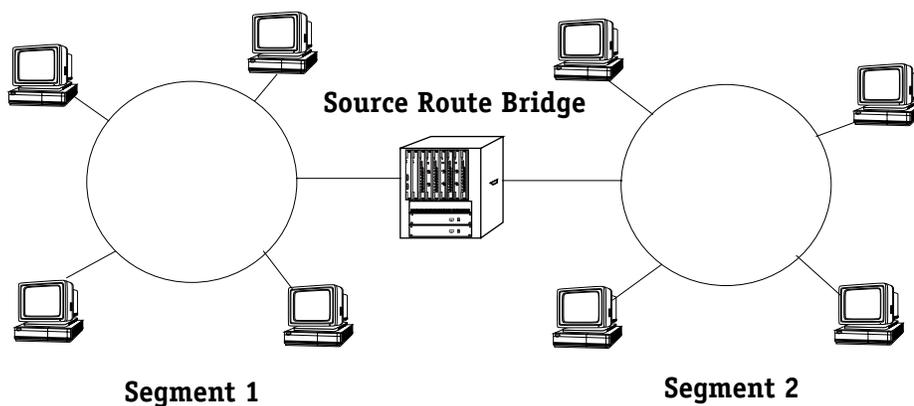
This chapter describes how to configure and maintain bridging parameters. Bridges are devices that interconnect LANs using one (or more) of the available standards such as transparent bridging, source route bridging, or source route to transparent bridging. Bridges primarily operate at Layer 2 of the OSI reference model, which controls data flow, transmission errors, physical addressing, and access to physical medium.

There are different types of bridging that are used to manage networks:

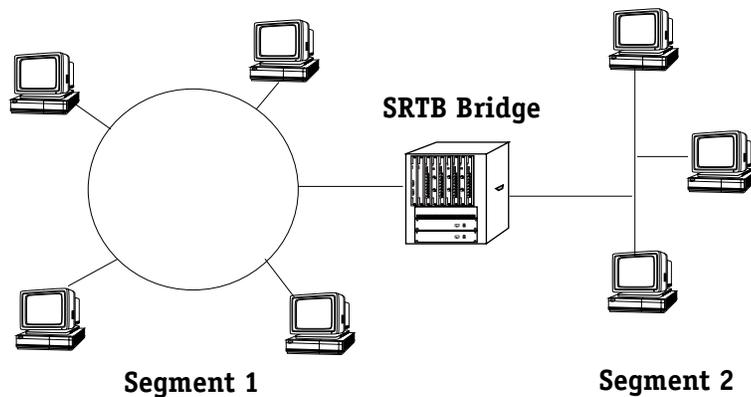
- **Transparent Bridging.** Used mainly in Ethernet environments, packets are usually forwarded without any changes being made to the packet. An ethernet environment is shown in the diagram below:



- **Source Route Bridging.** Used mainly in Token Ring environments, packets are transmitted along routes predetermined by explorer frames sent along multiple paths. Source Route Bridging modifies the routing information of the packet as it traverses the network. A token ring environment is shown in the diagram below:



- **Source Route to Transparent Bridging.** Used in mixed Ethernet and Token Ring environments, this protocol provides easy translation between transparent and source route bridging. A mixed ethernet and token ring environment is shown in the diagram below:



Spanning tree and fast spanning tree are also used to prevent physical loops in the network from creating excess traffic by blocking packet transmission on one or more ports.

This chapter describes the commands used for configuring various bridging commands for the above mentioned protocols, as well as diagnostic, spanning tree and fast spanning tree information.

◆ Important Notes ◆

In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. See Chapter 8, "The User Interface," for documentation on changing from CLI mode to UI mode.

Beginning with Release 4.4, FDDI is no longer supported.

Configuration Overview

When configuring bridging parameters, you will need to perform at least some of the following steps:

Step 1. Select a group

The bridging menu commands operate only on the currently selected group (or, for certain commands, VLAN). You can select a group with the **selgp** command. For information on using these commands, see *Selecting a Default Group* on page 22-7.

Step 2. Configure Bridging Parameters

There are several commands that allow you to configure and view basic bridging functions such as static MAC addresses, bridge forwarding tables, MAC information and statistics, and remote Trunking stations. Many of these commands are useful in diagnosing network problems, as they allow you to find specific MAC addresses and the port on which they were learned. For information on these commands, see *Bridging Commands* on page 22-8.

Step 3. Enable Spanning Tree (Optional)

Spanning tree is an algorithm that helps prevent broadcast storms by blocking ports in the network from transmitting data. If you plan to use spanning tree, you can use the spanning tree commands to configure and view IEEE and IBM Spanning Tree. For information on using spanning tree commands, see *Configuring Spanning Tree* on page 22-23.

Step 4. Enable Fast Spanning Tree (Optional)

Fast Spanning Tree is an algorithm that helps provide quick recovery from link, port and device failures on a network, by bringing blocked secondary links into forwarding mode as quickly as possible. You can the Fast Spanning Tree commands in the Bridge Management Menu to view and enable/disable Fast Spanning Tree parameters on a selected group or VLAN. For information on using Fast Spanning Tree commands, see *Configuring Fast Spanning Tree* on page 22-34.

Step 5. Configure Source Routing (Optional)

Traditional source routing is the practice of including routing information in the packet header. This serves to supply the route that the frame should take from source to destination. The source routing commands provided in the Bridge Management Menu are described in detail in Chapter 21, "Managing Token Ring Modules."

Step 6. Configure Source Route to Transparent Bridging (Optional)

If your network is a combination of Ethernet and Token Ring, you may want to use Source Route to Transparent Bridging (SRTB) to link these different network media. For information on SRTB, see *Configuring Source Route to Transparent Bridging* on page 22-43.

Bridge Management Menu

To view the Bridge Management Menu, enter the **br** command at the system prompt. If you are in verbose mode, the following table appears outlining the commands available to you. If you are not in verbose mode, enter a **?** at the prompt to display the Bridge Management Menu.

Command	Bridge Management Menu
fls	Display Flood Limit of selected Group
flc	Configure Flood Limit on selected Group
sts	Display Spanning Tree parameters on selected Group
fstps	Display Fast Spanning Tree port parameters on selected VLAN
actfstps	Activate Fast Spanning Tree port parameters on selected VLAN
stc	Configure Spanning Tree parameters on selected Group
stps	Display Spanning Tree Port parameters on selected VLAN
stpc	Configure Spanning Tree Port parameters on selected VLAN
srs	Display Source Routing parameters on selected Group
src	Configure Source Routing parameters on selected Group
srsf	Enable or disable Source Routing SAP Filter Support
srtbcfg	View and configure Source Route to Transparent Bridging
srtbrif	View learned RIF from Source Route to Transparent Bridging Table
srtbclrrif	View and Clear learned RIF from Source Route to Transparent Bridging Table
fwf	Display Bridge Forward table on selected VLAN
fs	Display Bridge Static Address
fc	Configure Bridge Static Address
bps	Display Bridge Port Statistics on selected VLAN
macinfo	Locate learned Bridge MAC address in this chassis
macstat	Show statistics of Bridge MAC address
macclrstat	Clear statistics of Bridge MAC address
selgp	A Group can be selected for the bridge operations or to generate MIB reports
rts	Display remote Trunking Stations discovered
dbrmap	View the Domain Bridge Mapping table
+ / -	Select next / previous VLAN

Details on commands included in the Bridge Management Menu commands are given in the following sections:

Setting the Default Group. These commands allow you to choose which group you are modifying or viewing, and include the **selgp**, **+**, and **-** commands. For more information, see:

- *Selecting a Default Group* on page 22-7
- *Using the + or - to Change Groups* on page 22-7 for more information.

Bridging Commands. These commands allow you to view bridge forward tables, create and view static address tables, display bridge port statistics, view MAC address information, view remote trunking stations, and view the domain bridge mapping table. Commands in this section include **fw**, **fs**, **fc**, **bps**, **macinfo**, **macstat**, **macclrstat**, **rts**, and **dbrmap**. For more information, see:

- *Displaying Bridge Forwarding Table* on page 22-8
- *Configuring a Static Bridge Address* on page 22-10
- *Displaying Static Bridge Addresses* on page 22-13
- *Displaying Bridge Port Statistics* on page 22-14
- *Displaying Media Access Control (MAC) Information for a Specific MAC address* on page 22-16
- *Display Statistics of Bridge MAC Addresses* on page 22-17
- *Clear Statistics of Bridge MAC Addresses* on page 22-18
- *Display Remote Trunking Stations* on page 22-18
- *View the Domain Bridge Mapping Table* on page 22-19

Setting Flood Limits. These commands allow you to configure and view flood limits for a specific group using the **flc** and **fls** commands. For more information, see:

- *Setting Flood Limits for a Group* on page 22-21
- *Displaying Group Flood Limits* on page 22-22

Configuring Spanning Tree. These commands allow you to configure and view IEEE and IBM Spanning Tree for a specific group, and include the **stc**, **sts**, **stpc** and **stps** commands. (The **stc** and **sts** commands can also be used to configure and view Fast Spanning Tree for a selected VLAN.) For more information, see:

- *Configuring Spanning Tree Parameters* on page 22-25
- *Display Spanning Tree Bridge Parameters* on page 22-28
- *Configuring Spanning Tree Port Parameters* on page 22-30
- *Displaying Spanning Tree Port Parameters* on page 22-32

Configuring Fast Spanning Tree. These commands allow you to configure and view Fast Spanning Tree for a specific group or VLAN, and include the **actfstps** and **fstps** commands. Information is also included on configuring the Truncating Tree Timing and Speedy Tree Protocol features. For more information, see:

- *Configuring Truncating Tree Timing & Speedy Tree Protocol* on page 22-35
- *Displaying Fast Spanning Tree Port Parameters* on page 22-36
- *Enabling Fast Spanning Tree Port Parameters* on page 22-38
- *Disabling Fast Spanning Tree Port Parameters* on page 22-39

Configuring Source Routing. These commands allow you to configure and view Source Routing for a specific ring, as well as set a SAP filter for outgoing traffic. These commands include the **src**, **srs**, and **srsf** commands. These commands are described in Chapter 21, “Managing Token Ring Modules.” For more information, see:

- *SAP Filtering* on page 22-40.

Configuring Source Route to Transparent Bridging. These commands allow you to configure and view source routing to transparent bridging for networks with bridges connecting Ethernet and Token Ring segments, and include the **srtbcfg**, **srtbrif**, and **srtbclrrif**. For more information, see:

- *Enabling SRTB for a Group* on page 22-44
- *Disabling SRTB for a Group* on page 22-45
- *Viewing the RIF Table* on page 22-46
- *Clearing the RIF Table* on page 22-47.

Selecting a Default Group

Most commands in the Bridge Management Menu allow you to specify a group when entering the command at the system prompt. If you do not specify a group when entering a command, the bridge operations are performed on the currently selected group.

◆ Note ◆

You can view the current groups in the switch by entering **gp** at any prompt.

To select a group, enter the **selgp** command as follows:

```
selgp <group number>
```

where **<group number>** is the number of the group you wish to modify or view. For example, to select Group 2 you would enter **selgp** and the number **2** as shown:

```
selgp 2
```

A message confirming the selection of the new group ID followed by the group description.

```
Group number: 2 is now selected (New GROUP (#1)).
```

Using the + or - to Change Groups

At any time from the system prompt, you can select a different group by typing a plus (+) to move up one group, or a minus (-) to move back one group. For example, if you are currently working on Group 4 and wish to change to Group 3, you would enter a - at the system prompt. The following message displays to confirm the change:

```
Currently GROUP 3 is selected (New GROUP (#3))
```

Bridging Commands

The Bridge Management menu provides several commands that are useful in pinpointing problems in the network. The commands allow you to lookup specific MAC addresses and where they were learned, create and view static bridge addresses, view information on remote trunking stations, view MAC address statistics for a group or a port, or look up information on domain mappings. Many times a network problem can be tracked down by viewing MAC address information, finding out where it came from, and where it forwards data.

The following sections detail the specific bridging commands that perform these functions.

Displaying Bridge Forwarding Table

You can display the MAC addresses and their forwarding and filtering information for a given group. The information in the table is used by the transparent bridging function in determining how to propagate a received frame.

To display the information for a group in the switch follow these steps:

1. Enter the **fw**t command at the system prompt as follows:

```
fw t <group number>
```

where **<group number>** is the number of the group for which you want to view MAC addresses. For example, to view MAC addresses for group 2, you would enter:

```
fw t 2
```

As a variation of this command, you can enter the **fw**t command without a group ID. This will display MAC addresses for the currently selected group in this switch. For information on selecting a group, see *Selecting a Default Group* on page 22-7.

2. Once you have entered the group number you will be prompted for a slot and port, as shown:

```
Enter Slot/Interface (return for all ports):
```

3. Enter the slot and interface (port) number and press **<return>**. For example, to view MAC addresses for port 2 on slot 3, enter 3/2 as shown:

```
Enter Slot/Interface (return for all ports): 3/2
```

The following screen appears listing the MAC addresses on this port:

Total number of MAC addresses learned for VLAN 2: 8										
Sl/If/Srv/In	MAC Address	Non-Canonical MAC Address	T	Group ID	CAM Indx	S	Last Seen	Exp Timer	ATM VCI	
3/1/ Brg/ 1	0020DA:A373B0	00045B:C5CE0D	E	2	305A	T	11	300		
3/1/ Brg/ 1	0020DA:8656F0	00045B:616A0F	E	2	3060	T	11	300		
3/1/ Brg/ 1	00045B:ED48C0	00045B:2251A1	E	2	3080	T	29	300		
3/1/ Brg/ 1	000077:8DDBB9	00045B:65EE22	E	2	3010	T	29	300		
3/1/ Brg/ 1	000039:F5520C	0009E4:3ED444	E	2	300E	T	35	300		
3/1/ Brg/ 1	009027:17F7EB	00045B:2D43EF	E	2	3018	T	59	300		
3/1/ Brg/ 1	0020DA:0C41E5	00045B:ED48C0	E	2	3078	T	26	300		
3/1/ Brg/ 1	0020DA:9645A1	0000EE:B1DB9B	E	2	304E	T	18	300		

Field Descriptions

The following section explains the fields displayed with the **fw**t command.

Sl/In/Srvc/In. The slot number (**Sl**), interface (port) number (**In**), type of service (**Srvc**), and service instance (**In**). For example, a bridge service on port 1 of slot 3 would be:

3/1/Brg/1

Services provide connection options for switches in a LAN, between LANs, or in a WAN. Other possible services include trunking, routing, and LANE. It is possible to have more than one instance of a service if there are more than one connections on a single port.

MAC Address. The learned MAC address for this port.

Non-Canonical MAC address. The non-canonical version of the learned MAC address. The non-canonical MAC address is different from a canonical MAC address in that the order in which the address information is sent is different. Ethernet uses canonical address, while other media (e.g., token ring, FDDI) use non-canonical.

T. The protocol type of this MAC address. There are two possibilities:

E	Ethernet
F	FDDI
T	Token Ring

Group ID. The associated group ID for this learned MAC address.

CAM Indx. The index number to the Content-Addressable Memory (CAM), where the MAC addresses are stored, in hexadecimal form.

S. The source of the MAC address (how it was learned). There are two possibilities:

T	Transparent Bridge
S	Source Route Frame.

Last Seen. The time in seconds since this MAC address was last seen on this port.

Exp. Timer. There are three possibilities for this column:

Value	The configured ageing timer, in seconds, for this MAC address is shown. Once this time period is exceeded, the MAC address is removed from the CAM.
STATIC	This MAC address was manually assigned to this group and will not age out.
OPSWT	This MAC address was learned on an optimized switch port and will not age out.

ATM VCI. The ATM Virtual Channel Identifier (VCI) for this MAC address entry. The VCI is shown for any media that uses Virtual Circuits (ATM, LANE).

Configuring a Static Bridge Address

You can configure static bridge address information by entering the **fc** command. A static bridge address is a fixed MAC address bridge that does not change or age out.

To configure a static MAC address follow these steps:

1. Enter the **fc** command as follows:

```
fc <groupNumber>
```

where **<groupNumber>** is the number of the group for which you want to create a static bridge MAC address. For example, to set up a static bridge address for Group 2, you would enter the following:

```
fc 2
```

As a variation of this command, you can enter the **fc** command at the system prompt with no group number. This will allow you to set up a static bridge address on the currently selected group. For information on selecting a group, see *Selecting a Default Group* on page 22-7.

The system displays the following:

```

Bridge Static Address for Group 2 (New GROUP (#2))
-----
Index   MAC Address   Slot/Intf/Service/Inst   Static Status
          (A)
-----
  1     21A33E:00B001   3/ 1/ Brg/1             permanent
-----

```

The entries can be modified by specifying the index and column.

For Static Status, use 2 to delete, 3 for Permanent,

4 for Delete on Reset, 5 for Delete on Timeout

To add an entry: Use command 'add MAC addr, receiving port, static status'.

Receiving port and Status must be provided.

Port could either be slot/intf or virtual port begin with v.

For non-canonical MAC format add 'nc' before MAC.

ie: add 123456:7890AB, 2/3, 3 or add nc001122:334455, v99, 3

NOTE: add command will be executed immediately.

save|cancel|next only applies to existing entry.

add|save|cancel|next :

2. To add an entry, use the format as described in the above screen:

```
add [MAC Addr], [Slot/Intf], [Static Status]
```

For example, to add a permanent non-canonical MAC address of 123456:123456 to port 2 of slot 3, you would enter the following:

```
add nc123456:123456, 3/2, 3
```

When you complete the operation by pressing **<return>**, an entry with MAC address 123456:123456, on slot 2, port 3, with a **Static Status** of **Permanent** is created.

3. Type **save** at the **fc** command prompt to save the entry. If you do not save the entry before exiting the **fc** command, the static bridge address is not created.

◆ Note ◆

The newly created static bridge address will not show up in the **fc** command table until you have exited the **fc** command by typing **cancel** at the command prompt.

Field Descriptions

The following section describes the fields in the **fc** command table.

Index. A number assigned to the row to identify a previously created static bridge address, when modifying the address.

MAC address. The canonical MAC address for this static bridge.

Slot/Intf/Service/Inst. The slot number, interface (port) number, type of service, and service instance. For example, a bridge service on port 1 of slot 3 would be:

3/1/Brg/1

Static Status. The status of the static MAC address as determined when created. The **Status** will be one of the following:

Invalid	This entry was deleted within the current session.
Permanent	This entry is in use and will remain so until it is deleted from the table. See <i>Deleting a Static Bridge Address</i> on page 22-12 for specific information.
deleteOnReset	This entry is in use and will remain so until the bridge is reset.
deleteOnTimeOut	This entry is currently in use and will remain so until it is aged out.

Modifying a Static Bridge Address

Once you have created a static bridge address, you can modify its interface assignment or its status. To modify a static bridge address:

1. Enter the **fc** command as documented above. The Bridge Static Address table will display as shown:

Bridge Static Address for Group 2 (Default GROUP (#2))

Index	MAC Address	Slot/Intf/Service/Inst (A)	Static Status (B)
1	21A33E:00B001	3/ 1/ Brg/1	permanent
2	001122:223344	3/ 2/ Brg/1	deleteOnReset

The entries can be modified by specifying the index and column.

For Static Status, use 2 to delete, 3 for Permanent,

4 for Delete on Reset, 5 for Delete on Timeout

To add an entry: Use command 'add MAC addr, receiving port, static status'.

Receiving port and Status must be provided.

Port could either be slot/intf or virtual port begin with v.

For non-canonical MAC format add 'nc' before MAC.

ie: add 123456:7890AB, 2/3, 3 or add nc001122:334455, v99, 3

NOTE: add command will be executed immediately.

save|cancel|next only applies to existing entry.

add|save|cancel|next :

- To modify an entry, use the index number for the specific static bridge address (listed in the leftmost column), the column letter for the column you want to change, an equal sign, and a new value. For example, to change the **Static Status** of the first address's in the table from **permanent** to **deleteOnReset**, you would enter a **1** (the static bridge address **Index** number), a **b** (the column letter for **Static Status**), an equal sign (=), and the number **4** (the value for **deleteOnReset**), as shown:

1b=4

- Press **<return>** to complete the operation.
- Type **save** at the **fc** command prompt to save the changes.

Deleting a Static Bridge Address

Deleting a previously created static bridge address is much the same process as modifying a Static Bridge Address. To delete a Static Bridge Address, follow these steps:

- Enter the **fc** command as documented above. The Bridge Static Address table will display as shown:

Bridge Static Address for Group 2 (Default GROUP (#2))

Index	MAC Address	Slot/Intf/Service/Inst (A)	Static Status (B)
1	21A33E:00B001	3/ 1/ Brg/1	permanent
2	001122:223344	3/ 2/ Brg/1	deleteOnReset

The entries can be modified by specifying the index and column.

For Static Status, use 2 to delete, 3 for Permanent,

4 for Delete on Reset, 5 for Delete on Timeout

To add an entry: Use command 'add MAC addr, receiving port, static status'.

Receiving port and Status must be provided.

Port could either be slot/intf or virtual port begin with v.

For non-canonical MAC format add 'nc' before MAC.

ie: add 123456:7890AB, 2/3, 3 or add nc001122:334455, v99, 3

NOTE: add command will be executed immediately.

save|cancel|next only applies to existing entry.

add|save|cancel|next :

- To delete an entry, use the index number for the specific static bridge address, the column letter **b** (the column letter for **Static Status**), an equal sign (=), and a **2** (the value for **Delete**).

For example, to delete the first address in the table, you would enter a **1** (the static bridge address **Index** number), a **b** (the column letter for **Static Status**), an equal sign (=), and the number **2** (the value for **Delete**), as shown:

1b=2

- Press **<return>** to complete the operation.
- Type **save** at the **fc** command prompt to save the changes. The **Static Status** will change to **Invalid**. Once you exit the **fc** command, the Static Bridge Address is removed from the table.

Displaying Static Bridge Addresses

You can view static bridge address information by entering the **fs** command. To display the information, enter the **fs** command as follows:

```
fs <group number>
```

where **<group number>** is the number of the group for which you want to view static bridge MAC addresses. For example, to view MAC addresses for Group 1, you would enter the following:

```
fs 1
```

This command will display a table similar to the following:

Bridge Static Address Summary for Group 1 (Default GROUP (#1))

MAC Address	Slot/Intf/Service/Inst	Static Status
002A3113:0012EA	3/ 1/ Brg/ 1	permanent

As a variation of this command, you can enter the **fs** command at the system prompt with no group number. This will allow you to view the static bridge addresses on the currently selected group. For information on selecting a group, see *Selecting a Default Group* on page 22-7.

The descriptions for the variables in the table displayed with the **fs** command are the same as those in the table displayed with the **fc** command. For details on these variables, see *Configuring a Static Bridge Address* on page 22-10.

Displaying Bridge Port Statistics

You can display statistics on bridge ports with the **bps** command. To view bridge port statistics enter the **bps** command as follows:

```
bps <group number>
```

where **<group number>** is the number of the group for which you want to view bridge port statistics. For example, to view statistics for Group 1, you would enter the following:

```
bps 1
```

This command will display a table similar to the following:

Frames discarded due to full Forwarding Database:0

Port Statistics for Group 1

Slot/Intf Service/Inst	Frames In	Frames Out	In Frames Discards	MTU Exceeded Discards	Delay Exceeded Discards	Flood Limit Discards
=====	=====	=====	=====	=====	=====	=====
2/ 1/ Brg/ 1	0	0	0	0	0	0
2/ 2/ Brg/ 1	0	0	0	0	0	0
3/ 1/ Brg/ 1	3354	85	0	0	0	0
3/ 2/ Brg/ 1	0	0	0	0	0	0
3/ 3/ Brg/ 1	0	0	0	0	0	0
3/ 4/ Brg/ 1	0	0	0	0	0	0
3/ 5/ Brg/ 1	0	0	0	0	0	0
3/ 6/ Brg/ 1	0	0	0	0	0	0
3/ 7/ Brg/ 1	0	0	0	0	0	0
3/ 8/ Brg/ 1	0	0	0	0	0	0
/VLAN/Bridge %						

As a variation on this command, you can enter **bps** at the prompt without a group number. This will display the port statistics for the currently selected group. For information on selecting a group, see *Selecting a Default Group* on page 22-7.

Field descriptions

The following section describes the fields displayed in the above table.

Frames discarded to full Forwarding Database. The number of frames that were not transmitted because the forwarding database is full. The forwarding database holds all known MAC address for this bridge and is used to learn the next hop MAC address for the packet(s) in question.

Slot/Intf/Service/Inst. The slot number (**SI**), interface (port) number (**Intf**), type of service (**Service**), and service instance (**Inst**). For example, a bridge service on port 1 of slot 3 would be:

3/1/Brg/1

Services provide connection options for switches in a LAN, between LANs, or in a WAN. Other possible services include trunking, routing, and LANE. It is possible to have more than one instance of a service if there are more than one connections on a single port.

Frames In. The number of frames received on the associated port.

Frames Out. The number of frames sent on the associated port.

In Frames Discards. The number of received frames discarded due to error.

MTU Exceeded Discards. The number of frames that were discarded because they exceeded the Maximum Transmission Unit (MTU) size. The MTU is set to the default of the media type (Ethernet, Token Ring, etc.) and is not configurable.

Delay Exceeded Discards. Frames that were delayed, usually due to collisions, but that were ultimately transmitted.

Flood Limit Discards. The number of frames that were discarded because they exceeded the flood limit set for the port or the group in which this port is a member. This flood limit is set with the **flc** command for groups or the **modvp** command for ports. For more information on setting flood limits, see *Setting Flood Limits* on page 22-21 for the **flc** command. For details on using the **modvp** command, see Chapter 24, “Managing Groups and Ports.”

Displaying Media Access Control (MAC) Information for a Specific MAC address

Media Access Control (MAC) information for the switch can be examined by using the **macinfo** command. You can view specific MAC address information, or choose a slot and view all MAC addresses associated with the selected slot.

To view MAC information for a specific address:

1. Enter **macinfo** at the system prompt and press **<return>**.
2. You will be prompted with the following message:

Enter MAC address ([XXYYZZ:AABBCC] or return for none):

Enter the MAC address you are interested in viewing, and press **<return>**.

3. You will be prompted with the following message:

Is this MAC in Canonical or Non-Canonical form (C or N) [C]:

Enter **c** for Canonical or **n** for Non-Canonical (the default is at the end of the prompt in brackets) and press **<return>**. A table similar to the following is shown:

Slot/Intf/Srvc/Inst	Group ID	CAM Index	Set by	MAC Type	Last Seen	Exp Timer	ATM VCI	Protocol
3/ 1/ Brg/ 1	1	0346	TB	ETH	11	15		

Field Descriptions

The following section explains the fields displayed using the **macinfo** command that are not previously explained in other sections.

Set by. This field lists what type of bridging was used to learn this MAC address. There are two possibilities:

- TB** This MAC address was learned using Transparent Bridging.
- SR** This MAC address was learned using Source Routing.

MAC Type. The media type of this MAC address. There are two possibilities:

- E** Ethernet
- F** FDDI
- T** Token Ring

Protocol. If Group Mobility is enabled, this field will list the type of packet encapsulation used when this MAC address was learned. For additional information on Group Mobility, see Chapter 24, “Managing Groups and Ports.”

Displaying Media Access Control (MAC) Information for all MAC addresses

Media Access Control (MAC) information for the switch can be examined by using the **macinfo** command. You can view all MAC addresses associated with the selected slot.

To view MAC information for all addresses:

1. Enter **macinfo** at the system prompt and press **<return>**. You will be prompted with the following message:

Enter MAC address ([XXYYZZ:AABBCC] or return for none):

2. Press **<return>**. You will be prompted with the following message:

Enter Slot Number (1-3):

Enter the slot number for the slot for which you are interested in viewing MAC addresses. The possible options are displayed on the right in parenthesis. A screen similar to the following is shown:

```
Total number of MAC addresses learned for VLAN 2: 8
```

Sl/If/Srvcln	MAC Address	Non-Canonical MAC Address	Group T	ID	CAM Indx	S	Last Seen	Exp Timer
3/1/ Brg/ 1	0020DA:A373B0	00045B:C5CE0D	E	2	305A	T	11	300
3/1/ Brg/ 1	0020DA:8656F0	00045B:616A0F	E	2	3060	T	11	300
3/1/ Brg/ 1	00045B:ED48C0	00045B:2251A1	E	2	3080	T	29	300
3/1/ Brg/ 1	000077:8DDBB9	00045B:65EE22	E	2	3010	T	29	300
3/1/ Brg/ 1	000039:F5520C	0009E4:3ED444	E	2	300E	T	35	300
3/1/ Brg/ 1	009027:17F7EB	00045B:2D43EF	E	2	3018	T	59	300
3/1/ Brg/ 1	0020DA:0C41E5	00045B:ED48C0	E	2	3078	T	26	300
3/1/ Brg/ 1	0020DA:9645A1	0000EE:B1DB9B	E	2	304E	T	18	300

Descriptions of the fields displayed with the **macinfo** command are identical to those displayed using the **fw** command. See *Displaying Bridge Forwarding Table* on page 22-8 for more information.

Display Statistics of Bridge MAC Addresses

The **macstat** command allows you to view a list of MAC address statistics for this switch on a slot-by-slot basis. To view MAC address statistics, enter the **macstat** command at the system prompt as shown:

macstat <slot>

where **<slot>** is the slot number on the switch for which you want to see statistics. For example, to view statistics for MAC addresses on slot 3, you would enter:

macstat 3

A table similar to the following is shown:

Slot	Discarded	Aged	Learned	in CAM
3	0	4	7	37

As a variation of this command, you can enter **macstat** at the prompt with no slot specified. This will display the statistics for all slots in the switch.

Field Descriptions

The following section describes the fields displayed using the **macstat** command.

Slot. The slot number of the switch to which the MAC address statistics apply.

Discarded. The number of MAC addresses that have been discarded on this slot due to the CAM being full.

Aged. The number of MAC addresses that have exceeded the age limit and been removed from the CAM by this slot.

Learned. The number of MAC address that have been learned on this slot.

in CAM. The total number of MAC addresses currently stored in the Content-Addressable Memory (CAM) of this module.

Clear Statistics of Bridge MAC Addresses

MAC address statistics for a slot can be cleared using the **macclrstat** command. To clear statistics, enter the **macclrstat** command at the system prompt as shown:

```
macclrstat <slot>
```

where **<slot>** is the slot number of the switch for which you want to clear MAC address statistics. For example, to clear statistics for slot 3, you would enter:

```
macclrstat 3
```

Once you have enter the command, a message appears to confirm the action.

As a variation of this command, you can enter **macclrstat** without specifying a slot. This will clear MAC statistics for all slots.

Display Remote Trunking Stations

The **rts** command displays a table of the remote trunking stations learned by this switch. A remote trunking station is a switch that has set up a trunking service to convey media through a network. Trunking services allow for media to be masked so that it appears to be a different type (for example, trunking ethernet over an ATM backbone). To display the remote trunking stations this switch has learned, follow these steps:

1. Enter the **rts** command as shown

```
rts <groupNumber>
```

where **<groupNumber>** is the number of the group on the local switch for which you want to view known trunking stations. For example, to view remote trunking stations for Group 1, you would enter the following:

```
rts 1
```

As a variation of this command, you can enter the **rts** command without a group number. This will show all the remote trunking stations for all groups in this switch.

- The following prompt is shown:

Enter service's Slot/Station (return for all services):

Enter the slot and station (port) number for the local switch for which you wish to view remote trunking services. For example, to list the trunking station at port 1 of slot 3, you would enter:

3/1

If you do not enter a specific slot and station, the system automatically sends information on all services for the remote trunking stations associated with this group.

- Once you have entered a slot and station, a table similar to the following is shown:

Remote Trunking Stations		
Slot/Station	Group ID	Remote MAC
=====	=====	=====
3/ 1	1	0020DA:022061
3/ 1	1	0020DA:05EAD1

Field Descriptions

The following sections describes the fields displayed by the **rts** command.

Slot/Station. The slot number and station (port) number associated with the remote trunking station.

Group ID. The group number of the switch that is associated with this remote trunking station.

Remote MAC. The Media Access Control address of the remote trunking service.

View the Domain Bridge Mapping Table

The **dbrmap** command allows you to display the mapping between a packet's destination MAC address and the remote Domain Bridge behind which it originated. To view this table:

- Enter the **dbrmap** command as shown:

dbrmap <groupNumber>

where **<groupNumber>** is the number of the group for which you want to see domain mappings of MAC addresses. For example, to view the mapping table for group 2, you would enter:

dbrmap 2

As a variation of this command, you can enter the **dbrmap** command without specifying a group. This will display mapping information for all groups on this switch.

- A prompt asking for a canonical MAC address is displayed, as shown:

Enter canonical MAC address ([XYZZ:AABBCC] or return to display everything):

Enter the MAC address you want to see the Domain Mapping for, or press **<return>** without entering a MAC address to see the mappings for all MAC addresses associated with this group.

3. A screen similar to the following is shown:

DOMAIN BRIDGE MAPPING				
Group 2				
Destination MAC	Group ID	Age	Slot / Intf	Domain MAC
00:20:da:7d:ef:44	2	14	8 / 1	00:20:da:6c:fb:85
00:20:da:7d:ef:45	2	120	8 / 1	00:20:da:6c:fb:85
00:20:da:7d:ef:46	2	220	8 / 1	00:20:da:6c:fb:86

Field Descriptions

The fields displayed by the **dbrmap** command are described below.

Destination MAC. The destination MAC address learned from a domain bridge port.

Group ID. The destination MAC's group number.

Age. The time, in seconds, since the destination MAC address was last seen.

Slot/Intf. The slot and interface number on this switch where the destination MAC address was learned.

Domain MAC. The remote domain MAC address behind which this destination MAC address was learned.

Setting Flood Limits

The flood limit is the number of bytes per second of flooded data that may be transmitted on a port on a group. This limit is a mechanism for controlling broadcast storms on the network.

The default flood limit for a port, regardless of the media type, is 192,000 bytes per second. You can change this default by configuring the flood limit on a per port or a per Group basis.

The **modvp** command (described in Chapter 24, “Managing Groups and Ports”) allows you to set the flood limit on a per port basis. The **flc** command (described in the following section) allows you to set the flood limit on a per Group basis. Configuring the flood limit for a Group is particularly useful when you need to disable flood limits for all ports in a single Group.

Setting Flood Limits for a Group

The **flc** command allows you to set flood limits for a Group. To set the flood limit for a Group

1. Enter the following at the system prompt follow these steps:

```
flc <groupNumber>
```

where **<groupNumber>** is the number of the group for which you are setting the flood limit. For example, to set the flood limit on Group 2 you would specify:

```
flc 2
```

As a variation of this command, you can enter the **dbbrmap** command without specifying a group. This will display mapping information for all groups on this switch.

The following prompt displays:

```
Enter flood limit override value (bytes/second) for Group 2 (192000):
```

2. Enter the flood limit for this Group and press **<Return>**.

◆ **Note** ◆

A value of negative one (-1) disables flood limits for the Group.

When new ports are added to a group, they will use the flood limit specified through **flc**. If a value has not been specified through **flc** for this Group, then the default port value (192000) is used.

◆ **Note** ◆

Flood limits set through **modvp** (set on a per-port basis) override the flood limit set through **flc**.

Displaying Group Flood Limits

The **fls** command allows you to view the current flood limits set for groups. The limits are set using the **flc** command. To display flood limits for all Groups, enter

```
fls <groupNumber>
```

where **<groupNumber>** is the number of the group for which you are viewing the flood limit. For example, to set the flood limit on Group 2 you would specify:

```
flc 2
```

A message similar to following is shown:

```
Flood Limit Override for Group 2(Group Name 1) is 190000 bytes per second.
```

A value will only be displayed for a Group on which **flc** has been used to set a flood limit.

As a variation of this command, you can enter **fls** at the system prompt without specifying a group number. This will return flood limit information for each group configured for this switch.

Configuring Spanning Tree

Spanning Tree is an algorithm developed to help prevent the occurrence of broadcast storms in a network. A packet can be broadcast multiple times in a network if the network is physically configured with loops.

If packets are broadcast to all ports (or flooded) in an attempt to deliver the data, networks with physical loops will rebroadcast packets repeatedly and cause a network to become severely congested. This congestion will adversely affect network performance.

Spanning Tree prevents broadcast storms by establishing a loop-free topology throughout the network. This is done by blocking ports in the physical topology that could result in flooded traffic being looped.

Both the IEEE and IBM versions of spanning tree are supported in the OmniSwitch and OmniSwitch/Router. The IBM Spanning Tree protocol is only supported by IBM Token Ring environments that make use of functional addresses for the transmission of Bridge Protocol Data Units (BPDUs). The following are the primary differences between the IEEE 802.1d and IBM Spanning Tree algorithms:

- The Hello BPDUs in IBM Spanning Tree are sent to the bridge functional address, X'C00000000100'. In the IEEE 802.1d Spanning Tree, they are sent to the Group address X'800143000000'.
- The Port ID in IBM Spanning Tree consists of a ring identifier and a bridge number. In 802.1d, it consists of a port priority and port number.
- IBM Spanning Tree has no learning process. Therefore, a port can be in one of three states—blocking, listening, or forwarding.
- IBM Spanning Tree does not support the Topology Change Notification (TCN) protocol.
- When you enable IBM Spanning Tree, the switch automatically sets defaults for the maximum age, forward delay, and hello time. In the interests of screen consistency, it is possible to change these defaults with the UI. In IBM Spanning Tree specification, these values are fixed, and should remain at the set defaults.
- When you enable IBM Spanning Tree, some additional defaults are set:
 - All virtual ports attached to the group with a physical port speed of 4 or 16 Mb are set to use Functional Addresses rather than Group Addresses.
 - All virtual ports attached to the group with a physical port speed that is not 4 or 16 Mb are set to manual forwarding.
 - As other virtual ports are attached to the group, the above two rules are applied.

Virtual ports in a manual forwarding state do not participate in either the IEEE or IBM versions of spanning tree. Any IEEE Spanning Tree frame received on a port in a manual forwarding state is forwarded to all other virtual ports in the same group also in a manual forwarding state. This is done to prevent loops from occurring in the network topology that could arise from applying the second default condition automatically.

- IBM SRT bridges send an IEEE-style STE RIF over Token Ring networks. The OmniSwitch and OmniSwitch/Router do not support this frame, and any frame of this type received by the switch is discarded.
- The OmniSwitch and OmniSwitch/Router do not support using the same Functional Address (FA) for both data and spanning tree frames. The FA for IBM Spanning Tree is programmed into the MPM CAM, and all data frames with this FA are claimed by the MPM. Therefore, any data with the same FA as the IBM Spanning Tree FA will not be able to pass through the switch. There are two workarounds for this situation:
 - If you are *not* using IBM Spanning Tree and you want to prevent the specific FA from being programmed into the MPM CAM, then enter the command *faBpGrpDisable* into the MPM.cmd file, before the *cmInIt* command, with a value of 1.
 - If you are using IBM Spanning Tree and need the FA (0300 0000 0800), and you are using all Alcatel equipment (or other third party switch that allows you to change the IBM Spanning Tree FA), you can enter the command *faBpGrpOverride* into the MPM.cmd file with a new value for the lower 32-bit part of the address (0000 0800).

◆ **Note** ◆

If you change a group to IBM Spanning Tree, all non-Token Ring ports are put into manual forwarding state. Messages are displayed indicating these port state changes; in addition, SNMP traps are sent to indicate these changes. (Manual forwarding state is where the port is put into forwarding state and the Spanning Tree algorithm is disabled.) Token Ring ports will be set to use functional addresses.

The following sections provide specific information on using the spanning tree commands.

Configuring Spanning Tree Parameters

The **stc** command allows you to configure parameters for the spanning tree, and enable or disable the Fast Spanning Tree feature for a VLAN. To configure these parameters:

1. Enter the **stc** command as follows:

```
stc <groupNumber>
```

where **<groupNumber>** is the number of the group in the switch for which you are configuring spanning tree. For example, to configure spanning tree for Group 2, you would enter:

```
stc 2
```

2. The system shows you the current values and allows you to change them through a series of prompts, the first of which is shown below:

```
Spanning Tree Parameters for Group 2 (New GROUP (#2))
```

```
Spanning Tree is OFF for this Group, set to ON ? (y/n) :
```

Enter **y** to enable spanning tree or **n** to leave it disabled and press **<return>**. This field allows you to toggle spanning tree On or OFF by typing the appropriate response. Answering Yes (**y**) selects the option opposite the currently selected option.

◆ Important Note ◆

Remember to read the prompt carefully before responding. If spanning tree has already been activated for this group, this prompt will ask you if you would like to turn it *off*.

3. The following prompt is displayed asking whether you would like to use IEEE or IBM Spanning Tree:

```
IEEE spanning tree for this Group, set to IBM ? (y/n) :
```

Enter **n** to use IEEE Spanning Tree, or **y** to use IBM Spanning Tree, and press **<return>**. Select either the IEEE 802.1d Spanning Tree or IBM Spanning Tree. Answering Yes (**y**) changes the spanning tree type to the type not currently in use for this Group. The system automatically sets defaults for later **stc** prompts, such as **Bridge Hello Time** and **Bridge Max Age**, based on the spanning tree type you select here.

◆ Important Note ◆

Remember to read the prompt carefully before responding. If IEEE Spanning Tree is what you would like to use, the correct response to this prompt is *no*. A yes response changes it to IBM Spanning Tree.

- The following prompt is displayed asking whether you would like to use the Fast Spanning Tree feature:

Fast Spanning Tree is OFF for this Group, set to ON? (y/n) :

Enter **n** to leave Fast Spanning Tree disabled, or **y** to enable Fast Spanning Tree, and press **<return>**. Answering Yes (**y**) changes the setting of Fast Spanning Tree to the status not currently in use for this Group.

◆ Important Note ◆

Read the prompt carefully before responding. If Fast Spanning Tree is what you would like to use, the correct response to this prompt is *yes*. A *no* response leaves the Fast Spanning Tree feature disabled.

- The following prompt is shown allowing you to set the priority:

New Priority (0..65535) (current value is 32768[0x8000]) :

Enter the **Priority** value as a number between 0 and 65535, or press **<return>** to accept the default listed in parenthesis. A value of 0 is the highest priority. Bridge priority is utilized by the spanning tree algorithm to decide which bridge will be the root bridge. You can set the bridge priority by entering a decimal number from 0 to 65,535. 0 is the highest priority.

◆ Note ◆

To make sure that the proper negotiation occurs for the switch to become the Spanning Tree root bridge, always set the priority for the switch accordingly. Do not rely on MAC addresses to determine which switch becomes the root bridge.

- The following prompt is displayed allowing you to set the Bridge Hello Time:

New Bridge Hello Time (1..10 secs) (current value is 2) :

Enter the **Bridge Hello Time** as a number between 1 and 10, or press **<return>** to accept the default listed in parenthesis. The amount of time between the transmission of Configuration Bridge Protocol Data Units (BPDUs) on any designated port. Enter a value between 1 and 10 seconds. Shortening the time will make the protocol more robust, while lengthening the time lowers the overhead of the algorithm as the interval between transmission of configuration messages is larger.

- The following prompt is displayed allowing you to set the Bridge Maximum Age:

New Bridge Max Age (6..40 secs) (current value is 6) :

Enter the **Bridge Max Age Time** as a number between 6 and 40, or press **<return>** to accept the default listed in parenthesis. The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in seconds. Enter a value between 6 and 40 seconds. A smaller value causes Spanning Tree to reconfigure more often.

8. The following prompt is displayed allowing you to set the Bridge Forward Delay:

New Bridge Forward Delay (4..30 secs) (current value is 4) :

Enter the **Forward Delay Time** as a number between 4 and 30, or press **<return>** to accept the default listed in parenthesis. This time value controls how fast a port changes its spanning state when moving toward the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. This value is also used when a topology change has been detected and is underway to age out all dynamic entries in the Forwarding Database. Enter a value between 4 and 30 seconds. A value that is too small can cause temporary loops in the network due to data being forwarded before the reconfiguration message has reached all nodes on the network.

9. The following prompt is displayed allowing you to set the Ageing Time:

Ageing Time (10..1000000 sec) (current value is 300) :

Enter the **Ageing Time** as a number between 10 and 1000000, or press **<return>** to accept the default listed in parenthesis. The timeout period in seconds for aging out dynamically learned forwarding information. Enter a new Ageing Time between 10 and 1000000 seconds.

10. The following prompt is displayed allowing you to set the Auto-Tracker VLAN Ageing Time:

Auto-Tracker VLAN Ageing Time (10..1000000 sec) (current value is 1200) :

Enter the **Auto-Tracker VLAN Ageing Time** as a number between 10 and 1000000, or press **<return>** to accept the default listed in parenthesis. The length of time in seconds to remember which VLAN a port belonged to even after the port has been aged out of the Bridge Filtering Database. The MAC and port information are preserved for the set length of time. In the case of IPX it should be set to greater than the server Keep Alive Timer in order to prevent the server from losing communication with the station. The default is 1200 seconds.

11. The final prompt is displayed asking you if you would like to save the new parameters:

Save the new Spanning Tree Bridge parameters ? y/n :

Enter **y** to save the parameters, or **n** to discard them. If you chose to save the parameters, a confirmation message similar to the following is shown:

**Port 5/1 set to Forwarding!
Port 5/2 set to Forwarding!
Port 5/3 set to Forwarding!**

As a variation of this command you can enter the **stc** command without specifying a group. This will allow you to set up spanning tree for the previously selected group. For information on selecting a group see *Selecting a Default Group* on page 22-7.

Display Spanning Tree Bridge Parameters

The **sts** command allows you to display spanning tree bridge parameters. To display spanning tree parameters, enter the **sts** command as shown:

```
sts <groupNumber>
```

where **<groupNumber>** is the number of the group in the switch for which you want to view spanning tree bridge parameters. For example, to view parameters for Group 2, you would enter:

```
sts 2
```

A screen similar to the following is displayed:

```

Spanning Tree Parameters for Group 2 (New GROUP (#2))
Spanning Tree Status      :          ON
Fast Spanning Tree Status:          OFF
Bridge Protocol Use       :          IEE E 802.1D
Priority                   :          32768 (0x8000)
Bridge ID                  : 8000-0020DA:022860
Designated Root           : 8000-0020DA:022860
Cost to Root Bridge       :          0
Root Port                  :          None
Next Best Root Cost       :          0
Next Best Root Port       :          None
Hold Time                  :          1
Topology Changes          :          1
Last Topology Change      : 1 hours, 25 minutes, 54 seconds ago
Bridge Aging Timer        :          300

```

Current Parameters		Parameters system uses when attempt to become root	
Max Age	20 secs	System Max Age	20 secs
Forward Delay	15 sec	System Forward Delay	15 secs
Hello Time	2 secs	System Hello Time	2 secs

As a variation of this command, you can enter **sts** at the system prompt without specifying a group. This will display bridge parameters for the currently selected group. For information on selecting a group, see *Selecting a Default Group* on page 22-7.

Field Descriptions

The following sections describe the fields displayed using the **sts** command.

Spanning Tree Status. Spanning tree is either **ON** or **OFF**.

Fast Spanning Tree Status. Fast spanning tree is either **ON** or **OFF**.

Bridge Protocol Used. The bridge spanning tree protocol is set up through the **stc** command. This protocol can be IEEE 802.1D or IBM Spanning Tree. The type of spanning tree protocol used will affect other bridge parameters, such as **Maximum Age**, **Forwarding Delay**, and **Hello Time**. See *Configuring Spanning Tree Parameters* on page 22-25 for more information on the differences between IEEE and IBM Spanning Tree.

Priority. Bridge priority is utilized by the spanning tree algorithm to decide which bridge will be the root bridge. You can set the bridge priority by entering a decimal number from 0 to 65,535. Zero is the highest priority.

Bridge ID. The bridge identification number is a number created by concatenating the bridge **Priority** with its six-byte MAC address.

Designated Root. The bridge identifier of the root of the spanning tree as determined by the spanning tree protocol. It is created by concatenating the root bridge **Priority** with its six-byte MAC address.

Cost to Root Bridge. The cost of the path to the root bridge as seen from this bridge. Cost represents the distance of the group from the root bridge, in number of hops. If this is the root bridge, this number is 0.

Root Port. The slot number, port number, and service type of the root port. The root port is the bridge's preferred path to the root bridge.

Next Best Root Cost. The next-best available cost of the path to the root bridge as seen from this bridge. Cost represents the distance of the group from the root bridge, in number of hops. If this is the root bridge, this number is 0.

Next Best Root Port. The next-best available root port (slot number, port number, and service type). The root port is the bridge's preferred path to the root bridge.

Hold Time. This time value determines the interval length during which no more than two Configuration Bridge BPDUs shall be transmitted, in seconds.

Topology Changes. The total number of topology changes detected by this bridge since the management entity was last reset or initialized. Topology changes happen when spanning tree reconfigures to prevent logical loops from occurring.

Last Topology Change. The time since the last time a topology change was detected by the bridge entity.

Bridge Aging Timer. The timeout period in seconds for aging out dynamically learned forwarding information.

Max Age. The maximum age (in seconds) of spanning tree protocol information learned from the network on any port before it is discarded.

Forward Delay. This time value (in seconds) controls how fast a port changes its spanning tree state when moving toward the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. This value is also used when a topology change has been detected and is underway to age out all dynamic entries in the Forwarding Database.

Hello Time. The amount of time (in seconds) between the transmission of Configuration Bridge Protocol Data Units (BPDUs) on any port when it is the root of the spanning tree, or trying to become so.

Configuring Spanning Tree Port Parameters

The **stpc** commands allows you to configure port parameters (as opposed to bridge parameters) for spanning tree. To configure port parameters

1. Enter the **stpc** command as shown:

```
stpc <groupNumber>
```

where **<groupNumber>** is the number of the group in the switch for which you want to configure spanning tree port parameters. For example, to configure parameters for Group 1, you would enter:

```
stpc 1
```

As a variation of this command, you can enter the **stpc** command without specifying a group. This will allow you to configure the port parameters on the currently selected group. For information on how to select a group, see *Selecting a Default Group* on page 22-7.

A screen similar to the following is displayed:

Spanning Tree Port Configuration for Group 1 (Default GROUP (#1))

Index	Slot/Intf/Service/Inst	Port Priority (a)	Path Cost (b)	Enable Spanning Tree (c)	tx FA (d)	Manual Mode (e)
1	2/ 1/ Brg/ 1	128	10	y	NA	n
2	2/ 2/ Brg/ 1	128	10	y	NA	n
3	3/ 1/ Brg/ 1	128	10	y	NA	n
4	3/ 2/ Brg/ 1	128	10	y	NA	n
5	3/ 3/ Brg/ 1	128	10	y	NA	n
6	3/ 4/ Brg/ 1	128	10	y	NA	n
7	3/ 5/ Brg/ 1	128	10	y	NA	n
8	3/ 6/ Brg/ 1	128	10	y	NA	n
9	3/ 7/ Brg/ 1	128	10	y	NA	n
10	3/ 8/ Brg/ 1	128	10	y	NA	n
11	3/ 9/ Brg/ 1	128	10	y	NA	n
12	3/ 10/ Brg/ 1	128	10	y	NA	n
13	3/ 11/ Brg/ 1	128	10	y	NA	n
14	3/ 12/ Brg/ 1	128	10	y	NA	n
15	3/ 13/ Brg/ 1	128	10	y	NA	n
16	3/ 14/ Brg/ 1	128	10	y	NA	n

save|cancel|next|prev :

2. To modify a parameter, enter the index (row) number, column letter (a, b, c, d, or e), an equal sign (=), and then the new parameter, as follows.

```
<index><column>=<new parameter>
```

For example, if you wanted to enable transmit Functional Address (**tx FA** in column **d**) for the slot identified by **index 10**, then you would enter:

```
10d=y
```

Field Descriptions

The following section explains the fields displayed by the **stpc** command.

Index

A number assigned as an identifier for the port.

Slot/Intf/Service/Inst

The slot number (**Slot**), interface (port) number (**Intf**), type of service (**Service**), and service instance (**Inst**). For example, a bridge service on port 1 of slot 3 would be:

3/1/Brg/1

Services provide connection options for switches in a LAN, between LANs, or in a WAN. Other possible services include trunking, routing, and LANE. It is possible to have more than one instance of a service if there are more than one connections on a single port.

Port Priority

The value of the priority field contained in the first (in network byte order) octet of the (2 octet long) Port ID. This value allows you to specify a particular port as more favorable if the bridge has more than one port connected in a loop.

Path Cost

The contribution of this port to the path cost towards the spanning tree root bridge that includes this port. 802.1D-1990 recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN. Path cost is a measure of the distance of the listed port from the root bridge, in number of hops.

Enable Spanning Tree

Whether or not spanning tree is enabled, either **y** or **n**.

tx FA

Transmit Functional Address. Values are:

- | | |
|-----------|---|
| NA | Function Addresses are not applicable because this port is not using spanning tree. |
| y | Transmit Functional Address instead of normal Spanning Tree Multicast Address. |
| n | Transmit normal Spanning Tree Multicast Address. This is the default setting. |

Manual Mode

Allows you to manually set the state for each port (forwarding or blocking) or defer the port's state configuration to the spanning tree protocol, which will either be IEEE 802.1d or IBM. This column is especially helpful if you are using the IBM Spanning Tree protocol with non-Token Ring (e.g., FDDI or Ethernet) ports that do not support this IBM Spanning Tree. In this situation you can manually set those ports to a forwarding (or blocking) state since the IBM Spanning Tree protocol will not be able to control these ports. The possible settings for this column are:

- f** The port is in forwarding state and remains so unless you change it.
- b** The port is in blocking state and remains so unless you change it.
- n** The state of the port is determined by the IEEE 802.1d Spanning Tree protocol. This option is not recommended because it means this Group will have a hybrid spanning tree algorithm that mixes the IEEE 802.1d and IBM Spanning Tree.

Displaying Spanning Tree Port Parameters

The **stps** command allows you to view the current spanning tree port parameters. To view the port parameters, enter the **stps** command as shown:

```
stps <groupNumber>
```

where **<groupNumber>** is the number of the group in the switch for which you want to view spanning tree port parameters. For example, to view parameters for Group 1, you would enter:

```
stps 1
```

A screen similar to the following is shown:

Spanning Tree Port Summary for Group 1 (Default GROUP (#1))

Slot Intf	Service Inst	Pri	State	MAC	Path Cost	Desig Cost	Des Pt	Rt Pt	SwT Pt	Fw Tx	Root Bridge ID Desig BridgeID
3/1	Brg/1	128	FORWD	C473C4	10	10	No	Yes	No	0	0010-0020DA:81D5B0 8000-0020DA:0C41E1

As a variation to this command, you can enter **stps** at the system prompt without specifying a group number. This will allow you to view the port parameters on the currently selected group. For information on how to select a group, see *Selecting a Default Group* on page 22-7.

Field Descriptions

The following section explains the fields displayed by the **stps** command.

Slot/Intf. The slot and interface (port) number of the port.

Service/Inst. The service type and instance of the service connected to the port.

Pri. The value (from 0 to 256) of the priority of the port, 0 being the highest priority.

State. The port's current state as defined by application of the spanning tree protocol. This state controls what action a port takes on reception of a frame. The **State** values are:

Disabled	This port has been disabled.
Blocking	This port is not participating in transmitting data to prevent loops.
Listening	This port is preparing to transmit data, but is temporarily disabled to prevent loops.
Learning	This port is preparing to transmit data, but is temporarily disabled to prevent loops. This is different from Listening in that the port is acquiring data to facilitate data transmission.
Forwarding	This port is transmitting data.

Some of these values are not available if you are using IBM Spanning Tree. For information on the differences between IEEE and IBM Spanning Tree, see *Configuring Spanning Tree Parameters* on page 22-25.

Path Cost. The contribution of this port to the path cost towards the spanning tree root. The spanning tree root will include this port.

Desig Cost. The path cost to the designated port of the segment connected to this port. If this is the root bridge this value is 0.

Des Port. The unique port identifier of the bridge port believed to be the designated port for the LAN associated with the port.

Rt Pt. This field indicates if this port is the root port. The root port is the port that offers the lowest cost path to the root bridge.

Swt Pt. This field indicates if this port is in Optimized Switch Mode. Optimized Switch Mode is appropriate for dedicated connections to a single workstation or server. For more information, see Chapter 24, "Managing Groups and Ports."

FWD Transition. The number of times this port has changed from the Learning state to the Forwarding state.

Root Bridge ID. The bridge identification number of the root bridge.

Desig Bridge ID. The unique bridge identifier of the designated bridge for this port (LAN).

Configuring Fast Spanning Tree

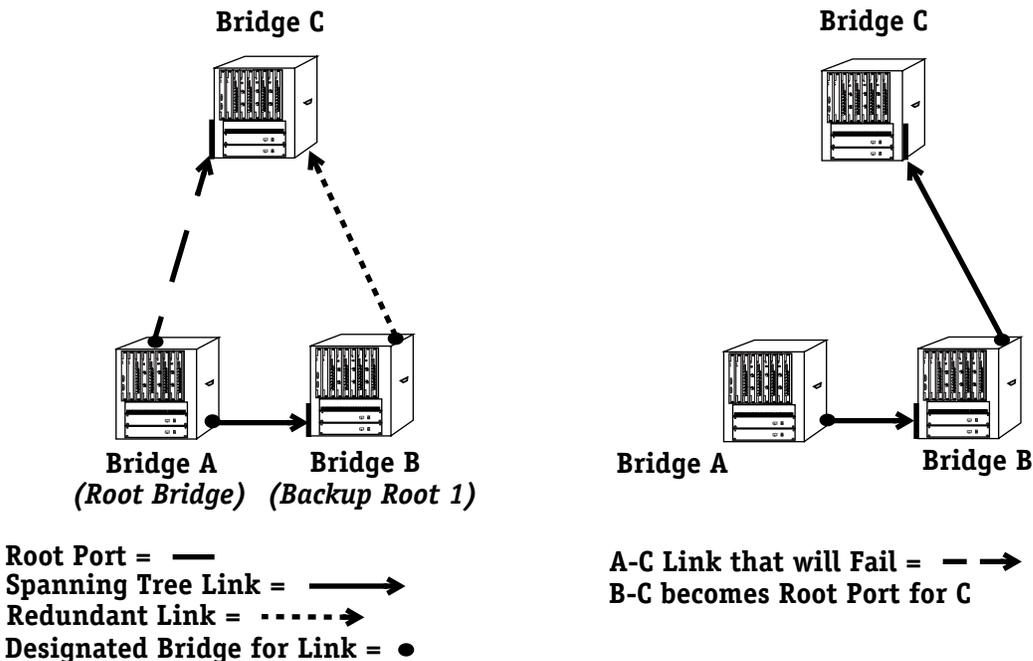
The Fast Spanning Tree (Rapid Reconfiguration) feature is designed to help provide an 802.1D standards-based method of quick recovery in the event of link, port and device failures in an Ethernet local area network. By automatically identifying and utilizing alternative secondary links, Fast Spanning Tree can rapidly converge backup connections between network devices within as little as 1 second. In addition, new Spanning Tree information can be processed faster.

If packets are broadcast to all ports (or flooded) in an attempt to deliver the data, networks with physical loops will rebroadcast packets repeatedly and cause a network to become severely congested. This congestion will adversely affect network performance.

While Spanning Tree prevents broadcast storms by blocking ports in the physical topology that could result in flooded traffic being looped, Fast Spanning Tree minimizes downtime by bringing these blocked secondary links into Forwarding mode as quickly as possible. If the Root Port is lost, an Alternate Port on the Bridge can be made the new Root Port, and placed into a Forwarding state immediately. The prior Root Port switches to a Listening state if it becomes a Designated Port; otherwise, it enters a Blocking state.

Similarly, any Designated Port on the Bridge can be made the new Root Port, and placed into a Forwarding state immediately. In this event, the existing (prior) Root Port changes to a Designated Port role, without a corresponding gain or loss of connectivity. A Backup Port can also be made the new Root Port and placed into Forwarding mode, resulting in the Designated Port assuming a Listening state.

The following diagram illustrates how a typical network connection can fail, such as the A-C Link shown below. Rapid Reconfiguration brings a blocked link - such as the B-C Link - into Forwarding state, helping achieve quick recovery from failure of networked devices.



Recovering from Linked Device Failure with Fast Spanning Tree

Truncating Tree Timing & Speedy Tree Protocol

Two additional enhancements are also included with the Fast Spanning Tree feature for improved performance: Truncating Tree Timing and Speedy Tree Protocol.

Truncating Tree Timing

Truncating Tree Timing allows Designated Ports attached to Point-to-Point links to change to Forwarding mode faster, by utilizing two extra bits in the Configuration BPDU for communication between neighboring bridges. This enhancement promotes quicker restoration of service between communicating stations and reduced flooding of traffic during relearning of station location information.

Speedy Tree Protocol

Speedy Tree Protocol significantly improves reconfiguration performance by allowing inferior information sent by the designated bridge for each LAN to be accepted, rather than timed out. Additionally, information previously received expires immediately on link failure. In both cases, spanning tree recomputation occurs, which can cause changes in both root and designated ports.

Configuring Truncating Tree Timing & Speedy Tree Protocol

Both Truncating Tree Timing and Speedy Tree Protocol are enabled by default. These features are configured by editing the following lines in the command file (**mpm.cmd**):

```
truncatingSt=1  
speedySt=1
```

To disable the Truncating Tree Timing feature, change the numeric entry for **truncatingSt** from **1** to **0**. (To re-enable the feature, change the numeric entry back to **1**.)

To disable the Speedy Tree Protocol feature, change the numeric entry for **speedySt** from **1** to **0**. (To re-enable the feature, change the numeric entry back to **1**.)

◆ Important Note ◆

Do not attempt to edit the command file (**mpm.cmd**) unless you have had significant experience working with files of this type. For additional information, see *Editing Text Files* in Chapter 11, “Managing Files.”

Displaying Fast Spanning Tree Port Parameters

The **fstps** command allows you to view the current Fast Spanning Tree port parameters on a selected group or VLAN. To view the port parameters, enter the **fstps** command as shown:

```
fstps <groupNumber>
```

where **<groupNumber>** is the number of the group in the switch for which you want to view Fast Spanning Tree port parameters. For example, to view parameters for Group 1, enter:

```
fstps 1
```

If Fast Spanning Tree is not enabled (default), a screen similar to the following will appear:

Fast Spanning Tree not enabled for Group 1 (Default GROUP (#1))

Slot Intf	Service		State	Role	Fwrds	Frwdr	FrgetRPs	PPs	Link Ups	Primary Port	
	Inst	Inst								Slot	Service Inst
8/3	Brg/1	FORWD	ROOT	0	0	0	0	0	2		

As a variation on this command, you can enter **fstps** at the system prompt without specifying a group number. This will allow you to view the port parameters on the currently selected group. For information on how to select a group, see *Selecting a Default Group* on page 22-7.

The fields displayed by the **fstps** command include.

Slot/Intf. The slot and interface (port) number of the port.

Service/Inst. The service type and instance of the service connected to the port.

State. The port's current state as defined by application of the fast spanning tree protocol. This state controls what action a port takes on reception of a frame. The **State** values include:

- DSABL** Disabled - The port has been disabled.
- BLOCK** Blocking - The port is not participating in transmitting data in order to prevent loops.
- LISTN** Listening - The port is preparing to transmit data, but is temporarily disabled in order to prevent loops. BPDU processing does occur, but no user data is being passed.
- LEARN** Learning - The port is preparing to transmit data, adding source MAC addresses to the bridging table, but incoming data frames are dropped.
- FORWD** Forwarding - The port is transmitting data. This state applies to Root Ports and Designated Ports.
- FRWDS** Forwards - The port is transmitting data. This state applies to Designated Ports, and monitors old root ports for a period equivalent to two times the Forward Delay Timer default time period (default = 15 seconds).
- FRWDR** Forwarder - The port is transmitting data. This state applies to Designated Ports, and monitors old root ports for a period equivalent to the Forward Delay Timer default time period (default = 15 seconds).
- FRGET** Forgetting - The port is discarding frames, and is not learning source addresses. This state applies to prior Designated Ports that are placed into an Alternate Role. Forgetting State minimizes potential denial of service due to information races during extensive reconfigurations.

Role. The port's current role as defined by application of the fast spanning tree protocol. The **Role** values include:

- DISABLED** The port has been disabled.
- ROOT** The Root Port on a Bridge has the best path to the Root Bridge, and connects the Bridge to the Root Bridge.
- DESIGNATED** The Designated Port on a Bridge provides an attached LAN the best path to the Root Bridge, and connects the LAN through the Bridge to the Root Bridge, forwarding frames between them. (A Designated Port can be in a Listening, Learning, Forwards, Forwarder, or Forwarding state.)
- ALTERNATE** The Alternate Port is connected to a LAN with another bridge functioning as the Designated Bridge. (An Alternate Port may be in either a Forgetting state or a Blocking state.)
- BACKUP** The Backup Port is connected to a LAN with another port on the same Bridge functioning as the Designated Port. (Backup Ports are always in a Blocking state.)

Frwds. This counter records each instance when the port is in the Forwards state.

Frwdr. This counter records each instance when the port is in the Forwarder state.

Frget. This counter records each instance when the port is in the Forgetting state.

RPs. This counter records each instance when the Root Port is retired.

PPs. This counter records each instance when the Primary Port is retired.

Link Ups. This counter records each instance when the port is linked up.

Primary Port Slot Intf. The slot and interface (port) number of the Primary Port.

Primary Port Service Inst. The service type and instance of the service connected to the Primary Port.

Enabling Fast Spanning Tree Port Parameters

The **actfstps** command allows you to activate Fast Spanning Tree port parameters on a selected group or VLAN. To enable Fast Spanning Tree, enter the **actfstps** command as shown:

```
actfstps <groupNumber>
```

where **<groupNumber>** is the number of the group in the switch for which you want to view Fast Spanning Tree port parameters. For example, to view parameters for Group 1, enter:

```
actfstps 1
```

If Fast Spanning Tree is not enabled (default), a screen similar to the following will appear:

```
Fast Spanning Tree disabled for Group 1 (Default GROUP (#1))
```

```
Enable 1/ Disable 2 Fast Spanning Tree/ Return nothing?
```

To enable the Fast Spanning Tree feature, enter **1** at the prompt. (If you press the Enter key without typing anything, the setting will not be changed.)

No confirmation message will appear. To view the Fast Spanning Tree Port Summary, enter **fstps** at the prompt. For details about the Fast Spanning Tree Port Summary, see *Displaying Fast Spanning Tree Port Parameters* on page 22-36.

◆ Important Notes ◆

To determine whether Fast Spanning Tree is enabled on a VLAN, enter **sts** at the prompt.

To enable Fast Spanning Tree on a VLAN, enter **stc** at the prompt, then follow the onscreen instructions to enable it. For more details, see *Configuring Spanning Tree Parameters* on page 22-25.

Disabling Fast Spanning Tree Port Parameters

The **actfstps** command allows you to disable Fast Spanning Tree port parameters on a selected group or VLAN. To disable Fast Spanning Tree, enter the **actfstps** command as shown:

```
actfstps <groupNumber>
```

where **<groupNumber>** is the number of the group in the switch for which you want to view Fast Spanning Tree port parameters. For example, to view parameters for Group 1, enter:

```
actfstps 1
```

If Fast Spanning Tree is enabled, a screen similar to the following will appear:

```
Fast Spanning Tree Port Summary for Group 1 (Default GROUP (#1))
```

```
Enable 1/ Disable 2 Fast Spanning Tree/ Return nothing?
```

To disable the Fast Spanning Tree feature, enter **2** at the prompt. (If you press the Enter key without typing anything, the setting will not be changed.)

No confirmation message will appear. To view the Fast Spanning Tree Port Summary, enter **fstps** at the prompt. For details about the Fast Spanning Tree Port Summary, see *Displaying Fast Spanning Tree Port Parameters* on page 22-36.

◆ Important Notes ◆

To determine whether Fast Spanning Tree is enabled on a VLAN, enter **sts** at the prompt.

To disable Fast Spanning Tree on a VLAN, enter **stc** at the prompt, then follow the onscreen instructions to disable it. For more details, see *Configuring Spanning Tree Parameters* on page 22-25.

Configuring Source Routing

The **srs** and **src** commands allow you to display and configure the source routing parameters for the selected group. For information on these commands, see Chapter 21, “Managing Token Ring Modules.”

SAP Filtering

The Service Advertising Protocol (SAP) filter is a method for allowing the user to decide what type of source routed packets are allowed to be transmitted out of the switch. When the filters are configured, they examine the DSAP (destination) and SSAP (source) fields in an outgoing packet, compare them to the filter values to see if they match, and then either allows or blocks packet transmission.

There are two types of filters that can be configured: a “permit” filter and a “deny” filter. If a packet matches the value in a deny filter, and the value is not 0, then the packet is discarded. If a permit filter is configured, and a packet does *not* match the filter value, then the packet is discarded. Only two of each type of filter can be configured.

To use this feature, it must first be enabled, then configured. Once a filter is enabled and configured, it can be viewed as part of the source routing statistics. These procedures are covered in the following sections:

- For information on enabling the SAP filter see *Enabling SAP Filtering* on page 22-40.
- For information on configuring SAP filters, see *Configuring SAP Filtering* on page 22-41.
- For information on viewing SAP filters, see *Viewing SAP Filtering* on page 22-42.

Enabling SAP Filtering

To use the **srsf** command to enable SAP filtering, follow the steps below:

1. Enter the **srsf** command at the system prompt.
2. The following message is displayed:

SAP Filter support is OFF, set it to ON? (n) :

Enter **y** and press **<return>**.

3. Another message is displayed confirming the activation of the SAP filtering feature:

SAP Filter Support is now “ON”

Disabling SAP filtering

To disable the SAP feature, use the **srsf** command as shown:

1. Enter the **srsf** at the system prompt.
2. The following message is displayed:

SAP Filter support is ON, set it to OFF? (n) :

Enter **y** and press **<return>**.

3. The following message is displayed:

Remove all SAP Filter values? (n) :

Enter a **y** to remove the configured filters, or an **n** to keep configured filters, and press **<return>**. See *Configuring SAP Filtering* on page 22-41 for information on how to set up a SAP filter.

4. Another message is displayed confirming the deactivation of the SAP filtering feature:

SAP Filter Support is now "OFF"

Configuring SAP Filtering

Once SAP filtering is activated, it is necessary to configure the filter value. This value is compared to the value of the packets DSAP and SSAP fields. Filters consist of 4 alphanumeric bits, 2 for the DSAP and 2 for SSAP. After enabling SAP filtering, another column is added to the **src** command, and four prompts are added to the ring configuration options.

To configure the filter value:

1. Enter the **src** command at the system prompt. The following screen is displayed:

Source Routing Parameters for Group 1 (Default GROUP (#1))

	Slot	Type/ Inst/Srvc	Ring Number	Bridge Number	Largest frame	HopCnt In Out	Port Type	Block ARE	SAP Filter
1.	2/1	Brg/ 1/ na	1 (0x001)	10 (0xA)	590	6 6	SRT	n	
2.	3/1	Brg/ 1/ na (V)	2 (0x002)	10 (0xA)	4472	7 7	SRT	n	
3.	3/2	Brg/ 1/ na	4 (0x004)	10 (0xA)	4472	7 7	SRT	n	
4.	3/3	Brg/ 1/ na	5 (0x005)	10 (0xA)	4472	6 6	SRT	n	
5.	3/4	Brg/ 1/ na	3 (0x003)	10 (0xA)	4472	7 7	SRT	n	
6.	3/5	Brg/ 1/ na (V)	2 (0x002)	10 (0xA)	4472	7 7	SRT	n	
7.	3/6	Brg/ 1/ na (V)	3 (0x003)	10 (0xA)	4472	7 7	SRT	n	

Enter index of the entry to configure (e.g. 1) <RETURN> to exit :

2. Enter the index number (on the far left) for the ring you want to filter.
3. Several prompts for configuring the ring are displayed. Follow the prompts and enter the values required, or accept the current values if the ring is already configured. (See Chapter 21, "Managing Token Ring Modules" for more information on how to configure token rings.) The following prompt is shown:

Output SAP Deny Filter 1 (0000):

Enter the SAP value that the first deny filter should screen. Any packet matching this filter will be rejected. Excepting the default of **0000** is the same as not having a filter.

4. Press **<return>**. The second deny filter prompt is displayed:

Output SAP Deny Filter 2 (0000):

Enter the SAP value that the first deny filter should screen. Any packet matching this filter will be rejected. Excepting the default of **0000** is the same as not having a filter.

5. Press **<return>**. The first permit filter prompt is displayed:

Output SAP Permit Filter 1 (0000):

Enter the SAP value that the first permit filter should screen. Any packet *not* matching this filter will be rejected. Excepting the default of **0000** is the same as not having a filter.

6. Press **<return>**. The second permit filter prompt is displayed:

Output SAP Permit Filter 2 (0000):

Enter the SAP value that the first permit filter should screen. Any packet *not* matching this filter will be rejected. Excepting the default of **0000** is the same as not having a filter.

7. Press **<return>**. A final message asking to save the new configuration is displayed:

Save the new configuration? (y/n) :

Enter a **y** to save the configuration, or an **n** to cancel the operation.

Viewing SAP Filtering

To see how many SAP filters are configured for a specific ring, enter the **srs** command at the system prompt. A screen similar to the following appears:

Source Routing Parameters for Group 1 (Default GROUP (#1))

	Slot	Type/ Intf	Type/ Inst/Srvc	Ring Number	Bridge Number	Largest frame	HopCnt In	HopCnt Out	Port Type	Block ARE	SAP Filter
1.	2/1	Brg/	1/ na	1 (0x001)	10 (0xA)	590	6	6	SRT	n	1
2.	3/1	Brg/	1/ na (V)	2 (0x002)	10 (0xA)	4472	7	7	SRT	n	2
3.	3/2	Brg/	1/ na	4 (0x004)	10 (0xA)	4472	7	7	SRT	n	
4.	3/3	Brg/	1/ na	5 (0x005)	10 (0xA)	4472	6	6	SRT	n	
5.	3/4	Brg/	1/ na	3 (0x003)	10 (0xA)	4472	7	7	SRT	n	
6.	3/5	Brg/	1/ na (V)	2 (0x002)	10 (0xA)	4472	7	7	SRT	n	
7.	3/6	Brg/	1/ na (V)	3 (0x003)	10 (0xA)	4472	7	7	SRT	n	

Enter index of the entry to configure (e.g. 1) **<RETURN>** to exit :

The last column (**SAP Filter**) lists how many SAP filters are in place for the ring. See *Configuring SAP Filtering* on page 22-41 for information on configuring the SAP filter.

Configuring Source Route to Transparent Bridging

In order to provide switching between source-routed token ring networks supporting the IBM Spanning Tree, and transparently bridged networks (primarily Ethernet supporting 802.1d Spanning Tree), commands have been provided in the bridging menu to enable Source Route to Transparent Bridging (SRTB) on a configured group basis.

It is important not to confuse SRTB with source-route transparent (SRT) bridging. SRT bridging is the defined method for bridging on source-routed networks. In SRT bridging, all bridges run the 802.1d Spanning Tree. SRT bridges have the ability to forward a frame based on source-routing information if a Routing Information Field (RIF) is present. Frames without a RIF are bridged transparently. SRT does not provide the ability to switch between a pure source-routed network and a transparent network.

SRTB allows source-routed token ring networks and transparently bridged networks to exist in the same group, and supports connectivity between end systems on the token ring network and the end systems on the transparently bridged network.

The SRTB functions in the following network environments:

- Between token ring and Ethernet networks.
- Between token ring networks and Ethernet LAN emulation (LANE).
- Between token ring LAN emulation and Ethernet networks.

◆ **Note** ◆

Ethernet networks include 10Mbit, 10/100 MB, and Gigabit networks.

Enabling SRTB for a Group

The **srtbcfg** command allows you to display configured groups and the status of SRTB (either **on** or **off**), and to enable or disable SRTB for a specific group. To display groups and the status of SRTB:

1. Enter the **srtbcfg** command at the system prompt, as shown

```
srtbcfg
```

A screen similar to the following is displayed:

```
Group 1: SRTB is OFF
Group 2: SRTB is ON
      Default Explorer: STE Ethernet Ring ID: 291(x123)
Group 3: SRTB is ON
      Default Explorer: ARE Ethernet Ring ID: 561(x231)
```

```
/VLAN SRTB>
```

2. To enable SRTB for a group, enter the **srtbcfg** command at the system prompt, as shown:

```
srtbcfg <groupNumber>
```

where **<groupNumber>** is the number of the group for which SRTB is to be enabled. For example, to enable SRTB for Group 1, you would enter the following:

```
srtbcfg 1
```

3. Once you have entered the command, a screen similar to the following is displayed:

```
Group 1: SRTB is OFF
      Would you like to turn on SRTB ? (n) :
```

Enter **y** to enable SRTB for this group.

4. Once you have enabled SRTB, the following prompt appears:

```
Enter Ring ID for Ethernet segment(s) (0 - 0x0)? :
```

Create a ring ID for the Ethernet segment assigned to this group. This number can be in decimal or hexadecimal form, but it must be unique. For example, if you have a token ring segment with a ring ID of 2, then you could not assign the number 2 to an Ethernet ring ID.

5. Once you have assigned an Ethernet token ID, the following prompt appears:

```
Send Multicast/unknown frames as STE or ARE ? (STE) :
```

Choose to employ Spanning Tree Explorer (STE) frames or All Route Explorer (ARE) frames by entering **ste** or **are**. Explorer frames are sent to learn MAC addresses when there is no record in the RIF table. ARE frames ignore port blocks set up by spanning tree to avoid loops, while STE frames adhere to the spanning tree configuration. The default is **STE**.

6. Once you have selected the frame type, you are returned to the menu prompt. By reentering the **srtbcfg** command as you did in step 1, you can now see that SRTB has been activated for group 1, as shown:

```
Group 1: SRTB is ON
Default Explorer: STE Ethernet Ring ID: 871(x321)
Group 2: SRTB is ON
Default Explorer: STE Ethernet Ring ID: 291(x123)
Group 3: SRTB is ON
Default Explorer: ARE Ethernet Ring ID: 561(x231)
```

The ring ID and default explorer frame are shown as well.

Disabling SRTB for a Group

To turn SRTB off for a group, enter the **srtbcfg** command as shown

```
srtbcfg <groupNumber>
```

where **<groupNumber>** is the number of the group for which you want to disable SRTB. For example, to disable SRTB on Group 3, you would enter:

```
srtbcfg 3
```

The following prompt appears:

```
Group 3: SRTB is ON
Default Explorer: ARE Ethernet Ring ID: 561(x231)
Would you like to turn off SRTB ? (n) :
```

Enter **y** to disable SRTB. Once you have done this you are returned to the system prompt. To view the changes to the group, enter the **srtbcfg** command to display a screen similar to the following:

```
Group 1: SRTB is ON
Default Explorer: STE Ethernet Ring ID: 871(x321)
Group 2: SRTB is ON
Default Explorer: STE Ethernet Ring ID: 291(x123)
Group 3: SRTB is OFF
```

Viewing the RIF Table

A Routing Information Field (RIF) is stored for each MAC address learned on a token ring port. One RIF is stored for each MAC address. The maximum size of each RIF is 32 bytes (long enough to traverse 15 bridge hops)

Once a RIF is learned for a MAC address, it is maintained until the MAC address is aged out of the CAM. You can view a list of RIFs using the **srtbrif** command. To view the RIF table follow these steps:

1. Enter the **srtbrif** command at the menu prompt. The following prompt is displayed:

Enter MAC address ([XXYYZZ:AABBCC] or return for none) :

Enter the MAC address for which you want to see the RIF and press **<return>**, or enter a **<return>** without a MAC address to list all RIFs.

2. Once you enter a MAC address (or **<return>**), the following prompt appears:

Enter Group ID (return for all Group) :

Enter a group ID and press **<return>**, or enter a **<return>** without a group ID to list the RIFs for all groups.

3. Once you enter the group ID (or **<return>**), a screen similar to the following appears:

Port	Group ID	Non-Canonical MAC Address	CAM Indx	Len	RIF
4/ 1/Brg/ 1	2	10009E:4B7DE1	010E	6	0610:1231:0010:

Field Descriptions

The following section describes the fields shown using the **srtbrif** command.

Port. This field lists the slot, port number, service type, and instance number for where the RIF was learned for this MAC address.

Group ID. The group number with which this RIF is associated.

Non-Canonical MAC Address. The MAC address for this RIF. It is shown in non-canonical form.

CAM Indx. The index number in the Content-Addressable Memory (CAM), where the MAC addresses are stored, in hexadecimal form.

Len. The length of the RIF packet, in bytes.

RIF. The RIF address for this MAC address.

Clearing the RIF Table

If there is a topology change in your network, you most likely will need to clear one or more RIFs from the table so that SRTB can relearn them. You can clear specific entries for MAC addresses in the RIF table, or flush the entire table with the **srtbclrrif** command. To clear an entry in the RIF table:

1. Enter the **srtbclrrif** command at the system prompt. The following prompt appears:

Enter MAC address ([000000:000036] or return for none) :

Enter the MAC address for the RIF entry you wish to clear in canonical or non-canonical form, and press **<return>**. If you enter **<return>** without a MAC address, you will flush the entire table of RIF entries.

2. Once you have entered the MAC address, the following prompt appears:

Is this MAC in Canonical or Non-Canonical (C or N) [N] :

If you entered the MAC address in canonical form, enter a **c**. If you entered the MAC address in non-canonical form, enter an **n**. If you respond incorrectly, the RIF entry will not be deleted.

3. Once you entered the distinction of canonical or non-canonical, the following prompt appears to verify the deletion on the RIF entry:

RIF clear successfully!

23 Configuring Frame Translations

Any-to-Any Switching

Because the OmniSwitch is a LAN switch that carries frames from multiple media types on its backplane fabric, it offers the facility to switch frames from any media to any other media. For example, an Ethernet frame onto a Token Ring. This feature is referred to as Any to Any Switching.

Normally, the only way for data to get from one media type to another is via routing. Routing removes the media specific headers of a received frame and prepends the new media specific aspects of the destination port before the frame is retransmitted on the new media. In this process the frame itself is not transmitted from one media to another, only the information within it. This process involves heavy computation, requiring table lookups to guide the header deletion/creation and additional router-to-router protocols to set up and maintain these tables.

Routing is not restricted, nor even primarily intended, for moving data between unlike media but instead seeks to break networks down into a number of smaller networks, each of which is a broadcast domain. Historically, networks based on different technologies and media naturally form distinct broadcast domains.

The advent of LAN switching has rewritten these rules. Today, the formation of broadcast domains and the allocation of devices to them is driven by logical requirements such as Virtual LANs and LAN switches. They seek to break free of topology and network constraints imposed by mere media differences.

Within this new paradigm there is still a place for routing. The installed base of clients and servers must communicate by established routing protocols but the broadcast domains handled by a router need not now consist of a single media.

To support this paradigm a LAN switch must “transform” a frame on one media into a frame on the other media in such a way that the frame is still acceptable to the routing protocols. Unfortunately, the requirements for this “transformation” algorithm are specific to the various protocols that currently exist. There is no single, simple algorithm that will allow the frame to be switched between media transparently to the higher level protocols and frame formats. This leads to a fairly complex set of configuration options and limitations on the applicability of the any to any switching features.

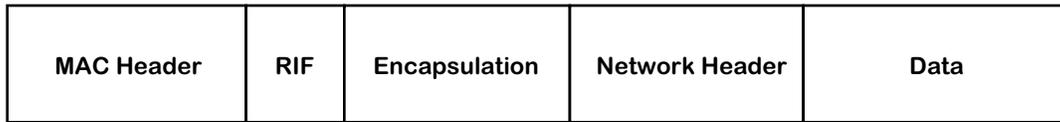
In order to understand why these options and limitations arise and to better understand the configuration options available, it is advisable to understand as background the theory of operation of any to any switching. This material is also required if you are trying to determine the applicability of any to any switching to a protocol not described in the reference material.

◆ Important Note ◆

Beginning with Release 4.4, FDDI is no longer supported.

Translating the Frame

In order to discuss these issues independent of particular media and protocols, consider that every frame, of any protocol, on any media, consists of the following parts.



The Essential Parts of Frame

MAC Header

Consists of a source and destination address specifying the transmitting station in the broadcast domain and the intended recipient(s), as well as other media specific fields. For example, AC and FC fields in Token Ring, FC in FDDI, etc.

RIF (Router Information Field)

If present, it is defined by the source routing standard and is only found on Token Ring and FDDI media.

Encapsulation

Defined by the various standards for the media, many of which reference common standards. For example, on Ethernet media, as defined by Ethernet II, this is a 16 bit type field. On Ethernet media, as defined by the IEEE 802.3 committee, this is a length field together with any encapsulation defined by the IEEE 802.2 Logical Link Control (LLC) committee. On Token Ring and FDDI, it is any encapsulation defined by the IEEE 802.2 LLC committee.

Network Header

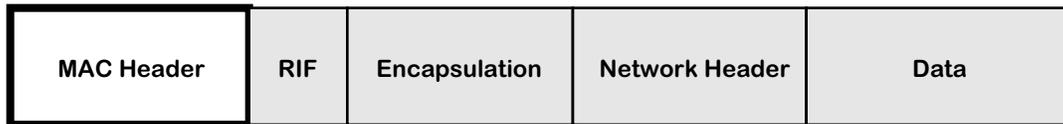
Defined by the organization responsible for the particular routing protocol whose data is being carried within the frame. The values of fields defined in the Encapsulation area allow the recipient to identify which protocol standard to use to decode the Network Header part of the frame.

Data

The payload being carried between the end-stations.

In a routing implementation the first three fields (i.e., MAC header, RIF, and Encapsulation) are the ones stripped and rebuilt when the frame is forwarded. These are the three areas that have to be manipulated. The next sections examine each of these frame packet areas further to see the media and protocol dependencies. We can also examine their interactions.

The MAC Header



The format and values defined for the MAC header are covered in the media standards but even here a variety of choices which are dictated by the upper layer protocol can be found.

Canonical versus Non-Canonical

The first requirement of the switch transformation is the bit ordering of the address fields. For Token Ring and FDDI, this is the so called *non-canonical* ordering or most significant bit first. For Ethernet, this is *canonical* or least significant bit first. Thus, when a frame is moved between these media, the addresses must be bit-swapped.

Abbreviated Addresses

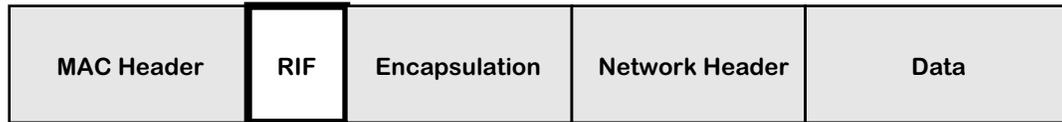
The FDDI and 802.5 Token Ring media allow for the use of small 16 bit addresses or full 48 bit addresses. The OmniSwitch *only* supports 48 bit MAC address LANs thus abbreviated address based protocols cannot be supported.

Functional Addresses and Multicasts

The 802.5 media also have different rules for the formation of multicast addresses or group addresses. In Ethernet a single bit defines the address as a multicast. In 802.5 a single bit also indicates a multicast but the remaining bits are structured into so called Functional Address groups with pre-assigned meanings and functions.

The OmniSwitch *does not* map MCASTs and Functional Addresses; thus protocols dependent on these features may not be switchable any to any.

The RIF Field



The same source routing standard is supported by FDDI and Token Ring so the RIF fields can be switched without problems between these media.

Ethernet does not support source routing thus frames with RIF fields cannot be switched onto these media. However, if you enable “RIF Stripping” you can switch source route frames with RIFs less than 2 bytes long (see Chapter 21, “Managing Token Ring Modules,” for more information).

The alternative of stripping fields, remembering them and reinserting them on replies, i.e. to terminate a source routed connection and act as a proxy to a transparent device is not well standardized and is difficult to execute and manage.

Source Route Termination by Proxy Not Supported

The OmniSwitch will not therefore allow RIF based frames onto Ethernet media unless RIF Stripping is enabled.

Ethernet frames are allowed onto rings if they support transparent bridging, i.e. the port is configured as either Transparent or Source Route/Transparent. Otherwise all communication between SR configured ring ports and transparent Ethernet ports is barred.

Encapsulation



Encapsulation is the biggest problem for implementing a transformation algorithm in support of any to any switching. All of the media provide a choice of more than one encapsulation and not all encapsulations are available on all media. Additionally, the methodology of these encapsulations vary from protocol to protocol.

An ideal protocol would dictate a single encapsulation which would be the same on all media.

Most protocols make use of more than one encapsulation. For example, IP uses Ethertype most of the time on Ethernet and SNAP (an instance of an 802.2 LLC) on FDDI and Token Ring. In this case, there may be clearly established rules for transforming from one encapsulation to another as media are traversed.

Some protocols may allow more than one encapsulation even on a single media type. Some might use the encapsulation to separate functional parts of the protocols, for example, routing table updating protocols from user data forwarding protocols. Others, like IPX may simply allow the user to arbitrarily choose them.

Some, most notably IPX, may entangle the notion of encapsulation with the notion of the network level broadcast domain to create multiple logical networks over a single physical broadcast domain.

Clearly, then there is no single algorithmic rule by which the any to any transformation function can switch arbitrary protocols. There are two choices available to address this situation.

1. The switch must be configurable, per device, per protocol, per media to select the transformation of encapsulations.
2. The switch performs a single transformation and the user must configure all end-stations and routers to use this single choice made by the switch.

The OmniSwitch uses the first approach for IP and IPX as the dominant protocols in the market. It uses the second approach for all other protocols.

Protocols other than IP and IPX

For protocols other than IP or IPX three encapsulations are possible on Ethernet media:

- Ethertype
- IEEE 802.2 LLC
- IEEE 802.2 SNAP (This is an instance of an LLC encapsulation defined by the 802.2 committee to support the transformation of Ethertype Ethernet frames to media which don't support that encapsulation.)

On Token Ring and FDDI, two encapsulations are permitted by the standards:

- IEEE 802.2 LLC
- IEEE 802.2 SNAP.

The SNAP Conversion

The intent of the 802.2 committee is that Ethertype frames are transformed to SNAP on crossing from Ethernet media to 802 media and restored to Ethertype in the reverse direction.

The OmniSwitch could follow this rule for all protocols including IP; however, this would prevent AppleTalk interworking between Ethernet and FDDI. The OmniSwitch explicitly checks for the AppleTalk protocol. If found, the rule is not applied. In addition, the OmniSwitch checks for the Banyan Vines protocol and translates according to the media type (see *Banyan Vines* on page 23-12).

As there may be other protocols with this problem, the SNAP-to-Ethertype transformation is configurable for all protocols other than AppleTalk.

Other Conversions

There are no equivalent algorithmic approaches which the transformation function can adopt for dealing with protocols which require Ethertype on Ethernet and some form of LLC encapsulation on FDDI and/or Token Ring. The mapping between Ethertype values and LLC values is arbitrary requiring tables indexed by protocol.

The approach followed in the OmniSwitch is therefore to simply pass LLC encodings between Ethernet, FDDI and Token Ring with no changes other than to insert/strip the length field required by IEEE 802.3 on Ethernet.

This leaves protocols which require transformations between Ethertype and LLC encapsulations as unswitchable unless the clients and servers can be configured to use SNAP.

Summary of Non-IPX Encapsulation Transformation Rules

To summarize:

- Ethertype/SNAP transformations are configurable for all protocols except AppleTalk and Banyan Vines. Ethertype frames going to FDDI or Token Ring are translated to SNAP unconditionally. SNAP frames going to Ethernet are translated to Ethertype or left as SNAP as per configuration, unless the protocol is AppleTalk in which case they are left as SNAP.
- LLC frames are passed unchanged in value but with the length field required on Ethernet media stripped/inserted.

IPX Encapsulation Transformation Rules

For IPX the encapsulation problems described above are compounded by the introduction of a fourth encapsulation on Ethernet media. Novell introduced a frame format when the IEEE 802.3 standards committee produced its version of Ethernet which was incompatible with Ethernet.

Novell places its network header and data within a raw IEEE 802.3 Ethernet frame with no intervening IEEE 802.2 LLC header. This is in direct contravention of the standards but has become a de facto standard encapsulation.

Novell refers to this encapsulation types as ETHERNET_802.3. It is also widely known as Novell Proprietary, Novell Raw, Raw 802.3, etc. Such frames are identifiable only by the fact that the Novell Network header starts with a two byte field called the *checksum*, which is never used and assumes the value 0xFFFF.

Routers, bridges and switches therefore check for the checksum after an 802.3 length field. In effect, Novell has usurped the value 0xFF for the Destination and Source SAP addresses (DSAP/SSAP) of an LLC header.

Thus on Ethernet media there are four encapsulations for IPX

- Ethertype - value 0x8137
- Novell Proprietary
- LLC - SAP value 0xE0
- SNAP - Protocol Identifier 0x0000008137

On Token Ring and FDDI, the same LLC and SNAP encapsulations are found as on Ethernet (without the length field.)

This leaves an aggregate of four encapsulations across all media with only two being universal (LLC and SNAP).

Unfortunately, the SNAP conversion rule isn't applicable and there is no algorithmic determination for the use of particular encapsulations on any media - it's purely the choice of the network administrator. Worse, multiple encapsulations can be found on a single media to create multiple logical networks over a single physical broadcast domain.

The OmniSwitch therefore allows configuration of the encapsulation transformations of IPX frames. Before transmission of a frame occurs the switch determines first the current encapsulation of the frame. Then, it consults configuration information to determine which of the permitted encapsulations for the media the frame is to be transmitted on is required. Thus, the administrator can choose not only a single output option but an option per possible received encapsulation.

For example, over FDDI media, LLC and SNAP are permissible so the administrator might configure one of the following:

- LLC and SNAP encapsulations received from other FDDI, Token Ring or Ethernet media are translated to SNAP.
- Ethertype and Proprietary encapsulations from Ethernet are translated to LLC.

Essentially, for each encapsulation, transformation to each of the other three encapsulations is available, but may simply be left as is. This choice may be further constrained by the output media type, for example, Ethertype is not a valid option on FDDI or Token Ring.

The Network Header



There are essentially two requirements for the any to any switching transformation function to address the network header fields:

- Network Address to MAC Address Mapping
In every protocol there is a mechanism for mapping global network wide addresses to the MAC addresses required in the local broadcast domain.
- Frame Size Requirements of the Media
Different media have different minimum and maximum frame sizes leading to the issues of padding insertion/stripping and fragmentation/reassembly or maximum frame size negotiation protocols at the network level.

Address Mapping

There are almost as many ways to map a global network level address to a local subnetwork MAC address as there are routing protocols. These may or may not be affected by any to any switching.

Some may construct MAC addresses algorithmically, for example, DECNET model. Some may involve table lookups with an additional protocol to build and maintain these tables, for example, the IP/ARP model. Others may involve some form of building the network address around the MAC address as in the IPX model.

In all cases these mechanisms are susceptible, without good design and forethought, to the problem of canonical versus non-canonical representation of addresses in the network header area.

Address Mapping in IP: ARP

To map a 32-bit IP network address into the MAC address of a locally connected station a router uses the Address Resolution Protocol (ARP) to build an ARP Table. The router broadcasts a request containing the IP address in the body of the frame. The station with that IP address responds with its MAC address *in the body* of an ARP reply frame. The router inserts these two addresses in its ARP table and can then use the MAC address received to transmit any frames addressed to that IP address.

Since a router can have interfaces to Ethernet ports (canonical MAC addresses) and FDDI and Token Ring (non-canonical MAC addresses), it is crucial that the router keeps track of what media type it receives on each port.

If IP ARP were defined such that all MAC addresses, *when conveyed in the body of an ARP*, were in canonical format, switching would be easy. A router, when taking an address from the ARP table and using it as the destination MAC address on an Ethernet port would use the address as is. If sending to FDDI or Token Ring it would bit swap the address to non-canonical format as required by the media.

Given this model of implementation a station responding with an ARP on Ethernet which was switched to FDDI would result in the same representation of the MAC address in the ARP table of the router. The router would then use the bit swapped form in the MAC address of subsequent frames to the FDDI ring and the switch would bit swap these MAC header address as it transformed the frame onto Ethernet, resulting in the correct representation to be received by the original station.

Unfortunately, this model has only been defined in IP for Ethernet and FDDI. Token Ring stations place MAC addresses into the body of ARP frames in their native, non-canonical format and routers use addresses from the ARP table as is when sending to Token Ring ports.

To achieve any to any switching with IP it is therefore necessary for the OmniSwitch to be sensitive to ARP frames and to bit swap the MAC addresses *in the body of the ARP* when switching a frame between Token Ring and FDDI or Ethernet.

◆ Important Note ◆

Beginning with Release 4.4, FDDI is no longer supported.

Because IP is well designed, the issue of address mapping being confined to the ARP protocol, this is sufficient to isolate the problem allowing all subsequent IP frames to be switched any to any.

Address Mapping in IPX

A network address in IPX consists of three parts:

1. Network Number -- a globally unique identifier of a particular broadcast domain.
Strictly, because of the formation of logical networks using encapsulations, this is not equivalent to a physical broadcast domain but the distinction can be put aside for the purposes of this particular discussion.
2. Node Address -- the MAC address of a station on that domain.
3. Socket Number -- the task (process) within that station which should process the message.

Just as in IP, routers move a frame along hop by hop on the basis of the network number portion of the destination address. To do this, IP needs the MAC address of the next hop router. This address is obtained from the RIP table that is built up from the RIP updates sent out by all routers. When a router receives a RIP update frame it uses the source node address in the frame as the MAC address for the next hop router.

Although there is not an explicit ARP like protocol for mapping addresses in IPX, this same function is achieved by the use of source node addresses in RIP frames.

In IPX, as in IP, the canonical versus non-canonical representation of addresses in ARPs still applies. In switching, this needs to be considered for the source node address in IPX frames.

In IPX Ethernet and FDDI observe a convention of using MAC addresses in the IPX header in canonical format. For Token Ring these addresses are non-canonical.

Proprietary Token Ring IPX switching

The OmniSwitch offers the facility to modify IPX frames switching between Token Ring and FDDI or Ethernet. ARP bit swapping for IP is a de facto standard widely implemented in the industry. This is not the case with IPX. The switch must be able to co-exist with bridges that do not support any to any switching or applications where this feature is not required. Therefore this feature can be configured on or off.

Frame Size Requirements

The frame size requirement for the different media cause two problem areas which have to be addressed by the any to any switching transformation function.

- Ethernet has a minimum frame size requirement. This requires that padding is inserted on frames switched to it which are below the minimum size and stripped from frames switched from it.
- All media have different maximum frame size requirements. This gives rise to the problems of fragmenting large frames and/or negotiating maximum frame sizes.

Insertion of Frame Padding

Ethernet has a minimum frame size of 64 bytes. For frames smaller than 64 bytes it is a simple task for the OmniSwitch to perform padding. Stripping such padding from Ethernet frames when switching to FDDI or Token Ring is not so easy.

In most implementations of IP that we have tested the presence of padding on FDDI or Token Ring frames appears not to cause any problems. However, IPX implementations are adversely affected by its presence. Therefore the OmniSwitch takes a conservative approach *for all frames*, regardless of protocol type, and strips padding *where it can be detected*.

Stripping of Padding for all IEEE 802.3 Frames.

Ethernet frames in IEEE 802.3 format can be stripped of padding because of the presence of the length field. This includes all LLC and hence SNAP encapsulated protocols as well as Novell Proprietary format.

No stripping of non-IPX Ethertype Frames

Padding can only be detected for Ethertype encapsulated frames if the protocol is known and the protocol has some length information which can allow the valid data size to be inferred. This is protocol specific and is currently only performed for IPX frames. Thus, the OmniSwitch *does not* strip padding from non-IPX Ethertype encapsulated frames *including IP*.

IPX Specific Stripping

For IPX the OmniSwitch performs pad stripping for all frame types including Ethertype. This is possible because all IPX frames have a common header that includes the data length, allowing the frame size to be inferred.

In fact, for IPX, the length in the IPX header is used to strip padding in all frame encapsulations including the 802.3 based formats. This is because many IPX Ethernet implementations also pad frames to an even byte length. This single byte pad when performed on 802.3 based frames is included in the 802.3 length field. Thus the generic 802.3 based stripping technique is not sufficient to strip this odd-byte padding. When performing any to any switching FDDI implementations of IPX were found to be tolerant of this extra byte whereas Token Ring implementations would not work with it present. By adopting the single IPX stripping strategy of using the IPX header length these problems are avoided thus the OmniSwitch unconditionally strips all padding from IPX frames.

Also, it *does not* support odd-byte pad insertion when switching to Ethernet. This was a feature added to overcome limitations of some NIC cards which is now of only historical importance and in fact, Netware 4.1 servers provide this insertion as a port configuration option.

MTU Handling

Routers address the problem of maximum frame size limitations with the notion found in many protocols of a Maximum Transmission Unit (MTU) size. Protocols use this notion in two possible ways.

- PDU Fragmentation/Reassembly

The router is configured with the MTU of each port. If a frame that is too large is required to be sent on a port, the Protocol Data Unit (PDU) within the frame is fragmented into many smaller PDUs, each of which is re-encapsulated and sent as a frame that fits within the MTU.

- Connection-oriented end-to-end MTU negotiation

When an end-station enters into a protocol to communicate with another station the initial PDU exchanges are guaranteed to fit all possible MTUs. In the handshaking between end-stations to establish the connection a phase is entered where large frames are sent. If an intervening link has an MTU too small for these frames it will be dropped and the handshaking will time out. The end-stations send progressively smaller frames until the handshaking succeeds and hence establish the MTU to be used between the two stations for the remainder of their connection use.

IP supports the former mechanism and IPX the latter.

IP Fragmentation

The OmniSwitch Ethernet interfaces will use IP fragmentation if they are allowed to (i.e., if the *Don't Fragment* bit is not set.) Fragmentation by FDDI and Token Ring is not supported though technically the Token Ring could send frames larger than those supported by FDDI and LAN Emulation could generate frames larger than both.

ICMP Based MTU Discovery

IP uses the Don't Fragment bit to support an MTU discovery protocol that superficially resembles the negotiation of IPX. The difference is that when IP stations attempt to discover an MTU size for their use, which doesn't require fragmentation by intermediate routers, the protocol expects a protocol response *by the intermediate router*, this is an ICMP reporting that a frame was dropped because it couldn't be fragmented.

The OmniSwitch transformation function of any to any switching *does not* support this ICMP generation but just silently drops IP frames which can't be fragmented. The IP *router* in the OmniSwitch does honor this protocol and support ICMP. It is only the any to any switching which doesn't because it is not a router and may not even have an IP address with which to respond.

IPX Packet Size Negotiation

For IPX the requirement of intervening devices is simply to drop frames that are too large to be forwarded. This is what the OmniSwitch does.

Other Protocols

Dropping oversize frames is the approach for all protocols other than IP. If the protocol in question is modeled like IPX this will be the correct thing to do and will not cause problems. If the protocol is modeled like IP and expects fragmentation to occur or requires explicit response from the OmniSwitch then the protocol will not succeed in any to any switching.

Banyan Vines

Banyan Vines supports Ethernet, FDDI, and Token Ring networks. Each type of network generates a different frame format, so the OmniSwitch performs translations for frames moving from one network type to another. The Banyan Vines protocol only uses one frame format per network type—no user configuration of translations is necessary. This protocol uses Ethernet II frames on Ethernet, SNAP frames on FDDI, and IEEE 802.2 (LLC) frames on Token Ring. The OmniSwitch uses these frame formats when translating Banyan Vines frames.

Note

Checksums for Banyan Vines frames are automatically set to the null checksum, 0xFFFF, so that the checksum header does not require recalculation. Receiving stations will ignore this field and assume the sender is not using checksums.

Configuring Encapsulation Options

You will configure frame encapsulation based on the destination MAC address or the destination switch port. Whether a frame is encapsulated based on the destination MAC or the port depends whether the frame has a unicast, multicast, or broadcast destination.

Forwarding versus Flooding

Such frames will be handled in two ways:

- **Forwarded Frames.** If the frame has a unicast destination address which has been learned on a particular port, the encapsulation translation choices are driven by options associated with the destination MAC address.
- **Flooded/Multicast Frames.** If the frame has a unicast destination address which has not been learned on a particular port, or if the destination address is a multicast address, then the frame has to be transmitted on potentially many ports. In this case the encapsulation translation choices are driven by options associated with each destination port.

Port Based Translation Options

The translation options for ports allow configuration of IP and IPX protocols on a per encapsulation basis.

MAC Address Based Translation Options

The translation options for MACs arises from two possible sources.

- Inheritance from Port Options During Source Address Learning
- When a source MAC address is learned, the translation options of the port on which it is learned are copied into the MAC-based database.
- Automatic Determination by AutoTracker
- When a frame is processed by AutoTracker as part of determining the VLAN to be associated with the MAC the frames protocol type and encapsulation are also determined. This information is used to update/set the translation options in the MAC based database.

Which of these options is used is determined by setting the autoencaps option.

“Native” versus “Non-Native” on Ethernet

For the Ethernet one further distinction is made. If the frame received from the backplane is an Ethernet media type frame from another Ethernet switching module in the same chassis, then *no encapsulation translations are applied*. Such frames are referred to as Native frames.

If the frame is of an Ethernet media type but was put onto the backplane by some other type of switching module, for example, the frame came from a FDDI card via a trunk port, or from the MPM via routing, then *encapsulation translations are applied*. Such frames are referred to as Non-Native frames.

◆ Important Note ◆

The `.cmd` file contains a command called `hreXnative` that by default is set to `1`. If your switch uses multiple encapsulations (for example, VLAN 2:1 is 802.3 IPX and VLAN 3:1 is Ethernet II IPX) then the `hreXnative` command must be set to `0`. See Chapter 11, “Managing Files,” for more information on the `.cmd` file.

“Native” versus “Non-Native” on FDDI and Token Ring

For FDDI, Token Ring and LAN Emulation on ATM, a native/non-native distinction is not made. Instead, no encapsulation translations are applied by these switching modules to frames which are of their own media type.

No Translation on Trunk or PTOP ports

Switching modules which support encapsulation mechanisms, such as Trunking ports on FDDI and Token Ring, and Point to Point ports on ATM do not apply translation to frames destined to such ports.

All other aspects of the transformation process are driven by the media type of the frame, the media type of the port on which the frame is to be transmitted and the protocol type determined for the frame. Thus frame padding insertion/stripping, IP fragmentation, IP ARP bit swapping, etc., are all automatic.

The Proprietary Token Ring IPX Option

The one area which remains configurable is the bit swapping of source addresses for IPX in order to allow Token Ring to work with FDDI and Ethernet. This is the equivalent function to IP ARP bit swapping.

This option is configurable and by default is on.

The User Interface

This chapter documents User Interface (UI) commands to configure encapsulation options. For documentation on Command Line Interface (CLI) commands to configure encapsulation options, see the *Text-Based Configuration CLI Reference Guide*.

◆ Important Note ◆

In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. See Chapter 8, “The User Interface,” for documentation on changing from CLI mode to UI mode.

Simple encapsulation options can be configured through the **modvp**, **addvp**, **crgp** commands. More advanced encapsulation options can be found in the commands under the **Switch** menu.

Essentially, the forwarding code is now capable of applying the transformation function per protocol per encapsulation per port for flooded/mcast traffic and per protocol per encapsulation per destination MAC address for forwarded unicast traffic. The old interface provides a small subset of these possible port translation options.

The `advp`, `modvp` and `crgp` Commands

All of these commands include in their dialogue an Output Format question for ports and a subsidiary IEEE 802.2 Pass through option.

The options offered are:

- a default,
- Ethertype,
- SNAP and
- LLC.

Each of these represents a set of translation options for the IP and IPX protocols. The names chosen for these sets basically represent the translations for IPX with the translation for IP being implied.

For example, LLC represents a translation set where all IPX encapsulations are configured to translate to IEEE 802.2. This is not a valid encapsulation for IP which is therefore configured to a default appropriate to the media, Ethertype for Ethernet ports and SNAP for FDDI and Token Ring ports. The translation of all other protocol types and encapsulations is fixed by the OmniSwitch. Thus AppleTalk is never translated and Ethertype/SNAP based protocols follow the IP option.

For those options which imply a translation of IEEE 802.2 IPX frames to something else a subsidiary question is asked, "IEEE 802.2 IPX Pass Through(y/n):" An IEEE 802.2 pass through option is provided because 4.1 Novell servers use this encapsulation by default and it is becoming Novell's encapsulation of choice.

The Default Translation Option

The meaning of the default is determined separately for each media type and is fully configurable. The factory defaults are chosen so that the latest release is fully compliant with earlier ones. The default translation option is provided to allow a "single point of configuration of all ports" capability. When the default option for a media is changed all ports of that media type whose encapsulation is configured as default will inherit the new translation setting. All MAC address-based translation options which were inherited from those ports, as opposed to those set by AutoTracker, will also be updated. Ports which have an encapsulation setting other than default will be unaffected.

Ethernet Factory Default Translations

For Ethernet switching module ports the factory default is set to the following:

Ethernet Media - Default Mode
No translation is performed on outbound Ethernet frames where the inbound interface was Ethernet.
IP frames of any encapsulation are transmitted as Ethernet II frames.
IPX frames are transmitted as IEEE 802.3 Proprietary as the default setting. The only exception is when LLC passthrough mode is enabled, then the IEEE 802.2 (LLC) frames are forwarded as is.
No translation is performed on Appletalk frames, and we currently support only Appletalk Phase II (SNAP format).
Banyan Vines frames are transmitted as Ethernet II frames.
Other than IP and IPX, all other Ethernet II and SNAP encapsulated protocols are sent as Ethernet II frames.
All other IEEE 802.3 with LLC encapsulated protocols are not translated.

FDDI Factory Default Translations

For FDDI switching module ports the factory default is set to the following:

FDDI Media - Default Mode
IP of any encapsulation is encapsulated SNAP
IPX encapsulations are encapsulated SNAP except for IEEE 802.2 which is forwarded as is.
Banyan Vines of any type are transmitted as SNAP.
All other Ethertype and SNAP encapsulated protocols are sent as for IP.
All other LLC encapsulated protocols are forwarded as is.

Token Ring Factory Default Translations

For Token Ring switching module ports the factory default is set to the following:

Token Ring Media - Default Mode
IP of any encapsulation is encapsulated SNAP
IPX encapsulations are encapsulated SNAP except for IEEE 802.2 which is forwarded as is.
Banyan Vines of any type are transmitted as LLC.
All other Ethertype and SNAP encapsulated protocols are sent as for IP.
All other LLC encapsulated protocols are forwarded as is.

ATM LANE Factory Default Translations

For ATM LAN Emulation service ports the factory default is set to the following:

ATM LANE - Default Mode
No translations performed on Ethernet frames.
FDDI and Token Ring frames are translated to either SNAP or LLC and are transmitted as such on ATM LANE.
Banyan Vines Token Ring and FDDI frames are translated to Ethertype.

The Ethertype Option

This option can only be applied to Ethernet switching module ports. It is set to the following:

Ethernet Media - Ethernet II Mode
No translation is performed on outbound Ethernet frames where the inbound interface was Ethernet.
IP frames are transmitted as Ethernet II frames.
All IPX frames are transmitted as Ethernet II frames. The only exception is when LLC passthrough mode is enabled, then the IEEE 802.2 (LLC) frames are forwarded as is.
No translation is performed on Appletalk frames, and we currently support only Appletalk Phase II (SNAP format).
Other than IP and IPX, all other Ethernet II or SNAP frames are transmitted as Ethernet II frames.
Other IEEE 802.3 with LLC are not translated.

ATM LANE - Ethernet II Mode
IPX frames from FDDI, Token Ring, and Ethernet SNAP frames are translated to Ethertype.
All other SNAP frames from FDDI, Token Ring, and Ethernet SNAP are translated to Ethertype. However, Appletalk ARP SNAP frames from Token Ring and FDDI are left as SNAP; Banyan Vines frames from FDDI are translated to Ethertype.
All other 802.2 frames from FDDI, Token Ring, and Ethernet are left as is. The exception are Banyan Vine frames from Token Ring, which are translated to Ethertype.
All Ethernet Ethertype frames are not translated.

The SNAP Option

This option can be applied to all media type ports and is set to the following:

Ethernet Media - SNAP Mode
No translation is performed on outbound Ethernet frames where the inbound interface was Ethernet.
IP frames are transmitted as SNAP frames.
All IPX frames are transmitted as SNAP frames.
No translation is performed on Appletalk frames, and we currently support only Appletalk Phase II (SNAP format).
Other than IP and IPX, all other Ethernet II or SNAP frames are transmitted as SNAP frames.
Other IEEE 802.2 with LLC are not translated.

FDDI / Token Ring Media - SNAP Option
No translation is performed on outbound FDDI or Token Ring frames where the inbound interface was the same media type.
IP frames of any encapsulation type are transmitted as SNAP frames.
IPX frames received that do not have an IEEE 802.2 encapsulation type, are transmitted as SNAP.
IPX frames received that are of IEEE 802.2 encapsulation type are transmitted as SNAP if the LLC passthrough is disabled. If the LLC passthrough is enables, these frames will not be translated.
No translation is performed on Appletalk frames, and we currently support only Appletalk Phase II.
All other LLC encapsulated protocols are left as is.

In the **modvp** or **addvp** commands for FDDI and Token Ring the only choices other than default are SNAP or LLC and the default must be one of these. As the factory default is SNAP with IPX 802.2 Pass through and the SNAP does not imply pass through the additional question about pass through is not asked on FDDI and Token Ring ports as the preference can be expressed by choosing default or SNAP explicitly.

ATM LANE - SNAP Mode

All IPX frames are translated to SNAP unless they are already SNAP, in which case they are forwarded as is.

All Ethertype or SNAP frames from Ethernet and SNAP frames from Token Ring or FDDI are translated to SNAP or left as SNAP. The exception is Banyan Vines frames from FDDI, which are translated to Ethertype.

All other LLC frames are left as is. The exception is Banyan Vines from Token Ring, which is translated to Ethertype.

The LLC Option

This option can be applied to all media type ports and is set to the following:

Ethernet Media - LLC Mode
No translation is performed on outbound Ethernet frames where the inbound interface was Ethernet.
IP frames are transmitted as Ethernet II frames.
All IPX frames are transmitted as IEEE 802.2 (LLC) frames.
No translation is performed on Appletalk frames, and we currently support only Appletalk Phase II (SNAP format).
Other than IP and IPX, all other Ethernet II or SNAP frames are transmitted as Ethernet II frames.
Other IEEE 802.2 with LLC are not translated.

FDDI / Token Ring Media - LLC Mode
No translation is performed on outbound FDDI or Token Ring frames where the inbound interface was the same media type.
IP frames are transmitted as SNAP frames.
All IPX frames are transmitted as IEEE 802.2 (LLC) frames.
No translation is performed on Appletalk frames, and we currently support only Appletalk Phase II (SNAP format).
Other than IP and IPX, all other Ethernet II or SNAP frames are transmitted as SNAP frames.
Other IEEE 802.2 with LLC are not translated.

In the **modvp** or **addvp** commands for FDDI and Token Ring the only choices other than default are SNAP or LLC and the default must be one of these. As the factory default is SNAP with IPX 802.2 Pass through and SNAP does not imply IPX 802.2 Pass through, the additional question about pass through is not asked on FDDI and Token Ring ports. By choosing SNAP, it is implied that there is no IPX 802.2 Pass through.

ATM LANE - LLC Mode
IPX frames are translated to 802.2 LLC.
All other SNAP frames from FDDI, Token Ring, and Ethernet SNAP are translated to Ethertype. However, Appletalk ARP SNAP frames from Token Ring and FDDI are left as SNAP; Banyan Vines frames from FDDI are translated to Ethertype.
All other LLC frames are not translated. The exception is Banyan Vines frames from Token Ring, which are translated to Ethertype

Interaction with the new interface

If the port to which these commands are being applied has been configured with the new interface commands its encapsulation will be displayed as **SWCH** in the **vi** command output. The user is alerted to this fact in these commands by the default response to the output format question in the **modvp** command being displayed as "*" instead of **d,e,s** or **l**. A simple return will leave the options unchanged in this case. If the port is currently one of **d,e,s** or **l** and the user types "*" in response the encapsulation is changed to **SWCH** and the options are set to a null translation set.

The "vi" Command

The encaps column displays the encapsulation subset options set for each port. If the port has been configured with the new interface this is indicated by displaying "SWCH." The "canned" subsets offered in this interface are displayed as follows:

- **DFLT.** This indicates that the port is using the default translation options applicable to the media type of this port. See above.
- **802.2.** This indicates that IPX frames of any encapsulation will be encapsulated with IEEE 802.2. Non-IPX frames other than AppleTalk will be transformed to Ethertype on Ethernet ports and SNAP on FDDI or Token Ring ports. AppleTalk frames are never transformed.
- **SNAP.** This indicates that Ethertype frames of all protocols and IPX proprietary frames will be translated to SNAP and all SNAP frames will be left as is.

IEEE 802.2 encapsulated IPX frames may be left as is if the IEEE 802.2 pass through option is in effect for this port. All other IEEE 802.2 encapsulated protocols are left as is.

- **ETH.** This indicates that SNAP frames of all protocols except AppleTalk will be translated to Ethertype.

SNAP and Proprietary IPX frames will be transformed to Ethertype.

IEEE 802.2 encapsulated IPX frames may be left as is if the IEEE 802.2 pass through option is in effect for this port.

All other IEEE 802.2 encapsulated protocols are left as is.

To discover whether IEEE 802.2 pass through is in effect on a port the user must either use the **swch** command from the switch menu or use **modvp** and observe the encapsulation offered and/or the default response for the pass through question.

The Switch Menu

The switch menu contains commands that allow you to set translation options discussed earlier in this chapter. It also contains commands to change the default values.

To view the switch menu, enter **switch** at the prompt. If you are in verbose mode, the following screen is displayed. Otherwise, type a **?** at the switch menu prompt to display the Switch Menu:

Command	Switch Menu
propipx	Configure Default Proprietary IPX Token Ring to any switching
facdef	Configure Defaults to Factory values
ethdef	Configure Default Ethernet Translation
fddidef	Configure Default FDDI Translation
trdef	Configure Default TR Translation
swch	Configure Any To Any Switching Port Translations
swchmac	View per MAC Translation Options
autoencaps	Turn AutoTracker translations On or OFF

The commands above and their operations are described in the sections below.

Proprietary IPX Token Ring

The **propipx** command allows you to turn on or off the default proprietary IPX switch translation. (Refer to Appendix B, “Output Translation Options,” for information on the Proprietary IPX feature.)

To turn on the Proprietary IPX feature (the default), enter the following at the system prompt:

```
propipx on
```

A message is displayed to confirm the activation of the Proprietary IPX feature. Please note that the switch must be rebooted for the setting to take effect.

To turn off the Proprietary IPX feature type:

```
propipx off
```

Factory Defaults

You can reset all ports in the switch to their default factory settings. Any custom translations you configured through **modvp**, **ethdef**, **fddidef**, **trdef**, or **swch** commands will be overridden by the default translation for the given media type (i.e., Ethernet, FDDI, etc.). Factory defaults for each media type are described earlier in this chapter.

To reset to factory defaults, enter the **facdef** command at the system prompt. The following screen displays:

```
This will reset the default translations for each media type to a factory default.  
It will then set all port translation options to inherit these defaults.  
It will then reset the forwarding table translation options for all addresses learnt on  
those ports to those port defaults.  
Do you want to do this? (no):
```

Enter a **Y** to reset all port settings.

Default Ethernet Translations

The **ethdef** allows you to set up default translations for all Ethernet ports. To do so:

1. Enter **ethdef** at the system prompt. The following screen displays:

```

This will reset the default translations for Ethernet media to a new value.
All Ethernet ports currently set to default will inherit these new translation options.
It will then reset the forwarding table translation options for all addresses learnt on
those ports to those port defaults.
Do you want to do this? (no):

```

2. Press **Y** at the **Do you wish to do this?** prompt to indicate that you want to change the defaults. The current settings for Ethernet ports are displayed, in a screen similar to the following:

```

Translation Options:
1      IP Ethertype           -> Ethertype
2      IP IEEE 802 SNAP      -> Ethertype

3      IPX ETHERNET_II       -> 802.3
4      IPX ETHERNET_802.3    -> 802.3
5      IPX ETHERNET_802.3/FDDI/TOKEN_RING -> 802.3
6      IPX ETHERNET_SNAP/FDDI_SNAP/TOKEN-RING_SNAP -> 802.3

```

There are six frame types for which you can set translation options. The frame type in the left column indicates the incoming frame, and the frame type in the right column (after the **->**) indicates the outgoing frame. You can configure the outgoing frame type for each incoming frame.

3. You change an outgoing frame type by entering its line number, an equal sign (=) and a frame type indicator (**e**, **s**, **2**, or **3**). The frame type indicators represent the following frames:

```

e      Ethernet II or Ethertype
s      SNAP
2      802.2 or LLC
3      Ethernet 802.3

```

For example, if you wanted to change incoming IPX Ethernet II frames to Ethernet 802.3 frames, then you would enter

```
3=3
```

Please note that the IP Translation Options accept only Ethertype (**e**) or SNAP (**s**).

4. When you are done changing translations, enter **save** to save all of your settings. If you enter **quit**, you will exit the **ethdef** command without saving your changes.

Default FDDI Translations

The **fdiddef** command allows you to set up default translations for all FDDI ports. To do this:

1. Enter the **fdiddef** command at the system prompt. The following screen displays:

```
This will reset the default translations for FDDI media to a new value.
All FDDI ports currently set to default will inherit these new translation options.
It will then reset the forwarding table translation options for all addresses learnt on
those ports to those port defaults.
Do you want to do this? (no):
```

2. Press **Y** at the **Do you wish to do this?** prompt to indicate that you want to change the defaults. The current settings for FDDI ports are displayed, in a screen similar to the following:

```
Translation Options:
1      IP Ethertype          -> Ethertype
2      IP IEEE 802 SNAP      -> Ethertype

3      IPX ETHERNET_II       -> 802.3
4      IPX ETHERNET_802.3    -> 802.3
5      IPX ETHERNET_802.3/FDDI/TOKEN_RING -> 802.3
6      IPX ETHERNET_SNAP/FDDI_SNAP/TOKEN-RING_SNAP -> 802.3
```

There are six frame types for which you can set translation options. The frame type in the left column indicates the incoming frame, and the frame type in the right column (after the **->**) indicates the outgoing frame. You can configure the outgoing frame type for each incoming frame.

3. You change an outgoing frame type by entering its line number, an equal sign (=) and a frame type indicator (**e**, **s**, **2**, or **3**). The frame type indicators represent the following frames:

```
e      Ethernet II or Ethertype
s      SNAP
2      802.2 or LLC
3      Ethernet 802.3
```

For example, if you wanted to translate incoming IPX Ethernet 802.3 frames to Ethernet 802.3 frames (FDDI raw), then you would enter

```
4=3
```

Please note that the IP Translation Options accept only Ethertype (**e**) or SNAP (**s**).

4. When you are done changing translations, enter **save** to save all of your settings. If you enter **quit**, you will exit the **ethdef** command without saving your changes.

◆ **Important Note** ◆

The IP Translation Options allow only SNAP (**s**). The IPX translations allow SNAP (**s**), and LLC (**2**) for all frame types. The Ethertype (**e**) translation is not allowed for FDDI. The Ethernet 802.3 translation (**3**) is allowed only on incoming Ethernet 802.3 frames, which referred to as “FDDI raw.”

The **fdidef** command will accept your input and will not return an error message if you try to change an IPX translation option to Ethertype or Ethernet 802.3. However, that does not mean that the IPX frames are being translated to Ethertype or 802.3. Regardless of what the **fdidef** screen displays, switch software does not translate FDDI frames to Ethertype for any frame or to 802.3 for any frame except incoming 802.3.

Default Token Ring Translations

The **trdef** command allows you to set up default translations for all Token Ring ports. To do so:

1. Enter the **trdef** command at the system prompt. The following screen displays:

```
This will reset the default translations for TR media to a new value.
All TR ports currently set to default will inherit these new translation options.
It will then reset the forwarding table translation options for all addresses learnt on
those ports to those port defaults.
Do you want to do this? (no):
```

2. Press **Y** at the **Do you wish to do this?** prompt to indicate that you want to change the defaults. The current settings for FDDI ports are displayed:

```
Translation Options:
1      IP Ethertype          -> Ethertype
2      IP IEEE 802 SNAP     -> Ethertype
3      IPX ETHERNET_II      -> 802.3
4      IPX ETHERNET_802.3   -> 802.3
5      IPX ETHERNET_802.3/FDDI/TOKEN_RING -> 802.3
6      IPX ETHERNET_SNAP/FDDI_SNAP/TOKEN-RING_SNAP -> 802.3
```

There are six frame types for which you can set translation options. The frame type in the left column indicates the incoming frame, and the frame type in the right column (after the **->**) indicates the outgoing frame. You can configure the outgoing frame type for each incoming frame.

3. You change an outgoing frame type by entering its line number, an equal sign (=) and a frame type indicator (**e**, **s**, **2**, or **3**). The frame type indicators represent the following frames:

e	Ethernet II or Ethertype
s	SNAP
2	802.2 or LLC
3	Ethernet 802.3

For example, if you wanted to translate incoming IPX SNAP frames to LLC frame, then you would enter

6=2

4. When you are done changing translations, enter **save** to save all of your settings. If you enter **quit**, you will exit the **trdef** command without saving your changes.

◆ Important Note ◆

The IP Translation Options allow only SNAP (**s**). The IPX translations allow only SNAP (**s**), and LLC (**2**) for all frame types. The Ethertype (**e**) and 802.3 translations are not allowed for Token Ring.

The **trdef** command will accept your input and will not return an error message if you try to change an IPX translation option to Ethertype or Ethernet 802.3. However, that does not mean that the IPX frames are being translated to Ethertype or 802.3. Regardless of what the **trdef** screen displays, switch software does not translate Token Ring frames to Ethertype or 802.3.

Port Translations

The **swch** command allows you configure translations on a port-by-port basis. Its translation options are similar to those for **ethdef**, **fddidef**, and **trdef**. However, instead of applying translations to all ports for a particular media type, **swch** applies translations only to the port you specify.

To specify translation for a single port:

1. Start the **swch** command by entering it at the prompt as shown:

```
swch <slot>/<port>
```

where **<slot>** is the board on which the port is located and **<port>** is the port number. For example, to set the translation for port 1 on slot 2, enter the following:

```
swch 2/1
```

2. Something like the following screen displays, showing the current translation settings for the port:

```

Port Translations for Ethernet port 2/1/brg/1

0      Framing Type: DFLT

Translation Options:
1      IP Ethertype           -> Ethertype
2      IP IEEE 802 SNAP       -> Ethertype

3      IPX ETHERNET_II        -> 802.3
4      IPX ETHERNET_802.3     -> 802.3
5      IPX ETHERNET_802.2/FDDI/TOKEN_RING -> 802.3
6      IPX ETHERNET_SNAP/FDDI_SNAP/TOKEN-RING_SNAP -> 802.3

```

The top line of the display indicates the media type of the port as well as the slot number, port number, service type, and service number. The next line, **Framing Type**, indicates the framing type applied to this port through the **modvp** command. If the framing type had been defined through the Switch menu, then this field would read **SWCH**.

3. The Translation Options section shows the six frame types for which you can set translation options. The frame type in the left column indicates the incoming frame, and the frame type in the right column (after the **->**) indicates the outgoing frame. You can configure the outgoing frame type for each incoming frame.

Note that the default option is a question mark (?). If you press **<Return>**, the help information will be redisplayed.

4. You change an outgoing frame type by entering its line number, an equal sign (=) and a frame type indicator (**e**, **s**, **2**, or **3**). The frame type indicators represent the following frames:

e	Ethernet II or Ethertype
s	SNAP
2	802.2 or LLC
3	Ethernet 802.3

For example, if you wanted to translate incoming IPX SNAP frames to LLC frames, then you would enter

```
6=2
```

5. When are done changing translations, enter **save** to save all your settings. If you enter **quit**, you will exit the **swch** command without saving your changes.

Please note that valid translation options depend on the media type of the port. Ethernet ports allow all frame translation options, but FDDI and Token Ring ports have limitations. See *Default FDDI Translations* on page 23-26 and *Default Token Ring Translations* on page 23-27 for more information on media limitations.

Configuring Additional Ports

If you want to configure additional ports, you can use the **n** option of the **swch** command to configure the next port, or the **p** option of the **swch** command to configure the previous port. For example, if you want to configure translations on port 2 for the card in slot 4 after configuring Port 1 in Slot 4, enter

```
n
```

at the prompt. You are now ready to configure port 3 of slot 4.

If you want to configure translations on port 1 for the card in slot 5 after configuring Port 2 in Slot 5, enter

```
p
```

at the prompt. You are now ready to configure port 1 of slot 5.

When are done changing translations, enter **save** to save all your settings. If you enter **quit**, you will exit the **swch** command without saving your changes.

Displaying Ethernet Switch Statistics

The **swch** command can also be used to display basic statistics for Ethernet ports. These statistics are the lowest level, most primitive statistics maintained by an Ethernet board. The more familiar RMON and MIB II statistics are generated from these statistics. If you want to display the switch statistics for an Ethernet port, enter

```
swch <slot>/<port>
```

where **<slot>** is the slot number of the module, and **<port>** is the number of the port for which you want to view statistics. For example, to look at statistics for port 4 in slot 3, enter:

```
swch 3/4
```

A screen similar to the following is displayed:

```
Port Translations for Ethernet port 3/4/brg/1
0      Framing Type: DFLT
Translation Options:
1      IP Ethertype           -> Ethertype
2      IP IEEE 802 SNAP       -> Ethertype
3      IPX ETHERNET_II        -> 802.3
4      IPX ETHERNET_802.3     -> 802.3
5      IPX ETHERNET_802.2/FDDI/TOKEN_RING -> 802.3
6      IPX ETHERNET_SNAP/FDDI_SNAP/TOKEN-RING_SNAP -> 802.3
```

If this port is an Ethernet media port, enter **r** at the system prompt and then press **<Return>**. If you do this for a port other than an Ethernet port, this will be ignored.

If the port selected is an Ethernet based port, something like the following would be displayed:

```

Ethernet Statistics for Ethernet port 3/4/Brg/1
Received Good Octets      0      Transmitted Good Octets      0
Received Bad Octets       0
Total Octets              0
Received Unicasts         0      Transmitted Unicasts         0
Received Multicasts       0      Transmitted Multicasts       0
Received Broadcasts       0      Transmitted Broadcasts       0
Received Buffer Discards   0      Transmitted Buffer Discards   0
Received Collision Count   0      Transmitted Retry Count      0
Received Runt Count        0      Transmitted More Count       0
Received Error Discard    0      Transmitted Once Count       0
Drop Event Count          0      Transmitted Defer Count      0
Received Jabbers          0      Loss Carrier Count           0
Received Over Size        0      Transmitted Late Collisions   0
Received Late Collision    0      Transmit Underflow           0
Received 1024 +           0      Port Filtered                 0
Received 512 +            0      Vlan Filtered                 0
Received 256 +            0      Mtu Exceeded                  0
Received 128 +            0
Received 65 +             0
Received 64               0
vseTxDiscard              0

```

The fields displayed by the **r** option of the **swch** command are described below:

◆ **Note** ◆

The first group of statistics are the numbers of bytes transmitted and received. These are useful in working out bandwidth usage by the port. Bad octets are important to count in the total octets count as they consume bandwidth at the expense of useful traffic. To ignore them would lead to mysterious loss of bandwidth in any calculations performed.

Received Good Octets. The total number of bytes received in good frames.

Received Bad Octets. The total number of bytes received in bad frames.

Total Octets. The total number of octets transmitted or received in good or bad frames on this port.

Transmitted Good Octets. The total number of bytes successfully transmitted.

Received Unicasts. The number of frames received on this port whose destination address is a unicast format.

Transmitted Unicasts. The number of frames transmitted on this port whose destination address is a unicast format.

Received Multicasts. The number of frames received on this port whose destination address is a multicast format.

Transmitted Multicasts. The number of frames transmitted on this port whose destination address is a multicast format.

Received Broadcasts. The number of frames received on this port whose destination address is the broadcast address.

Transmitted Broadcasts. The number of frames transmitted on this port whose destination address is the broadcast address.

Note that these statistics merely indicate the format of the destination address of frames transmitted/received on this port, not that the addressed device and/or devices necessarily reside on that port. For example, unknown unicast addressed frames are flooded to many ports.

Received Buffer Discards. Due to congestion of traffic from multiple ports on the board, timely access to buffers was not available to receive a frame from the network port and the frame was discarded.

Transmitted Buffer Discards. Due to a shortage of buffers and/or congestion on the network port, frames received from the backplane destined to this port were dropped.

Transmit Underflow. Due to congestion of traffic from multiple ports on the board, timely access to the buffer containing the frame currently being transmitted by this port was not obtained and the frame had to be aborted and discarded.

vseTxDiscard. Due to congestion of traffic from multiple ports and boards in the system, traffic received from the network port could not be queued to the backplane due to buffer availability.

Received Collision Count, Received Runt Count. These counts may be considered normal on a shared segment (e.g., AUI and BNC connected Ethernet) where more than two stations exist. The first indicates that a frame which the port started to receive from a station was subjected to a collision from a third station. This is normal. Such collisions between third party stations may cause this port to see fragments of a frame which are discarded as runts. This too is normal on multiple station Ethernet segments. On point to point 10Base-T connections these events may be considered abnormal indicating a possible intermittent wiring problem (unless hubs which propagate fragments are in use.) These statistics do not indicate the loss of any frame but rather events associated with the attempts to finally successfully transfer the frame.

Transmitted Defer Count, Transmitted Once Count, Transmitted More Count, and Transmitted Retry Count. These statistics are all related to collisions and deferral where this port is actively trying to transmit a frame. The CSMA part of CSMA/CD, the protocol of Ethernet, requires that a station which wishes to transmit first listens to the media to see if a transmission is already in progress. If it is, then the station must defer transmission until the media is quiet. The Defer count is the number of times this happens and is normal. A high defer count, relative to total numbers of frames transmitted by the port, can be indicative of a busy segment. If a transmission is not in progress the station may begin to transmit. Due to propagation delays it is possible for a station to suffer a collision from another station trying to transmit, even though both listened for quiet media. When this occurs, both stations “back off” for a random time before attempting transmission again. In theory, subsequent collisions may occur on these retries. Once, More, and Retry indicate whether this is occurring. If a collision occurs but succeeds on the retry, the Once counter is incremented, i.e., we collided once. If more than one retry is required, the More count is incremented. If up to 16 retries are attempted and all collide, then the frame is dropped and the Retry count is incremented. Again, Once, More, and Retry are normal events on CSMA/CD media but high numbers, relative to total transmitted frames, are again indicative of a very busy segment whose throughput could be increased by further segmentation.

Received Error Discard. A frame was received with an FCS and/or alignment error. A high count here, relative to total received frames, is indicative of a noisy media subject to errors.

Loss Carrier Count. This is a count of transmitted frames which are lost due to a loss of carrier. This is indicative of poor quality/noisy wiring or adapter cards.

Received Late Collision, Transmitted Late Collisions. A late collision is a collision which occurs in a frame when more than 64 bytes have been received/transmitted. On a correctly configured network, which doesn't exceed physical limits of size, impedance, station spacing, etc., stations should always collide within 64 bytes due to propagation times. Late collisions indicate that the network is violating such restrictions or some stations are having a problem which prevents them correctly implementing the CSMA/CD protocol. For example, a station with a faulty receiver can not "hear" transmissions in progress and so may fail to defer its transmissions causing late collisions to be seen by other stations.

Received Jabbers, Received Over Size. The maximum frame size on Ethernet is 1518 bytes. Frames longer than this are illegal. When such a frame has a valid FCS it is counted as over-size. If it has an FCS error then it is counted as a Jabber. The former is indicative of a device with improper software, the latter of a device with some hardware fault on its transmitter. In both cases the faulty station causes other devices, such as this port, to see these errors.

Drop Event Count. When a frame is dropped, for example, frame reception is aborted because of lack of buffers, there may be only one or there may be many frames so affected. In either case there is a single occurrence of an "event" during which frames were lost. This is what this statistic counts. This statistic is used in RMON as follows. For example, at network start up there may be a huge amount of flooded traffic leading to much lost traffic. When a network administrator subsequently looks at the statistics they might see 2 million frames transmitted with 5000 frames lost. At that point they have no clue as to when and why those 5000 frames were lost. If drop event is 5000 it may indicate an intermittent problem where single frames are being lost. If drop event is 5 or 6 it might indicate a few events when large numbers of frames were lost such as in our example, the network restart.

Received 1024 +, Received 512 +, Received 256 +, Received 128 +, Received 65 +, and Received 64. These count the number of frames in the indicated frame sizes: **Received 64** counts 64 byte frames, **Received 65+** counts frames between 65 and 127 inclusive, **Received 128+** counts between 128 and 255, etc. These statistics are only applied to received frames.

◆ Note ◆

The **Received 1024 +, Received 512 +, Received 256 +, Received 128 +, Received 65 +, and Received 64** fields will always display zero for Gigabit ports.

Port Filtered. On shared media ports, Station A transmitting to Station B will be directly delivered. Therefore, the frame received by this port just needs to be dropped. This action is referred to as filtering and this counts the number of frames so filtered.

Vlan Filtered. The OmniSwitch restricts traffic above the normal Level 2 filtering by applying VLAN rules. Frames which are dropped because of VLAN rules are counted here.

Mtu Exceeded. This statistic is not currently supported and is always zero.

Displaying Token Ring Switch Statistics

In Release 3.4 and later, you can display statistics for the new generation of Token Ring modules known as “Bigfoot” (e.g., TSM-CD-16W, TSX-CD-16W, and TSX-C-32W). For example, if you want to display the switch statistics for a Token Ring port on Port 1 on Slot 4, enter:

```
swch 4/1
```

at the system prompt. Press **r** and then press **<Enter>** at the prompt. Something like the following displays:

```
n={e,s,2,3},quit,save,(?) : r
  Token Ring Statistics for 4/16 Mbit Token Ring port 4/1/Brg/1

Rx MAC Good Bytes           0      Rx LLC Good Bytes           0
Rx Total Mac Packets        0      Rx Total LLC Packets        0
Rx MAC Errored Bytes        0      Rx LLC Errored Bytes        0
Rx Unicast Packets          0      Tx Unicast Packets          0
Rx Multicast Packets         0      Tx Multicast Packets         0
Rx Broadcast Packets         0      Tx Broadcast Packets         0
Rx Buffer Discards           0      Tx Buffer Discards           0
Rx Error Discards            0      Tx Error Discards            0
Ring Purge Events            0      Ring Purge Packets          0
Beacon Events                0      Beacon Packets              0
Claim Token Events           0      Claim Token Packets         0
Internal Errors              0      Line Errors                  0
Burst Errors                 0      AC Errors                    0
Abort Errors                 0      LostFrame Errors            0
Congestion Errors            0      Frame Copied Errors          0
Frequency Errors             0      Token Errors                 0
Soft Errors                  0      Ring Poll Events            0
Internal Errors              0      NAUN Changes                 0
Received 18_63 byte Pkts     0      Received 64_127 byte Pkts   0
Received 128_255 byte Pkts   0      Received 256_511 byte Pkts  0
Received 512_1023 byte Pkts  0      Received 1024_2047 byte Pkts 0
Received 2048_4097 byte Pkts 0      Received 4096_8191 byte Pkts 0
Received 8K_18000 byte Pkts  0      Received 18000+ byte Pkts   0
n={e,s,2,3},quit,save,(?) : ?
```

Note that the default option is now **r**. If you press **<Enter>**, the switch statistics will be redisplayed.

The fields displayed by the **r** option of the **swch** command for Token Ring are described below.

The first group of statistics are the numbers of bytes transmitted and received. These are useful in working out bandwidth usage by the port. Bad octets are important to count in the total octets count as they consume bandwidth at the expense of useful traffic. To ignore them would lead to mysterious loss of bandwidth in any calculations performed.

Rx MAC Good Bytes. The total number of bytes received in good Media Access Control (MAC) packets. (MAC packets are used for management of the Token Ring network.)

Rx LLC Good Bytes. The total number of bytes received in good Logical Link Control (LLC) packets. (LLC packets are used to transfer data.)

Rx Total MAC Packets. The total number of bytes received in MAC packets.

Rx Total LLC Packets. The total number of bytes received in LLC packets.

Rx MAC Errored Bytes. The total number of bytes received in bad MAC packets.

Rx LLC Errored Octets. The total number of bytes received in bad LLC packets.

The next group of statistics are the types of packets being transmitted and received.

Rx Unicast Packets. The number of packets received on this port whose destination address is a unicast format.

Tx Unicast Packets. The number of packets transmitted on this port whose destination address is a unicast format.

Rx Multicast Packets. The number of packets received on this port whose destination address is a multicast format.

Tx Multicast Packets. The number of packets transmitted on this port whose destination address is a multicast format.

Rx Broadcast Packets. The number of packets received on this port whose destination address is the broadcast address.

Tx Broadcast Packets. The number of packets transmitted on this port whose destination address is the broadcast address.

Note that these statistics merely indicate the format of the destination address of packets transmitted/received on this port, not that the addressed device and/or devices necessarily reside on that port. For example, unknown unicast addressed packets are flooded to many ports.

The next group of statistics are the buffer resource related statistics. The NI board receives packets from the backplane to be transmitted to the network ports and receives packets from the network ports to be transmitted to the backplane. It requires buffers to store these packets in while being transferred across the board in this manner. Under heavy and congested traffic a shortage of buffers or lack of timely access to these buffers may occur. These statistics count these events which are more indicative of the amount of traffic on the board as opposed to this particular port.

Rx Buffer Discards. Due to congestion of traffic from multiple ports on the board, timely access to buffers was not available to receive a frame from the network port and the frame was discarded.

Tx Buffer Discards. Due to a shortage of buffers and/or congestion on the network port, packets received from the backplane destined to this port were dropped.

The next group are also indicative of network segment health but are indicative of ill health and indicate events where a frame is lost.

Rx Error Discards. The total number of errored packets (bad CRC, code violations, invalid frame length, etc.) received by this port that were discarded.

Tx Error Discards. The total number of errored packets exceeding the maximum frame length (MTU exceeded, FIFO underruns, etc.) by this port that were discarded.

The next group describe events that can occur when stations are inserted or removed from a ring.

Ring Purge Events. The total number of times this port enters the ring purge state from the normal ring state.

Ring Purge Packets. The total number of times that this port enters a beaconing state.

Beacon Events. The total number of beacon packets received and transmitted by this port.

Beacon Packets. The number of beacon MAC packets detected by this port.

Claim Token Events. The total number of times that this port enters the claim token state from

the normal ring state or ring purge state to elect a new active monitor.

Claim Token Packets. The total number of claim packets transmitted by this port.

The next group describe error statistics for token, MAC, and LLC packets.

Internal Errors. The total number of times this port detects a recoverable internal error.

Line Errors. The total number of errors caused by problems with the physical links (code violations, Frame Check Sequence (FCS) errors inside a frame).

Burst Errors. The total number errors when this port detects the absence of transmissions for five (5) half-bit timers (burst-five errors).

AC Errors. The total number of token packets with an invalid Access Control (AC) byte.

Abort Errors. The total number of times that this port detects an abort delimiter while transmitting a packet.

LostFrame Errors. The total number of packets that failed to reach their destination after the token ring rotation timer has expired.

Congestion Errors. The total number of packets lost due to the fact that no buffer was available at the destination station.

Frame Copied Errors. The total number of times that a frame has been incorrectly copied by another station on the ring or copied by a station with a duplicate address.

Frequency Errors. The total number of timing errors frames detected by this port that did not contain a proper ring-clock frequency.

Token Errors. The total number of times this port detects that a new token was generated by the Active Monitor on the ring due to a lost token.

Soft Errors. The total number of recoverable errors detected by this port.

The next group describe statistics for changes in ring topology.

Ring Poll Events. The total number of times that this port has learned its upstream neighbor's address and has broadcasted the inserting adapter's address to the port's downstream neighbor.

Internal Errors. The total number of insertion failures.

NAUN Changes. The number of times that the Nearest Active Upstream Neighbor (NAUN) for this port has changed.

The next set of statistics display information on network traffic. These statistics are only applied to received packets.

Received 18_63 byte Pkts. The total number of packets received on this port that were at least 18 bytes (octets) long and less than or equal to 63 bytes long.

Received 64_127 byte Pkts. The total number of packets received on this port that were at least 64 bytes (octets) long and less than or equal to 127 bytes long.

Received 128_255 byte Pkts. The total number of packets received on this port that were at least 128 bytes (octets) long and less than or equal to 255 bytes long.

Received 256_511 byte Pkts. The total number of packets received on this port that were at least 256 bytes (octets) long and less than or equal to 511 bytes long.

Received 512_1023 byte Pkts. The total number of packets received on this port that were at least 512 bytes (octets) long and less than or equal to 1023 bytes long.

Received 1024_2047 byte Pkts. The total number of packets received on this port that were at least 1024 bytes (octets) long and less than or equal to 2047 bytes long.

Received 2048_4097 byte Pkts. The total number of packets received on this port that were at least 2048 bytes (octets) long and less than or equal to 4095 bytes long. [check]

Received 4096_8191 byte Pkts. The total number of packets received on this port that were at least 4096 bytes (octets) long and less than or equal to 8191 bytes long.

Received 8k_18000 byte Pkts. The total number of packets received on this port that were at least 8192 bytes (octets) long and less than or equal to 18,000 bytes long.

Received 18000+ byte Pkts. The total number of packets received on this port that were more than 18,000 bytes long.

Any to Any MAC Translations

The **swchmac** command allows you to view the current frame translation settings for a given MAC address. Follow these steps:

1. Enter **swchmac** and the following prompt displays:

Enter MAC address ([XYZZ:AABBCC] or return for none :

2. Enter the MAC for which you want to view translations. The following prompt displays:

Is this MAC in Canonical or Non-Canonical (C or N) [C] :

3. Enter if the MAC address you entered is expressed in canonical (**C**) or non-canonical format. The default is canonical. A screen similar to the following displays:

Port Translations for Ethernet port 3/4/brg/1

Translation Options:

IP Ethertype	-> Ethertype
IP IEEE 802 SNAP	-> Ethertype
IPX ETHERNET_II	-> 802.3
IPX ETHERNET_802.3	-> 802.3
IPX ETHERNET_802.2/FDDI/TOKEN_RING	-> 802.3
IPX ETHERNET_SNAP/FDDI_SNAP/TOKEN-RING_SNAP	-> 802.3
Proprietary Token Ring IPX Switching	-> Off

The screen shows how each incoming frame type is translated. The frame type in the left column indicates the incoming frame type, and the frame type in the right column (after the ->) indicates the outgoing frame translation.

Default Autoencapsulation

Autoencapsulation is a technique employed by AutoTracker software to learn the protocol and encapsulation type used by a source MAC address and automatically translate frames bound to that MAC address to the appropriate encapsulation type.

Normally all devices attached to a switch port receive frames translated according to the translation options defined for that port. However, some devices attached to the same port may require different frame formats.

For example, one workstation may support IPX 802.3 frames and another may support IPX SNAP frames. The switch port may be configured to translate incoming IPX 802.3 frames to LLC frames, which would not satisfy either of the workstations. If autoencapsulation is on, then the switch would translate frames for the first workstation to IPX 802.3 and frames for the second workstation to IPX SNAP. The translation setting for the port is overridden for those ports that require a special translation.

Autoencapsulation operates only on learned unicast frames. It does not work for broadcast, multicast, or unlearned unicast frames. For this reason it is recommended only for ports attached to client devices. It is not recommended for ports attached to servers due to high volume of broadcast traffic on such a connection.

In addition, autoencapsulation is not supported for Banyan Vines frames. It operates only on IP and IPX frames.

To turn on autoencapsulation type the following at the prompt:

```
autoencaps on
```

To turn off autoencapsulation type the following at the prompt:

```
autoencaps off
```

Translational Bridging

Translational Bridging enables internetworking between FDDI, Ethernet, and Token Ring LANs. There is no standard which encompasses this. The OmniSwitch's features focus on bridging of frames between media and translating the MAC and LLC headers into the appropriate "native" frame formats. This provides media-independent internetworking.

Learning

For VLAN trunk frames, the switch will learn the source MAC address of the encapsulated frame and associate this with the source MAC address of the originating switch. When a frame arrives, the switch checks to see if the frame has been learned. If so, then the frame will be encapsulated and sent directly to the destination switch. If not, then the switch will learn the association of VLAN, trunk service, virtual port, source, and destination MACs. If the switch has no ports in the VLAN associated with the frame's destination, the frame is dropped.

Translations across Trunks

The OmniSwitch sends frames onto the trunk in the same format as the original LAN type. Any required translation is done at the destination switch.

Dissimilar LAN Switching Capabilities

Switching traffic between like media requires no changes to the frame, whereas switching traffic between unlike media requires some level of change to the frame. To fully explain the various changes possible we need to define the portion of the frame where changes could occur.

Media Specific fields and MAC address fields are different for Token Ring, FDDI, and Ethernet. For Token Ring and FDDI, the switch generates MAC addresses in non-canonical format, where Ethernet generates MAC addresses in canonical format. The OmniSwitch will perform media translations which means the media specific, source MAC and destination MAC will be changed for each frame which changes media.

The source routing field is optional, and use of this field is driven by endstations who wish to communicate using source routing. The OmniSwitch participates in source routing on FDDI and Token Ring interfaces when it is configured as a Source Route Bridge. The OmniSwitch will also forward source route frames transparently while performing standard switching of frames on Token Ring and FDDI interfaces as well as when using the virtual ring feature.

The encapsulation type field can be a number of different encapsulations, which really includes the Media Specific fields, source MAC address, and destination MAC address. The choices are Ethernet II, IEEE 802.2 (LLC), SNAP, and Novell 802.3 or FDDI proprietary formats. There are configuration options for Ethernet, FDDI, and Token Ring interfaces. The encapsulation type field may or may not be changed. This decision is made based on the incoming encapsulation type, the user configuration, and the topology that frame is traveling.

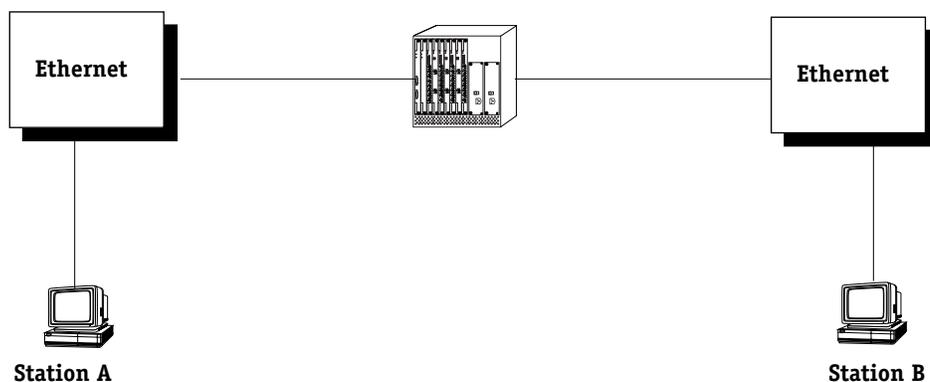
The data field is the remainder of the frame which is application dependent. This data field is not changed for switched traffic. Each frame is followed by a CRC.

Below are some examples when translation can occur.

Switching Between Similar LANs

Translations are not performed for switched traffic between similar LANs within one OmniSwitch. For example in the diagram below, if Station A on an Ethernet segment wants to talk to Station B on another Ethernet segment, the switched frames are not changed.

This is true for any two media where the originating media and the destination media are of the same type (i.e. Ethernet, FDDI, Token Ring).

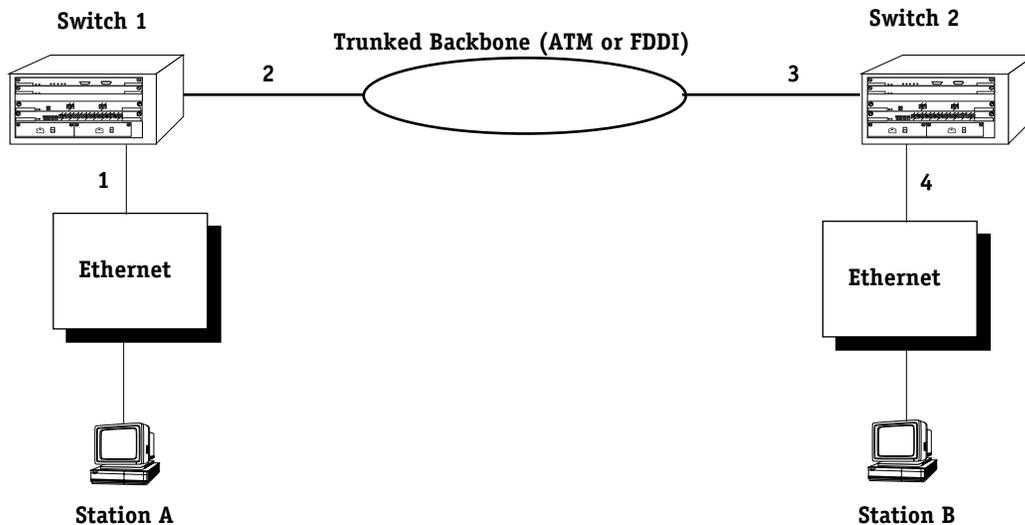


Similar LANs

Switching Between Ethernet LANs Across a Trunked Backbone

Frames that are switched between like media across a Trunked backbone will only be translated at the egress port of the egress OmniSwitch. For example in the figure below, frames switched from Station A to Station B will be translated at point 4, where point 4 is the egress port of Switch 2. Frames switched from Station B to Station A will be translated only at point 1, where point 1 is the egress port of Switch 1.

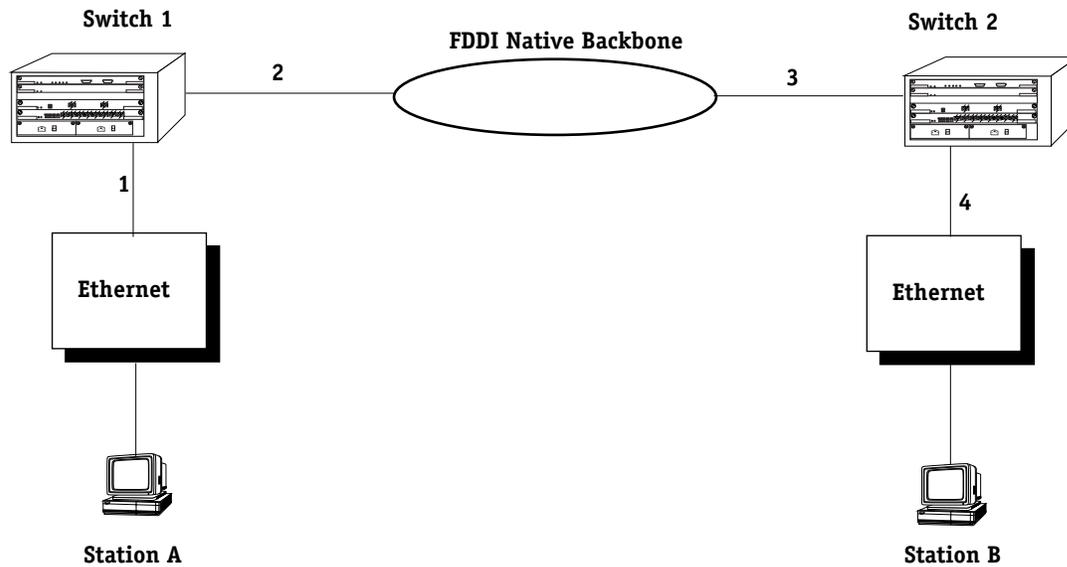
This is true if the originating media and destination media are Ethernet. It is not true if the originating media and destination media are either Token Ring or FDDI.



Ethernet LANs Across a Trunked Backbone

Switching Between Similar LANs across a Native Backbone

Switched traffic between similar LANs across a non-trunked or native backbone will have translations performed at each egress point. In the figure below, for traffic originating from Station A destined to Station B, point 1 represents the ingress (input) port of Switch 1. Likewise, point 2 represents the egress (output) port of Switch 1, point 3 represents the ingress (input) port of Switch 2 and the point 4 represents the egress (output) port of Switch 2. Translations will occur at points 2 and 4. For traffic from Station B to Station A, output translations will occur at points 3, and 1.



Similar LANs Across a Native Backbone

In the above example, the backbone could be of any media type other than Ethernet. If all three media types were Ethernet, then no translations would occur, because the traffic is being switched from like media to like media.

Dissimilar LAN Switching Capabilities

The following table shows interoperability between dissimilar LANs with two switches where the client and server are resident on like media types and the connection is switched over various LAN backbone types. This table is representative of the IP and IPX protocol only.

	<i>Backbone</i>			
	<i>Token Ring</i>	<i>FDDI</i>	<i>Ethernet</i>	<i>ATM</i>
<i>Token Ring to Token Ring</i>	No	Yes	Yes	No
<i>FDDI to FDDI</i>	Yes	No	Yes	No
<i>Ethernet to Ethernet</i>	Yes	Yes	No	No

Dissimilar LANs

24 Managing Groups and Ports

In a traditional hub-based network, a broadcast domain is confined to a single network interface, such as Ethernet or Token Ring, or even a specific physical location, such as a department or building floor. In a switch-based network, such as one comprised on OmniSwitches, a broadcast domain—or *Group*—can span multiple physical switches and can include ports using multiple network interfaces. For example, a single OmniSwitch Group could span three different switches located in different buildings and include Ethernet, Token Ring, ATM and WAN physical ports.

An unconfigured OmniSwitch or Omni Switch/Router contains one Group, or broadcast domain. It also contains one default Virtual Network, or VLAN, referred to as “default VLAN #1”. The default Group, Group #1, and its default VLAN contain all physical ports in the switch. When a switching module is added to the switch all of these additional physical ports are also assigned to Group #1, VLAN #1.

You can create Groups in addition to this default Group. When you add a new Group, you give it a name and number, optionally configure a virtual router port for its default VLAN, and then add switch ports to it. The switch ports you add to a new Group are moved from the default Group #1 to this new Group. (For more information on how ports are assigned to Groups, see *How Ports Are Assigned to Groups* on page 24-2.)

Up to 500 Groups can be configured on each OmniSwitch. An entire OmniSwitch network can contain up to 65,535 Groups. Each Group is treated as a separate entity.

There are three main types of Groups:

1. **Mobile Groups.** These groups allow ports to be dynamically assigned to the Group based on AutoTracker polices. In contrast to non-mobile Groups, AutoTracker rules are assigned directly to a mobile Group. No AutoTracker VLANs are contained within a mobile Group. (However, mobile groups do contain a default VLAN 1 to which AutoTracker policies are assigned; policies assigned to this default VLAN apply to the entire mobile group.) Any AutoTracker policy may be used as criteria for membership in a mobile Group. Mobile groups are described in more detail in *Mobile Groups* on page 24-5.
2. **Mobile Groups based on authentication.** Authenticated Groups are a special form of mobile Group. These Groups include devices that are dynamically assigned based on an authentication criteria. Typically the user will have to log in with a valid password before being included in an authenticated mobile Group. Group membership is based on users proving their identity rather than the physical location of user devices. Authenticated Groups are described in more detail in the *Switch Network Services User Manual*.
3. **Non-mobile Groups.** These Groups are the original Group type used in previous releases. They contain statically assigned ports and may contain AutoTracker or Multicast VLANs. These VLANs within a non-mobile Group use AutoTracker policies to filter traffic. AutoTracker rules are not assigned to non-mobile Groups, they are assigned to the VLANs within the Group. Non-mobile groups are described in more detail in *Non-Mobile Groups and AutoTracker VLANs* on page 24-18.

All three types of Groups may co-exist on the same switch. However, a switch port cannot belong to a non-mobile group and a mobile group.

How Ports Are Assigned to Groups

There are two methods for assigning physical OmniSwitch ports to a Group. One method is static and requires manual configuration by the network administrator; the other method is dynamic and requires only the configuration of AutoTracker rules for port assignment to occur. The two methods are described in this section.

Static Port Assignment

In the static method, the network administrator manually assigns a port to a Group through the **crgp** and **addvp** commands. The static method can be restrictive because it limits the mobility of users in a multi-Group network. Users can only move within their assigned Group. In addition, customized access for individual users is limited by this method. You can use the static method of port assignment with mobile and non-mobile groups. Static port assignment can be combined with dynamic port assignment for mobile groups, while static port assignment is the only method for assigning ports to non-mobile groups.

Dynamic Port Assignment (Group Mobility)

The dynamic method is available with the Group Mobility feature. Initially each port is part of the default Group #1 (only ports in the default Group and ports in mobile Groups are candidates for dynamic port assignment). Based on the nature of traffic and configured AutoTracker policies, ports are dynamically assigned to the appropriate Group.

For example, if a device attached to a port transmits traffic from the 140.0.0.0 subnet, AutoTracker will check to see if a policy exists for this IP address. If it does, then it will move the port from the default Group to the first Group using this policy. If this device detaches from the network the port will be re-assigned to a Group without intervention by the network administrator.

A port can belong to multiple mobile groups (up to 16) as long as devices attached to that port match policies of these mobile groups. However, an individual device, or MAC address, can only belong to one mobile group per protocol.

The dynamic method of port-to-Group assignment still requires the creation of Groups through the **crgp** command. The criteria for the dynamic assignment of ports to a Group are determined by AutoTracker policies that you can configure during the **crgp** procedure.

Only Ethernet and Token Ring ports can be dynamically assigned to Groups.

If more than one Group has the same type of rule, then ports matching that policy will be assigned to the first Group matching the policy. For example, if a device matched policies in both Groups 2 and 5, the port would be assigned to Group 2. To make the most out of Group Mobility it is best not to duplicate policies among Groups.

Configuring Dynamic Port Assignment

You can enable dynamic port assignment while creating a group through the **crgp** command. During the **crgp** procedure, you will be prompted

Enable Group Mobility on the Group ? [y/n] (n):

Answer **Yes** to this question to give this Group the capability of having ports and devices dynamically added to the Group. Port and devices will be dynamically assigned based on AutoTracker rules you define.

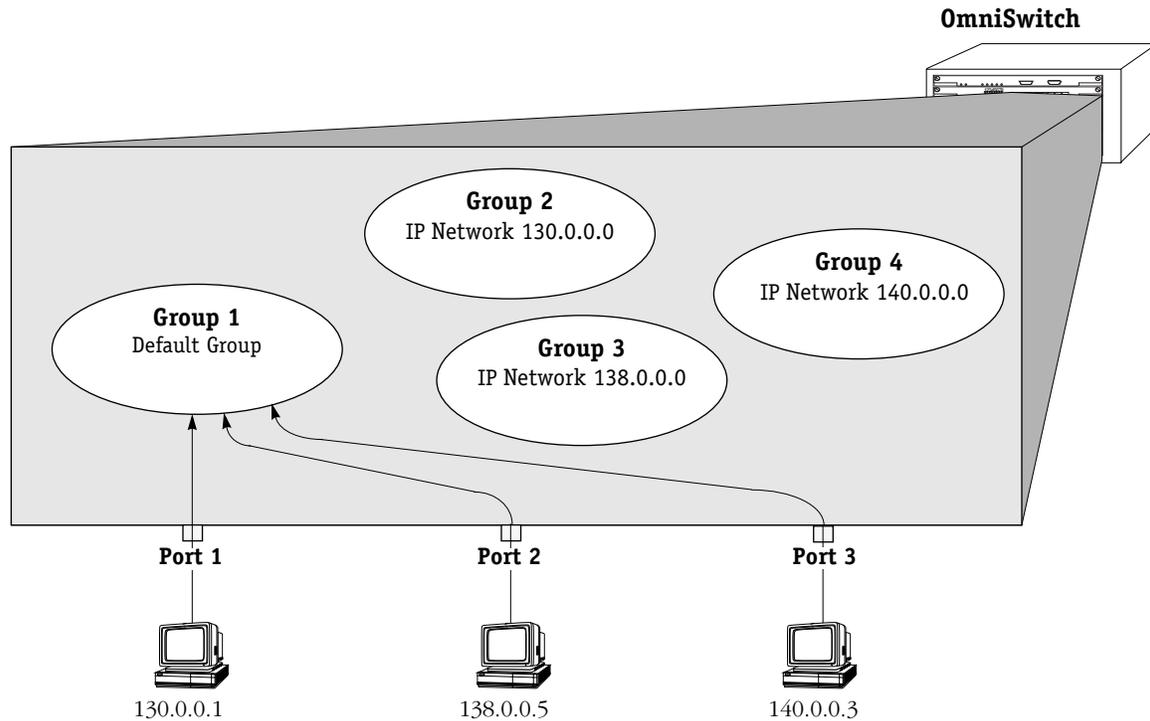
Service Ports and Group Mobility

Dynamic port assignment (ports carrying Ethernet and Token Ring traffic only) to Groups can also apply to LANE service ports configured for ATM access. These ports may be automatically added to the mobile group during the **crgp** procedure or through the **cats** command.

How Dynamic Port Assignment Works

Initially each port is assigned to the default Group. In this example, all three ports have workstations that belong to three different IP subnets (130.0.0.0, 138.0.0.0, and 140.0.0.0). All three ports start out in the default Group.

Group Mobility examines traffic coming from OmniSwitch ports. Three mobile groups are defined on the switch and each uses a different IP policy. Traffic that matches IP policies for a Group will trigger the movement of the port to the matching Group.



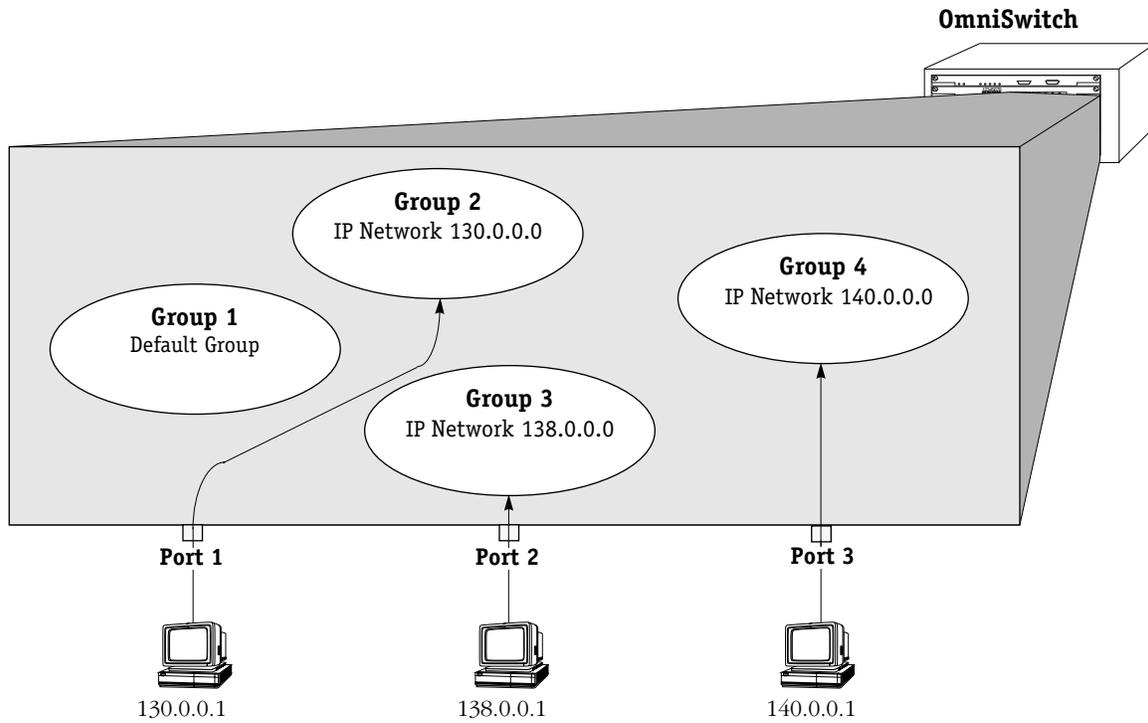
Initial Configuration: All Ports in Default Group

As soon as the workstations start transmitting traffic, Group Mobility checks the source subnet of the frames and looks for a match with any configured IP policies. If a match is found—and in this example all three ports can be matched with a corresponding Group—the port is moved to the matching Group.

Devices matching a policy trigger the assignment of a port to a mobile group. Therefore, the device is moved to the mobile group at the same time as the port to which it is attached. If more than one device comes in on a port, then that port can belong to more than one mobile group. Similarly, if a device transmits more than one protocol—such as IP and IPX—then the port to which it is attached can belong to more than one mobile group.

How Ports Are Assigned to Groups

As the illustration below shows, the three ports are each moved from the default Group to a Group with a policy that matches the subnet address of the workstation attached to the port. AutoTracker IP address policies have been set up in Groups 2, 3, and 4. The ports are moved to the Group with policies matching the subnet of the workstation.



Ports Move to Groups With Matching Policies

Mobile Groups

Switch ports can be dynamically assigned to mobile groups through AutoTracker policies. Support for dynamic port assignment is one of the main differences between mobile groups and non-mobile groups. AutoTracker rules are assigned *directly* to a mobile group. In contrast, AutoTracker rules are assigned to the VLANs *within* a non-mobile group. No AutoTracker VLANs are contained within a mobile Group, and each mobile group constitutes a single spanning tree.

A switch port can belong to multiple mobile groups, whereas a switch port can belong to only one non-mobile group. However, a port can *not* belong to a mobile and a non-mobile group at the same time.

Ports can be assigned to mobile groups either statically or dynamically. A port is *statically* assigned to a mobile group when one of the following occurs:

- Port by default assigned to default group 1
- Port assigned to a group through **crgrp** or **addvp** commands

Although switch ports can belong to multiple mobile groups, it is not possible to assign a port to two different groups using the **addvp** command. However, a switch port could be assigned to one mobile group via the **addvp** command and then gain membership to another mobile group by matching the policy criteria for that group.

A switch port is *dynamically* assigned to a mobile group after one of its attached devices matches an AutoTracker policy for that mobile group. An overview of how ports and devices are dynamically assigned to mobile Groups can be found in *How Ports Are Assigned to Groups* on page 24-2.

Dynamic LANE Services

Another feature of mobile groups is their support for dynamic LAN Emulation services. By specifying the ELAN name and the ATM port number of a LANE service, the LANE service will be brought up automatically as soon as Ethernet/Token Ring traffic is received from an Ethernet or Token Ring device. Dynamic LANE services are described in *Dynamic LANE Services* on page 24-15.

Authenticated Groups

Mobile groups provide the added flexibility of user-authentication policies. Using Authentication Management Console (AMC) software, you can configure mobile groups to use log-in procedures as a means of assigning group membership. Mobile groups that use authentication are a special group type called an Authenticated Group. Authenticated Groups are described in more detail in the *Switch Network Services User Manual*.

Configuring Mobile Groups

You configure mobile Groups through the **crgrp** command. During the **crgrp** procedure you will receive a prompt asking if you want to create a mobile Group

Enable Group Mobility on this Group ? [y/n] (n):

You must answer **Yes** to this prompt to set up a mobile group. After this question, you will be asked to configure virtual ports and AutoTracker policies for the Group. Documentation for the full **crgrp** procedure can be found in *Creating a New Group* on page 24-21.

Turning Group Mobility On or Off

The **gmstat** command turns group mobility on or off for a Group that you specify. Essentially, you can change a non-mobile group into a mobile group and a mobile group back into a non-mobile group through **gmstat**. The group you specify must previously have been created through the **crgp** command.

Use the following syntax for the gmstat command:

```
gmstat <group number>
```

For example, if you wanted to change the group mobility status of group 2, you would enter:

```
gmstat 2
```

Mobile Group to Non-Mobile Group

If this group is already a mobile group, the following would display:

```
Group Mobility is ON for Group 2  
Change Group Mobility Status for Group 2 to OFF ? [y/n] (y):
```

If you wanted to change this mobile group back to a non-mobile group, you would press **<enter>** and the group would lose its mobile status. All AutoTracker policies you set up for the Group would no longer be valid.

If you decided not to turn off group mobility, enter **n** and the following prompt displays:

```
Group Mobility Status unchanged
```

Non-Mobile Group to Mobile Group

If this group is currently a non-mobile group, the following would display:

```
Group Mobility is OFF for Group 8  
Change Group Mobility Status for Group 8 to ON ? [y/n] (y):
```

If you wanted to turn on Group Mobility, you would press **<enter>** and would then be asked if you want to configure AutoTracker policies. If you answer yes, then the AutoTracker policies menu would display as follows:

```
Select rule type:  
1. Port Rule  
2. MAC Address Rule  
    21) MAC Address Range Rule  
3. Protocol Rule  
4. Network Address Rule  
5. User Defined Rule  
6. Binding Rule  
7. DHCP PORT Rule  
8. DHCP MAC Rule  
    81) DHCP MAC Range Rule
```

```
Enter rule type (1):
```

You define policies for a mobile Group. Non-mobile groups do not require policies. However, mobile Groups use policies to define membership. Instructions for specifying AutoTracker policies may be found in Chapter 27.

◆ Note ◆

As of the current release, the MAC Address Range Rule and DHCP MAC Range are not supported for AutoTracker VLANs

After you configure rules for the mobile group, you will be given the option to configure a dynamic LANE service. A description of this service is provided on page 24-15.

If you decided not to turn group mobility on, you would enter **n** at the group mobility prompt and the following message would display:

Group Mobility Status unchanged

Understanding Port Membership in Mobile Groups

Switch ports can belong to multiple mobile groups. A port becomes a member of a mobile group as long as one of its attached devices matches the policy criteria for that group. However, the movement of ports between groups and the status of port membership in groups can be affected by more than just whether or not devices match policy criteria.

Group mobility uses three variables that can affect a port's default group and whether or not a port ages out of a group. These variables are as follows: `def_group`, `move_from_def`, and `move_to_def`. The `def_group` and `move_to_def` variables can be configured through the **gmcfg** command, which is described on page 24-12. The `move_from_def` variable is enabled by default, but can be disabled by entering a statement in the **mpm.cmd** file. The effects of these three variables are described through diagrams on the following pages.

From the perspective of a device or switch port, there are three types of mobile group—default, primary, and secondary. Keep in mind that definitions of these three types are relative and can change for each port and device depending on the settings of the group mobility variables and traffic patterns of devices.

Default Group

The default group is the group a port or device is statically assigned to by “default.” Typically, a port's default group will be Group 1. A port can also be statically assigned to its default group through the **crgp** or **addvp** commands. A port or device does not have to match a policy to gain membership into its default group.

The default group for a port or device is stored in memory; it can only be manually changed through the **addvp** or **crgp** commands. Depending on the settings of other group mobility variables a device or port can age out of other mobile groups but still remain a member of its default group.

Primary Group

The primary group is the group upon which Spanning Tree operations converge. The primary group is similar to the default group. There are two main differences between a primary and a default group.

1. A primary group only contains devices that have matched one of its AutoTracker policies. In contrast, switch ports may end up in a default group without matching any policy.
2. It is possible for the primary group of a port or device to change through learning or aging. For example, if the `move_from_def` variable is enabled and a device matches the policies of a mobile group other than its default group, then this new mobile group becomes the primary group for the device and the port to which the device is attached (see diagram on page 24-10). In this case the default group and primary group will be different.

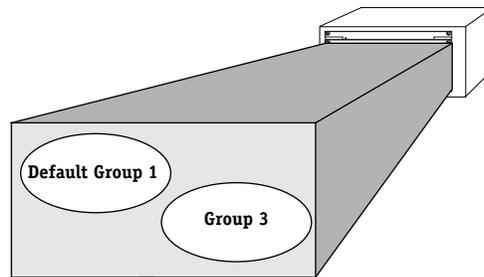
If the `move_from_def` is disabled, the port always remains in the default group (which can now also be the primary group).

In addition a port can age out of its primary group if the `move_to_def` variable is enabled (see diagram on page 24-11). A port cannot age out of its default group.

Secondary Group

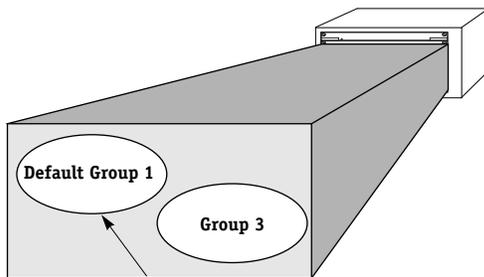
Switch ports and devices may become members of multiple mobile groups. A switch port starts in its default group, which initially is also its primary group. The primary group may change if the `move_from_def` variable is enabled. Any subsequent mobile groups to which a port gains membership beyond the primary group are “secondary” mobile groups. A port can age out of these secondary groups if the `move_to_def` variable is enabled (see diagram on page 24-11).

How a Device Is Dropped from the Default Mobile Group (def_group)



Device sends traffic that is forwarded to the MPM for processing. If the traffic matches the policies of an existing mobile group, then it will become a member of that group. If the device does not match the policies of any mobile group, then the `def_group` variable determines whether that device becomes a member of the default group.

If `def_group` is enabled....



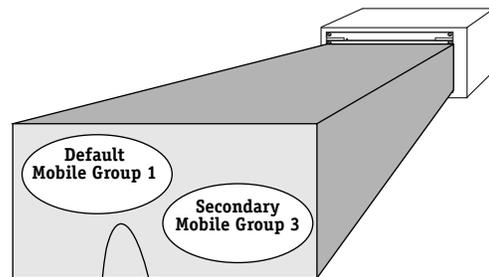
The device that does not match any policies becomes a member of the default group.



Why enable `def_group`?

- Ensure that all network devices will be a member of at least one mobile group.

If `def_group` is disabled....



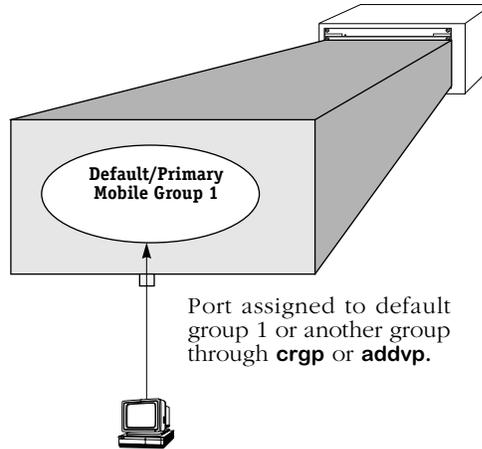
All traffic from the device that does not match any policies is dropped. The device is not a member of any mobile group, including the default mobile group.



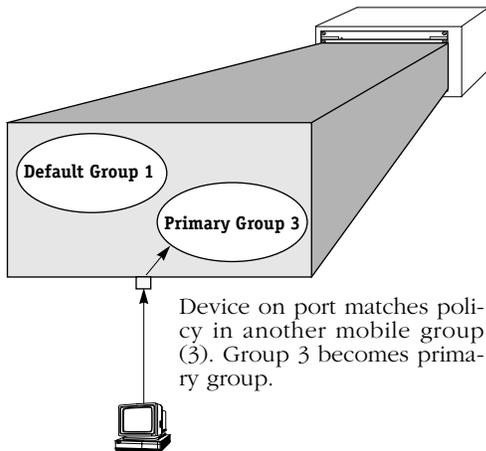
Why disable `move_from_def`?

- Reduces traffic to and from devices that do not satisfy any network policies.

How a Port's Primary Mobile Group Changes (move_from_def)



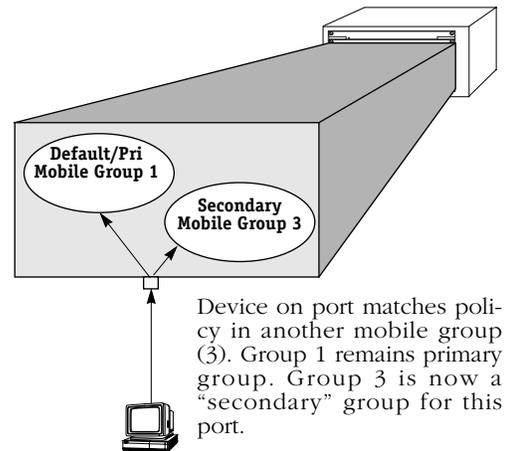
If move_from_def is enabled....



Helpful Hints:

- Reduces broadcasts to the default group.
- Best used when only one device is attached to each port.

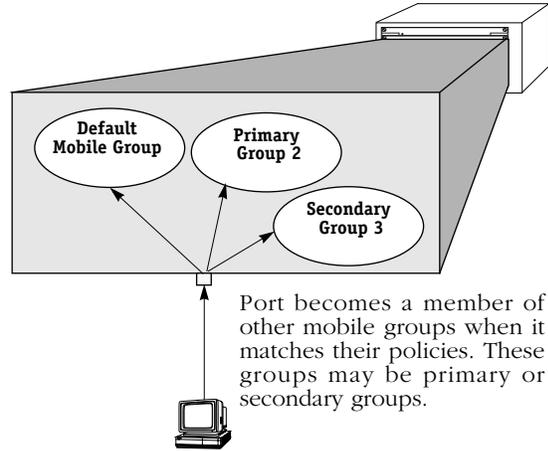
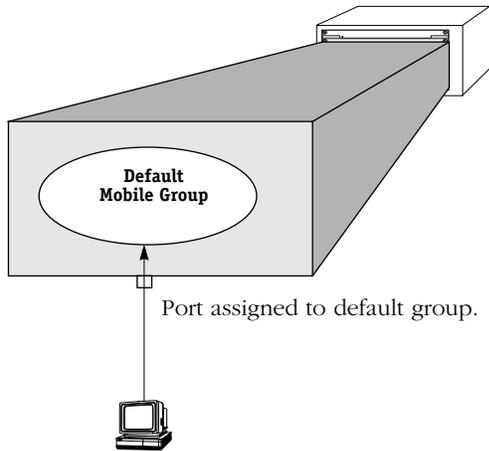
If move_from_def is disabled....



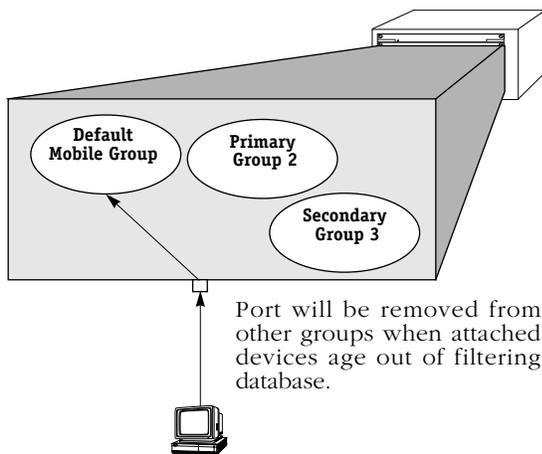
Why disable move_from_def?

- When multiple devices are attached to the switch port, the port must support multiple traffic in the default group as well as traffic in the secondary mobile groups.

How a Port Ages Out of a Mobile Group (move_to_def)



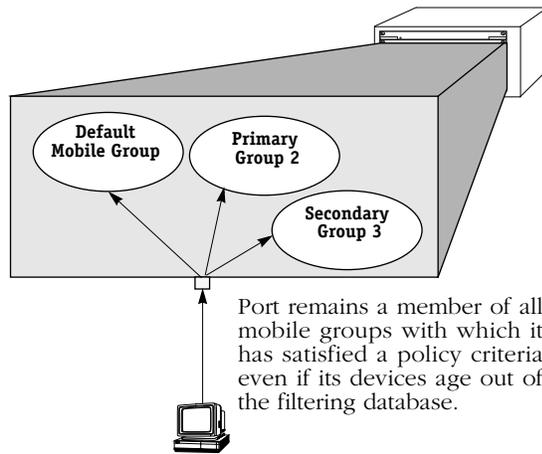
If move_to_def is enabled....



Why enable move_to_def?

- Security. Mobile groups only contain devices and ports that have recently matched policy criteria.

If move_to_def is disabled....



Why disable move_to_def?

- Switch ports retain group membership even when idle for some time. May be appropriate for silent devices, such as printers.

If the port is in “optimized mode,” then the MAC does not age out and the port would stay in the mobile group even if move_to_def is enabled.

Configuring Switch-Wide Group Mobility Variables

There are several switch-wide group mobility variables that you can configure through the **gmcfg** command. These variables control the status of group mobility on all groups in a switch as well as the use of the default group. These variables are illustrated through diagrams on pages 24-9 to 24-11.

Follow these steps to use the **gmcfg** command:

1. Enter **gmcfg**. You do not need to specify a group number as this command applies to all mobile groups in this switch.
2. The following prompt displays:

Group Mobility is Enabled. Disable Group Mobility ? [yes/no] (no) :

This prompt controls the status of group mobility in this switch. If you disable group mobility here then mobile groups will not be supported in this switch even if they are configured through the **crgp** command.

Default Group 1. When group mobility is enabled, default group 1 in the switch will be treated as a mobile group and you will not be able to create AutoTracker VLANs within this group. When group mobility is disabled, default Group 1 in the switch will be treated as a non-mobile group in which AutoTracker VLANs could be created.

The default is to turn Group Mobility off. If you want to enable group mobility, then you need to indicate that choice at this prompt. The prompt will always show the current status of Group Mobility and then ask if you want to change that status. If you want to change the current status, then enter a **y** at this prompt and press **<enter>**. To keep the current status, simply press **<enter>**.

3. The following prompt displays:

move_to_def is set to Disabled. Set to Enable ? [yes/no] (no) :

The **move_to_def** variable determines what happens to a port once the devices on that port age out of the filtering database. By default this variable is Disabled, which means that a port will remain a member of a mobile group as long as its attached device satisfied the criteria for membership in that mobile group at one point. If devices on a port stop transmitting, the port will still retain all its mobile group memberships.

If the **move_to_def** variable is Enabled, then a port will lose its membership in a mobile group if its devices age out of the filtering database for that mobile group (i.e., they stop transmitting traffic that satisfies the criteria for membership in the mobile group). Once a port loses membership in all criteria-based mobile groups, it will return to its default group. The effect of this variable is illustrated on page 24-11.

By default, the **move_to_def** variable is Disabled. If you want to enable it (ports lose mobile group membership when they age out), then you need to indicate that choice at this prompt. The prompt will always show the current status of **move_to_def** and then ask if you want to change that status. If you want to change the current status, then enter a **y** at this prompt and press **<enter>**. To keep the current status, simply press **<enter>**.

4. The following prompt displays:

def_group is set to Enable. Set to Disable ? [yes/no] (no) :

The **def_group** variable determines what happens to devices that do not match any mobile group policies. If **def_group** is Enabled (the default), then devices that do not match any mobile group policies will be part of the default group for that port. If the **def_group** variable is Disabled, then devices that do not match any mobile group policies will be dropped from their default group and will not be part of any mobile group.

By default the `def_group` variable is Enabled. If you want to disable it (devices that do not meet criteria for mobile group membership will not be part of any mobile group), then you need to indicate that choice at this prompt. The prompt will always show the current status of `def_group` and then ask if you want to change that status. If you want to change the current status, then enter a **y** at this prompt and press **<enter>**. To keep the current status, simply press **<enter>**.

The `move_from_def` Variable

The `move_from_def` variable controls whether or not a port's primary group can differ from the port's default mobile group. This variable is enabled by default, but can be changed to disabled in the `mpm.cmd` file.

The original default group for a port is group 1 or the group to which the port is assigned through the `crgp` or `addvp` commands. The primary group at this point is the same as the default group. However, if the `move_from_def` variable is enabled, the primary group can change as soon as a device on the port matches the policy criteria for another mobile group.

For example, Port 5 may start out in Group 1, its default group. The primary group in this case will also be Group 1. If the `move_from_def` variable is enabled and Port 5 matches AutoTracker policies for mobile group 3, then the new primary group for Port 5 will be Group 3. All further Spanning Tree operations for the port will converge on group 3 rather than group 1. The effects of the `move_from_def` variable are further illustrated through diagrams on page 24-10.

If you disable the `move_from_def` variable, then the primary group for a port will always match the default group regardless of the number of other mobile groups to which it gains membership. To disable the `move_from_def` variable, enter the following statement in the `mpm.cmd` file

```
move_from_def=0
```

For this new setting to take place you need to reboot the switch.

Viewing Ports in a Mobile Group

The **vpl** command lists all the Groups in the switch currently configured as mobile Groups and the ports currently assigned to those Groups. Since ports are assigned to mobile groups dynamically, this display is helpful to find out which ports the switch already sees in each group. Ports will only display in this screen for secondary groups (i.e., not default or primary groups). Enter **vpl** and a screen similar to the following displays:

```

=====
Group ID      Physical Port      Virtual Port
=====
Group ID: 2   4/2 4/3 4/4 4/5   12 13 14 15
Group ID: 3   3/1 5/2           8 20
Group ID: 6   NULL Port List
Group ID: 8   4/1 5/1           11 19

```

Group ID. The group number assigned to this mobile group during the **crgrp** procedure.

Physical Port. The physical switch ports that have been dynamically assigned to this group because they matched an AutoTracker policy. (Primary groups do not display in this screen. For a display of port-to-primary group mappings, use the **vi** command) If this column reads **NULL Port List**, then no physical ports have been assigned to the group yet.

Virtual Port. The virtual ports that are part of this mobile group. For Ethernet and Token Ring switch ports, there is a one-to-one relationship between physical and virtual ports. For ATM ports, multiple virtual ports may be associated with one physical port.

Viewing a Port's Mobile Group Affiliations

The **vigl** command lists all the ports in the switch that have been assigned to mobile Groups. It is similar to the **vpl** command, but it lists ports first and then Groups. Since ports are assigned to mobile groups dynamically, this display is helpful to find out which ports the switch already sees in each group. Ports will only display in this screen for secondary groups (i.e., not default or primary groups). Enter **vigl** and a screen similar to the following displays:

```

=====
Virtual Port  Physical Port      Group ID
=====
12 13 14 15  4/2 4/3 4/4 4/5   Group ID: 2
8 20         3/1 5/2           Group ID: 3
NULL Port List
11 19       Physical Port      Group ID

```

Virtual Port. The virtual ports in this mobile group. For Ethernet and Token Ring switch ports, there is a one-to-one relationship between physical and virtual ports. For ATM ports, multiple virtual ports may be associated with one physical port.

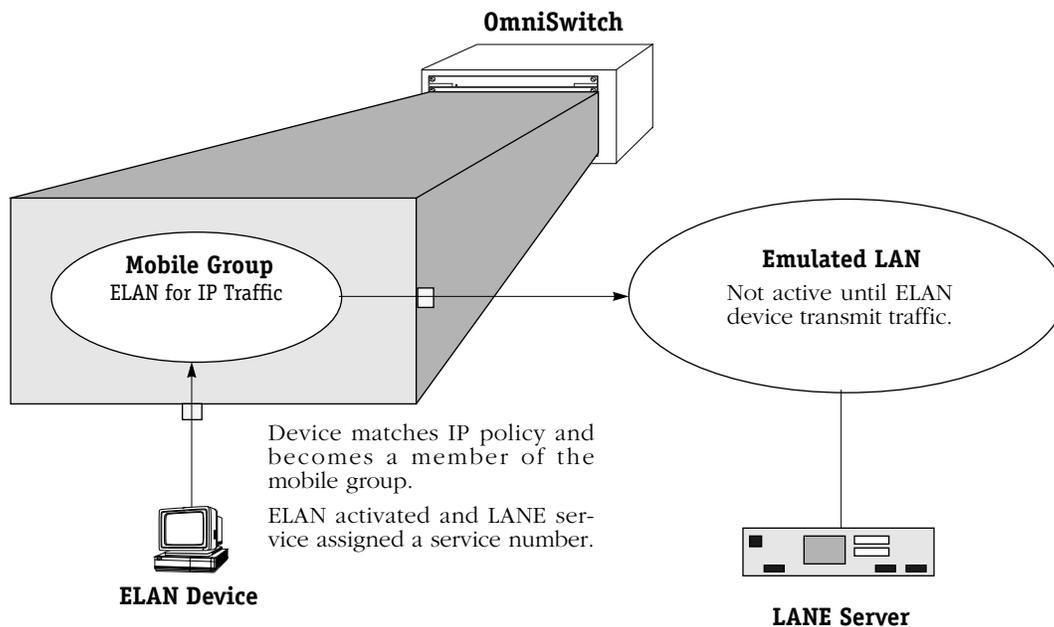
Physical Port. The physical switch ports that have been dynamically assigned to this secondary mobile group because they matched an AutoTracker policy. (Primary groups do not display in this screen. For a display of port-to-primary group mappings, use the **vi** command) If this column reads **NULL Port List**, then no physical ports have been assigned to the group yet.

Group ID. The group number assigned to this mobile group during the **crgrp** procedure.

Dynamic LANE Services

Mobile groups allow you to create dynamic LAN Emulation (LANE) services, which can be a powerful tool in reducing configuration time and LANE broadcasts. By configuring a dynamic LANE service within a mobile group, you enter basic configuration information for the ELAN but the ELAN is not activated until one of the attached devices sends traffic.

Normally when you create a LANE service (through the **cas** command) all switch ports in the associated group receive all broadcasts associated with an ELAN. Even switch ports with no devices currently active in an ELAN will receive these broadcasts. However, when you create a dynamic LANE service the service is not activated until a switch port receives traffic from a member device.



How a Dynamic LANE Service is Activated

Dynamic LANE services function the same way as standard LANE services created through the **cas** command. The difference is that they are only activated when traffic is sent by an Ethernet or Token Ring device. In this sense, a dynamic service can be considered an on-the-fly version of the **cas** command. Configuration information on the ELAN is retained, but the service itself is dormant until an Ethernet/Token Ring device transmits data.

Dynamic LANE Services and Non-Dynamic LANE Services

Once an Ethernet or Token Ring device sends data, the LANE service will be activated by the switch and assigned a service number. The service, once activated, can be viewed through the **vas** command or modified through the **mas** command—just like any other ATM service. A way to delete a dynamic LANE service is through the **dats** command, which is described on page 24-16.

The ELAN name configured for the dynamic service cannot be the same as an ELAN configured through the **cas** command. If you create a service through **cas** that uses the same name as a dormant dynamic service, then the dynamic service will not become operational.

Creating Auto-Activated LANE Services

You can add a LAN Emulation service to a mobile group. The LANE service will automatically be created in the mobile group as soon as Ethernet or Token Ring traffic is received. You can add a dynamic service to a mobile Group during the **crgp** procedure (see *Step 5. Configure Auto-Activated LANE Ports (Mobile Groups Only)* on page 24-37) or by using the **cats** command. The LANE service is dormant until traffic occurs, at which time the service is activated and ports are assigned to the service.

Follow these steps to use the **cats** command:

1. Enter **cats**. The following prompt displays

Enter the mobile Group Id:

You can also enter the **cats** command followed by the group number to bypass this prompt.

2. Enter the group number for the mobile group to which you want to assign this LANE service port. The following prompt displays:

Enter the primary slot/interface for this service:

3. Descriptions of this prompt and the remaining **cats** prompts can be found in the **crgp** procedure. Please continue with the section, *Step 5. Configure Auto-Activated LANE Ports (Mobile Groups Only)* on page 24-37.

Deleting an Auto-Activated Service

You can delete any dynamic LANE services that you assigned to a mobile group. These services are assigned through the **crgp** or **cats** commands. You use the **dat**s command to delete these services. Note that the **dat**s command deletes only auto-activated services; it does not delete services created via the **cas** command.

You will need to know the mobile group number and the service number of the auto-activated service before you can delete it. You can obtain the service number through the **vats** command, which is described in *Viewing Auto-Activated Services* on page 24-17.

The **dat**s command uses the following syntax:

dats <group number> <slot>/<port> <service index>

For example, if you wanted to delete the LANE service with an index number of 3 on port 4/2 in mobile group 8, you would enter:

dats 8 4/2 3

The service port is deleted once you enter the command and press **<enter>**. You can obtain the service index number for a dynamic LANE service through the **vats** command.

Viewing Auto-Activated Services

Using the **vats** command, you can obtain a listing of any LANE services that have been assigned to a mobile group. These ports are assigned through the **crgp** or **cats** commands. Note that the **vats** command displays only auto-activated services; it does not show services created via the **cas** command.

When you enter **vats**, a screen similar to the following displays:

Group ID	P. Port S. Port A. Port	Srvc Num	Srvc Index	Admin	Oper	Srvc Type	Service Name
3	3/1	2	1	Enabled	Inactive	LANE	elan1
8	4/2 4/1 4/2	3	1	Enabled	Active	LANE	elan2

Group ID. The mobile group number to which this service is assigned.

P. Port, S. Port, A. Port. This column lists the current primary physical port (**P. Port**), secondary port (**S. Port**), and the current active port (**A. Port**) for this LANE service.

Srvc Num. The internal service number assigned to this service. You will need this number if you want to modify or delete a service through the **mas** or **das** commands, respectively.

Srvc Index. The internal value used by dynamic LANE software to identify this service. The service index differs from the service number in that it is used exclusively by dynamic LANE software. You will need the service index to delete a dynamic service through the **dats** command.

Admin. The current administrative status of the service. When configuring auto-activated services through **crgp** or **cats**, you have the choice to enable or disable the service. If **Enabled**, the service may become operationally active if traffic uses this service and the connection is good. If **Disabled**, the service cannot become active until you enable it.

Oper. the current operational status of the service. If **Active**, the service is currently in use. If you have set up primary and secondary services, only one will be Active. A port cannot become operationally active until it has been administratively enabled.

Srvc Type. The type of ATM service. Currently only LANE services are supported as auto-activated services.

Service Name. The ELAN to which this service belongs.

Non-Mobile Groups and AutoTracker VLANs

Non-mobile Groups are comprised of *physical* entities—switch ports. Groups can span multiple switches, but they are still made up of physical ports that you can see and touch. But just as physically-based broadcast domains are limited, entirely port-based Groups can also be limiting. In a large, flat, switched network, broadcast traffic can overload the network. There needs to be a method for subdividing traffic even further. That's where virtual networks, or VLANs, come into play.

VLANs are created within a Group to subdivide network traffic based on specific criteria. The criteria you use to define a VLAN are called AutoTracker™ policies. AutoTracker policies can be defined by port, MAC address, protocol, network address, a user-defined policy, or a multicast policy. VLANs are described in more detail in Chapter 27, “Managing AutoTracker VLANs” and Chapter 28, “Multicast VLANs.”

Routing in a Non-Mobile Group

Communication within a Group containing only the default VLAN is switched; the ports are in the same broadcast domain and do not require routing to communicate. Communication between VLANs in the same Group or to VLANs in other Groups requires routing. That's why all VLANs—including the default VLAN within each Group—may contain their own virtual router port. A virtual router port for each VLAN can be configured to support IP and/or IPX routing. If you do not configure a virtual router port for a VLAN, the devices in that VLAN will not be able to communicate with devices in other VLANs unless there is an external router between the VLANs.

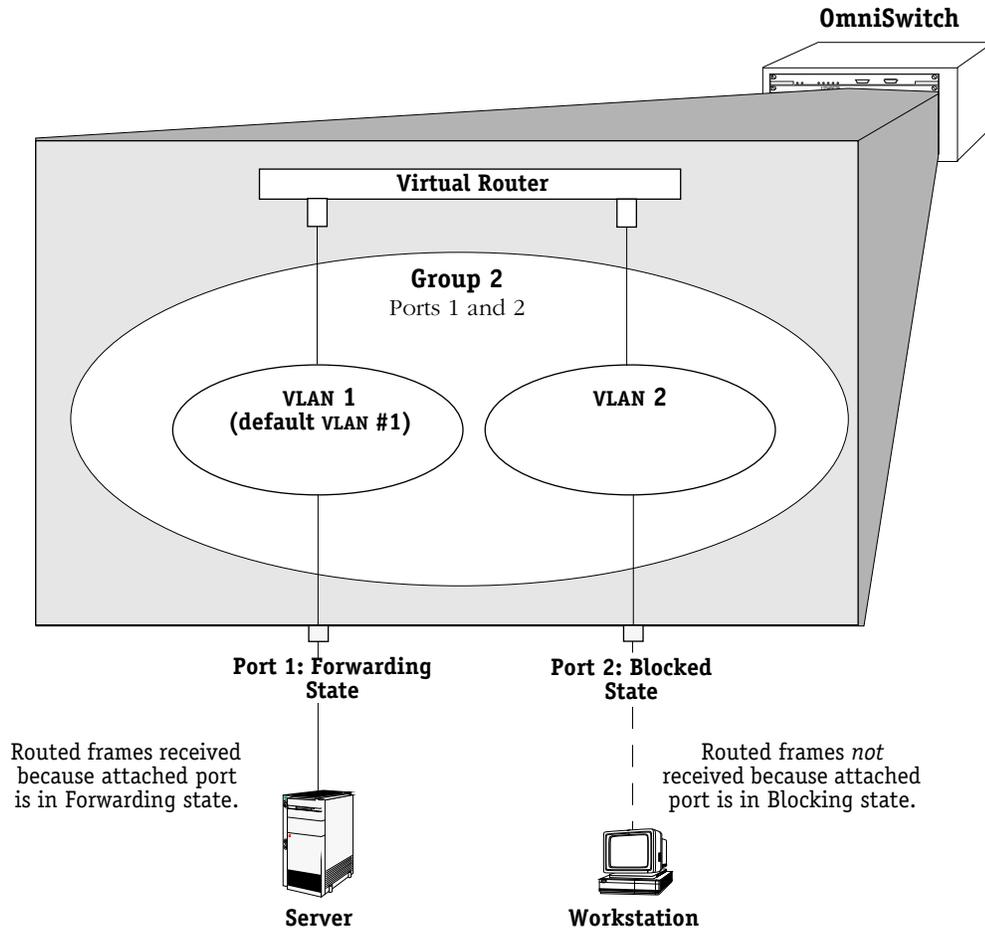
Each OmniSwitch supports up to 32 virtual router ports. A single router port, using one MAC address, can support IP routing, IPX routing, or both types of routing. When you enable a router port for a default VLAN, you are actually creating a static route to that VLAN. Routing is covered in more detail in Chapters 30 and 32.

◆ Note ◆

For mobile, non-mobile groups and AutoTracker VLANs, the router port operational status is not active unless an active switch port is a member of the group or VLAN.

Spanning Tree and Non-Mobile Groups

Each Group uses one Spanning Tree for bridging. The OmniSwitch supports both 802.1d and IBM Spanning Tree protocols. The Spanning Tree state for the port is Forwarding. Ports that are in Blocked state, or in another non-Forwarding state, will not receive frames from the router port. The figure below illustrates this concept.



Spanning Tree State and Routed Frames

Group and Port Software Commands

Group and Virtual Port commands are part of the VLAN menu within the User Interface. Entering **vlan** at any prompt displays the following menu:

<u>Command</u>	<u>VLAN Management Menu</u>
gp	View the list of Groups currently defined
crgp	Create a Group
modvl	Modify a VLANs configuration/availability
rmgp	Remove a Group
addqgp	Add 802.1q group/s to a port
delqgp	Delete 802.1q group/s from a port
viqgp	Display 802.1q groups on port/s
via	View ports assigned to the selected Group
vi	View info on a specific virtual port
vs	View statistics on a virtual port attachment
ve	View errors on a virtual port attachment
addvp	Add ports to a GROUP
modvp	Modify existing VPORT configuration information
rmvp	Remove ports from a Group
pmapcr	Create a Port Map
pmapdel	Delete a Port Map
pmapmod	Modify a Port Map
pmapv	View Port Mapping Configuration
br	Enter the Bridge Configuration/Parameter sub-menu
prty_mod	Modify the priority of a group
prty_disp	Display the priority of a group
at	Enter the AutoTracker sub-menu

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

The VLAN menu commands are divided into four sets of commands. The first set, at the top of the menu beginning with **gp**, contains commands that create, modify, delete, and view Groups. The second set of commands, beginning with **addqgp** are obsolete and no longer control 802.1Q implementation. (See Chapter 20 for information on 802.1Q.) The third set, beginning with **addvp**, contains commands for adding, modifying, and deleting virtual ports. All of these commands are described in this chapter.

The final set of commands at the bottom of the menu, **br** and **at**, are actually entry points to the Bridging and AutoTracker submenus, respectively. Commands for the Bridge Management (**br**) sub-menu are documented in Chapter 22, “Configuring Bridging Parameters” and Chapter 21, “Managing Token Ring.” Commands for the AutoTracker (**at**) sub-menu are documented in this chapter and in Chapter 27, “Managing AutoTracker VLANs” and Chapter 28, “Multicast VLANs.” Some commands in the **at** sub-menu apply to mobile groups and authenticated groups; those commands are described in this chapter.

The **pmapcr**, **pmapdel**, **pmapmod**, and **pmapv** commands allow you to create port mapping configurations. The port mapping feature is documented in *Port Mapping* on page 24-74. The **prty_mod** and **prty_disp** commands allow you to modify and view the priority of a selected group. These commands are detailed in *Priority VLANs* on page 24-81.

Creating a New Group

There are several steps involved in creating a new Group. Note that some steps apply only to mobile groups. These steps are as follows:

1. Enter Basic Group Information, such as the Group number and type. This section starts on page 24-22.
2. Configure the Virtual Router Port (Optional). This section starts on page 24-24.
3. Enable/disable Group Mobility and User Authentication. This section starts on page 24-30.
4. Configure Virtual Ports. This section starts on page 24-31.
5. Configure Auto-Activated LANE service ports (for mobile groups only). This section starts on page 24-37.
6. Configure AutoTracker policies (for mobile groups only). This section starts on page 24-38.

WAN Routing and ATM Classical IP (CIP) Groups follow a slightly different procedure for their creation. You will receive prompts during the procedure asking whether you want to create one of these special Groups.

Step 1. Entering Basic Group Information

- a. Type **crgp** at any prompt.
- b. The following prompt displays:

GROUP Number (5):

By default the Group number you entered or the next available Group number is displayed in parentheses. Enter the Group number or accept the number shown in parentheses. Each Group must have a unique number, which may range from 2 to 65,535. (Group 1 is the default switch Group. It does not need to be created and it cannot be deleted.) Press **<Enter>** after entering the Group number.

- c. The following prompt displays:

Description (no quotes) :

Enter a descriptive name for the new Group. Group names can consist of up to 30 alphanumeric characters. Press **<Enter>** after entering the Group name.

- d. The following prompt displays:

Enable WAN Routing? (n):

If you want to perform WAN Routing through this Group you must enter a **y** at this prompt. If you do not need to support WAN Routing, then answer **n** at this prompt and continue with Step e.

◆ **Note** ◆

You do not need to create a special WAN Routing Group to bridge or trunk traffic over a WAN connection. If you are just Bridging or Trunking on WAN, answer **n** to this prompt and continue with Step e.

A WAN Routing Group is different from other Groups; it must contain only WAN ports. In addition, the virtual router and virtual ports are configured differently. Please skip ahead to *Creating a WAN Routing Group* on page 24-39 to continue setting up this WAN Routing Group.

- e. The following prompt displays:

Enable ATM CIP? (n):

ATM Classical IP (CIP) must be enabled if there are devices on the ATM network that support only Classical IP or require Classical IP to communicate over the network. Answer **n** at this prompt if this Group will not support ATM CIP and skip ahead to *Step 2. Configuring the Virtual Router Port (Optional)* on page 24-24.

Answer **y** at this prompt if this Group must support ATM CIP. If you answer **y**, then this Group will support only CIP and you will need to configure it further through the Services menu. Skip ahead to *Creating an ATM CIP Group* on page 24-42 for further instructions on setting up this ATM CIP Group.

- f. The following prompt displays:

Enable MPLS? (n):

Answer **n** at this prompt.

◆ **Note** ◆

MPLS is not supported in the current release.

Step 2. Configuring the Virtual Router Port (Optional)

You can now optionally configure the virtual router port that the default VLAN in this Group will use to communicate with other VLANs. When you define a virtual router, a virtual router port for the default VLAN in the Group is created. If you do not define a virtual router, no virtual router port is created and the default VLAN in the new Group will be “firewalled,” unable to communicate with other VLANs.

◆ Important Note ◆

Use caution when setting up routing on the default VLAN for a Group. In some configurations enabling routing on the default VLAN may not be necessary or desirable. You can always enable routing on other, non-default VLANs, within this Group. Refer to *AutoTracker Application Example 4* in Chapter 27 for more information.

You will have the choice of configuring IP, IPX, or both IP and IPX routing. Continue with the steps below:

- a. After answering **n** to the **Enable ATM CIP?** prompt, the following prompt displays:

Enable IP (y):

Press **<Enter>** if you want to enable IP Routing on this virtual router port. If you do not enable IP, then the default VLAN in this Group will not be able to route IP data. If you don't want to set up an IP router, enter **n**, press **<Enter>** and skip to Step j.

◆ Note ◆

You may enable routing of both IP and IPX traffic on this router port. If you set up dual-protocol routing, you must fill out information for both IP and IPX parameters.

- b. The following prompt displays:

IP Address:

Enter the IP address for this virtual router port in dotted decimal notation (e.g., 198.206.181.10). This IP address is assigned to the virtual router port of the default VLAN within this Group. After you enter the address, press **<Enter>**.

- c. The following prompt displays:

IP Subnet Mask (0xfffff00):

The default IP subnet mask (in parentheses) is automatically derived from the default VLAN IP address class. Press **<Enter>** to select the default subnet mask or enter a new subnet mask in dotted decimal notation or hexadecimal notation and press **<Enter>**.

- d. The following prompt displays:

IP Broadcast Address (198.200.10.255):

The default IP broadcast address (in parentheses) is automatically derived from the default VLAN IP address class. Press **<Enter>** to select the default address or enter a new address in dotted decimal notation and press **<Enter>**.

- e. The following prompt displays:

Description (30 chars max):

Enter a useful description for this virtual IP router port using alphanumeric characters. The description may be up to 30 characters long. Press **<Enter>**.

- f. The following prompt displays:

Disable routing? (n) :

Indicate whether you want to disable routing in the group. You can enable routing later through the **modvl** command.

- g. The following prompt displays:

**IP RIP Mode {Deaf (d),
Silent (s),
Active (a),
Inactive (i)} (s):**

Define the RIP mode in which the virtual router port will operate. RIP (Router Information Protocol) is a network-layer protocol that enables the default VLAN in this Group to learn and advertise routes. The RIP mode can be set to one of the following:

Silent. The default setting shown in parentheses. RIP is active and receives routing information from other VLANs, but does not send out RIP updates. Other VLANs will not receive routing information concerning the default VLAN in this Group and will not include the VLAN in their routing tables. Simply press **<Enter>** to select Silent mode.

Deaf. RIP is active and sends routing information to other VLANs, but does not receive RIP updates from other VLANs. The default VLAN in this Group will not receive routing information from other VLANs and will not include other VLANs in its routing table. Enter **d** and press **<Enter>** to select Deaf mode.

Active. RIP is active and both sends and receives RIP updates. The default VLAN in this Group will receive routing information from other VLANs and will be included in the routing tables of other VLANs. Enter **a** and press **<Enter>** to select Active mode.

Inactive. RIP is inactive and neither sends nor receives RIP updates. The default VLAN in this Group will neither send nor receive routing information to/from other VLANs. Enter **i** and press **<Enter>** to select Inactive mode.

- h. If routing domains *are not* configured on the switch, go to the next step. If routing domains *are* configured on the switch, the following prompt displays:

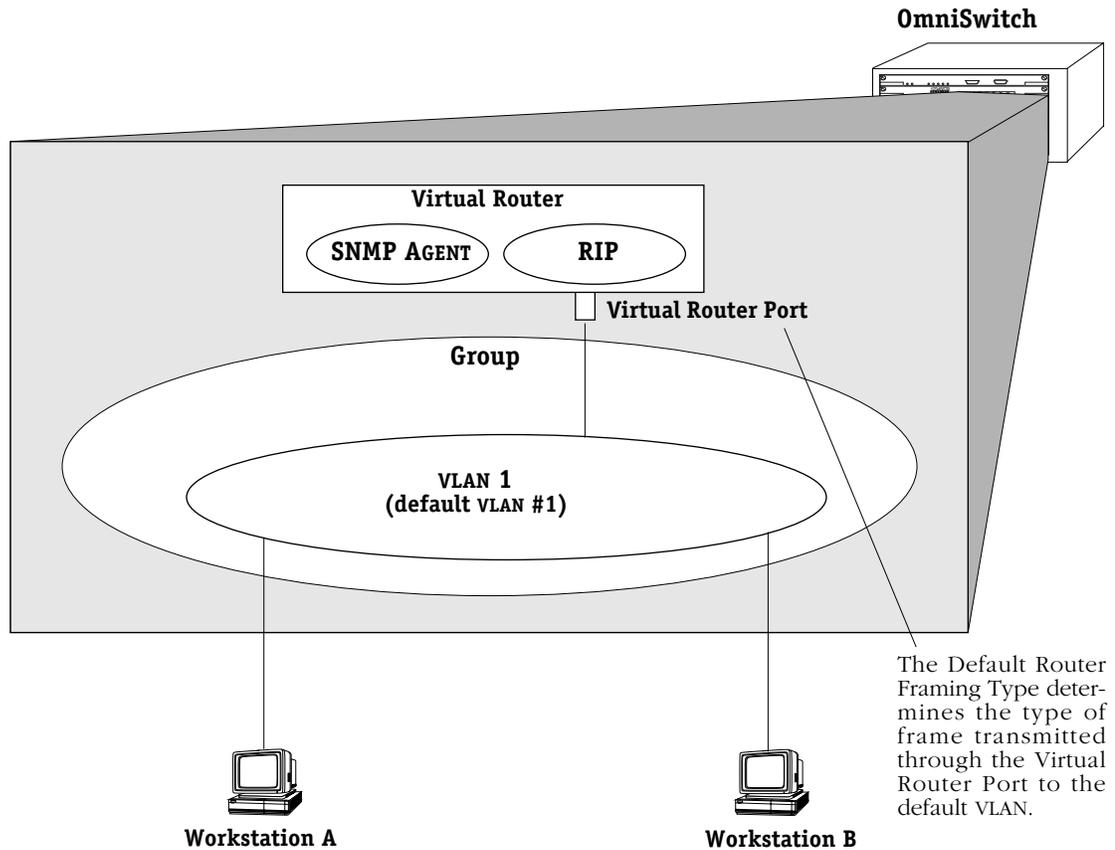
Apply to Routing Domain ID (none) :

Enter a routing domain in which this group should be included, or press **Enter**. A routing domain is a grouping of IP router interfaces that can forward packets only within the domain. Routing domains are part of Advanced Routing software and are not part of the base code. For more information about routing domains, see Chapter 14, "Routing Domains," in the *Advanced Routing User Manual*.

- i. After you enter the RIP mode, or after you enter a routing domain ID, the following prompt displays:

**Default framing type [Ethernet II(e),
fddi (f),
token ring (t),
Ethernet 802.3 SNAP (8),
source route token ring(s)} (e):**

Select the default framing type for the frames that will be generated by this router port and propagated over the default VLAN to the outbound ports. Set the framing type to the encapsulation type that is most prevalent in the default VLAN. If the default VLAN contains devices using encapsulation types other than those defined here, the switching modules must translate those frames, which slows throughput. The figure on the next page illustrates the Default Framing Type and its relation to Virtual Router Port communications.



Default Framing Type and the Virtual Router Port

- j. You can now configure IPX routing on this port. The following message displays:

Enable IPX? (y) :

Press **<Enter>** if you want to enable IPX Routing on this virtual router port. If you do not enable IPX, then the default VLAN in this Group will not be able to route IPX data. You can set up a virtual router port to route both IP and IPX traffic.

If you don't want to set up an IPX router for the default VLAN in this Group, enter **n**, press **<Enter>**, and skip ahead to step **p** below. You can always set up IPX routing for other VLANs within this Group.

- k. After selecting to enable IPX, the following prompt displays:

IPX Network:

Enter the IPX network address. IPX addresses consist of eight hex digits and you can enter a minimum of one hex digit in this field. If you enter less than eight hex digits, the system prefixes your entry with zeros to create eight digits.

- l. The following prompt displays:

Description (30 chars max):

Enter a useful description for this virtual IPX router port using alphanumeric characters. The description may be up to 30 characters long. Press **<Enter>**.

- m. The following prompt displays:

IPX Delay in ticks (0):

Enter the number of ticks you want for the IPX network. A tick is about 1/18th of a second. The default is 0.

- n. The following prompt displays:

**IPX RIP and SAP mode {RIP and SAP active (a)
RIP only active (r)
RIP and SAP inactive (i)} (a):**

Select how you want the IPX protocols, RIP (router information protocol) and SAP (service access protocol), to be configured for the default VLAN in this Group. RIP is a network-layer protocol that enables this VLAN to learn routes. SAP is also a network-layer protocol that allows network services, such as print and files services, to advertise themselves. The choices are:

RIP and SAP active. The default setting. The default VLAN to which this IPX router port is attached participates in both RIP and SAP updates. RIP and SAP updates are sent and received through this router port. Simply press **<Enter>** to select RIP and SAP active.

RIP only active. The default VLAN to which this IPX router port is attached participates in RIP updates only. RIP updates are sent and received through this router port. Enter an **r** and press **<Enter>** to select RIP only active.

RIP and SAP inactive. The IPX router port is active, but the default VLAN to which it is attached does not participate in either RIP nor SAP updates. Enter an **i** and press **<Enter>** to select RIP and SAP inactive.

- o. After selecting the RIP and SAP configuration, the following prompt displays the default router framing type options:

```
Default router framing type for : {  
  
  Ethernet Media:  
    Ethernet II (0),  
    Ethernet 802.3 LLC (1),  
    Ethernet 802.3 SNAP (2),  
    Novell Ethernet 802.3 raw (3),  
  
  FDDI Media:  
    fddi SNAP (4),  
    source route fddi SNAP (5),  
    fddi LLC (6),  
    source route fddi LLC (7),  
  
  Token Ring Media:  
    token ring SNAP (8),  
    source route token ring SNAP (9),  
    token ring LLC (a),  
    source route token ring LLC (b) }      (0) :
```

Select the default framing type for the frames that will be generated by this router port and propagated over the default VLAN to the outbound ports. Set the framing type to the encapsulation type that is most prevalent in the default VLAN. If the default VLAN contains devices using encapsulation types other than those defined here, the switching modules must translate those frames, which slows throughput. See the figure, *Default Framing Type and the Virtual Router Port* on page 24-26 for an illustration of the Default Framing Type and its relation to Virtual Router Port communications.

◆ Note ◆

The `.cmd` file contains a command called `hreXnative` that by default is set to 1. If physical ports in an end station are using a different encapsulation than the virtual router ports (for example, the `modvl` command shows router ports set to Ethernet II IPX, but the `swch` command shows that physical ports are using SNAP) then the `hreXnative` command *must* be set to 0. See Chapter 13, “Switch Wide Parameters,” for more information about the `.cmd` file.

- p. If you chose a Source Routing frame format in the last step (options 5, 7, 9, or b), an additional prompt displays:

```
Default source routing broadcast type : {  
  ARE broadcasts(a), STE broadcasts(s)}      (a) :
```

Select how broadcasts will be handled for Source Routing. The choices are:

ARE broadcasts. All Routes Explorer, the default setting. Broadcasts are transmitted over every possible path on inter-connected source-routed rings. This setting maximizes the generality of the broadcast. Simply press **<Enter>** to select All Routes Explorer.

STE broadcasts. Spanning Tree Explorer. Broadcasts are transmitted only over Spanning Tree paths on inter-connected source-routed rings. This setting maximizes the efficiency of the broadcast. Enter an **s** and press **<Enter>** to select Spanning Tree Explorer.

- q. The following prompt displays:

Enter a priority level (0...7)(0):

Prioritizing VLANs allows you to set a value for traffic based on the destination VLAN of packets. Traffic with the higher priority destination will be delivered first. VLAN priority can be set from 0 to 7, with 7 being the level with the most priority.

Modifying and displaying a group's priority is described in *Priority VLANs* on page 24-81.

You have now completed the configuration of the virtual router port for this group. At this point, you will be asked whether you want to enable group mobility. The following prompt will display:

Enable Group Mobility on the Group ? [y/n] (n):

Mobile groups are discussed in detail in *Mobile Groups* on page 24-5. If you want to enable group mobility answer **Y** to this prompt, press **<enter>**, and go on to *Step 3. Set Up Group Mobility and User Authentication* on page 24-30.

If you do not want to configure group mobility answer **N** at the prompt, press **<enter>**, and go on to *Step 4. Configuring Virtual Ports* on page 24-31 for further instructions.

Step 3. Set Up Group Mobility and User Authentication

A mobile group offers more flexibility than a non-mobile group. With a mobile group, ports are assigned dynamically to the group based on AutoTracker policies that you configure. In a non-mobile group, ports are statically defined and AutoTracker policies are assigned to individual VLANs within the Group. In most cases, you will want to set up a mobile group. The following steps show you how.

- a. After configuring the virtual router port, you will receive the following prompt:

Enable Group Mobility on the Group ? [y/n] (n):

To create a mobile group, enter a **Y** as this prompt, press **<enter>**, and continue with step b. If you want to configure a non-mobile Group, enter **N**, press **<enter>**, and you will see the following prompt:

This Group will not participate in Group Mobility

If you are *not* creating a mobile group, go on to *Step 4. Configuring Virtual Ports* on page 24-31.

- b. The following prompt displays:

Enable User Authentication on the Group ? [y/n] (n):

An authenticated group is a special type of mobile group. It uses an authentication process as its criteria for group membership. Typically, users will be prompted for an id and password before gaining membership to an authenticated group. Authenticated groups require additional Windows NT server software. More detailed information on these groups can be found in the *Switch Network Services User Manual*. If you are not sure whether this is an authenticated group, simply press **<enter>** at this prompt.

- c. The following prompt displays:

Enable spanning tree for this group [y/n] (y):

Spanning Tree prevents broadcast storms by limiting logical loops in the network. For more information on Spanning Tree, see Chapter 22, titled “Configuring Bridging Parameters.” If you wish to enable Spanning Tree, enter **y** and press **<enter>**. Otherwise, enter **n**.

- d. The following prompt displays:

Do you wish to configure the interface group for this Virtual LAN at this time? (y)

You can assign physical ports to the new Group at this time. To begin assigning ports to the new Group, press **<Enter>** and go to Step 4.

To assign ports to the Group later, type **n** and **<Enter>**. The new Group is configured but does not yet contain any ports. You can use the **addvp** command later to assign ports to the Group (see *Adding Virtual Ports* on page 24-52). A message similar to the following displays confirming the creation of the new Group.

**GROUP 6 has been added to the system.
You may add interfaces to this group using the addvp command at a later date.
For now, the GROUP is inactive until you add interfaces.
Configure Auto-Activated LANE service ? [y/n] (y) :**

If you want to configure switch ports later (or simply rely on the dynamic port assignment capability’s of the mobile group) skip ahead to *Step 5. Configure Auto-Activated LANE Ports (Mobile Groups Only)* on page 24-37.

Step 4. Configuring Virtual Ports

You can now enter configuration parameters for each switch port to be included in this Group. These configuration parameters include the bridging mode, output format type, and administrative state. In addition, if the port you are configuring is Ethernet (10/100 Mbps) or Token Ring, you can also configure port mirroring.

Prompts for configuring virtual ports follow directly after Group Mobility prompts. You can choose to add ports now or add them later through the **addvp** command. Follow these steps:

- a. After you have stepped through the Routing and/or Group Mobility prompts, the following message displays:

Do you wish to configure the interface group for this Virtual LAN at this time? (y)

You can assign physical ports to the new Group at this time. To begin assigning ports to the new Group, press **<Enter>** and go to Step b.

To assign ports to the Group later, type **n** and **<Enter>**. The new Group is configured but does not yet contain any ports. You can use the **addvp** command later to assign ports to the Group (see *Adding Virtual Ports* on page 24-52). A message similar to the following displays confirming the creation of the new Group.

**GROUP 6 has been added to the system.
You may add interfaces to this group using the addvp command at a later date.
For now, the GROUP is inactive until you add interfaces.**

- b. After indicating that you want to set up ports, the following prompt displays:

Initial Vports (Slot/Phys Intf. Range) - For example, first I/O Module (slot 2), second interface would be 2/2. Specify a range of interfaces and/or a list as in: 2/1-3, 3/3, 3/5, 4/6-8

Enter the port or ports that you want to include in this new Group. The notation for adding a port to a group is

<slot number of module>/<port number on the module>

Omni-5 slots are numbered from 1 to 5, top to bottom. Omni-9 slots are numbered 1-9, left to right. Port numbers are labelled on the front panel of switching modules.

You may enter multiple ports from multiple switching modules. For example, to add ports 1 through 3 on the module in slot 2, specify **2/1-3**. To additionally add the third and fifth port on the module in the third slot, specify **3/3, 3/5**. The complete slot port specification would be:

2/1-3, 3/3, 3/5

- c. If you enter a port that is already assigned to another Group, then you will be prompted on whether or not you want to change its assignment. A message similar to the following displays for each port that you enter:

**Initial Slot/Interface Assignments: 2/8
2/8 - This interface has already been assigned to GROUP 1 -
(Default GROUP #1).
Do you wish to remove it from that GROUP and assign it (with
new configuration values) to this GROUP (n)?**

Simply enter a **y** at each port prompt to change its Group assignment and begin setting port parameters. You could also enter a **c** at this prompt to accept all default port parameters and skip port configuration prompts. If you enter a **c**, *all* remaining ports are automatically added to the Group with default settings, and your work is complete.

- d. The virtual port configuration menu displays:

Modify Ether/8 Vport 2/8 Configuration

```
1) Vport                : 9
2) Description          :
3) Bridge Mode         : Auto-Switched
   31) Switch Timer     : 60
4) Flood Limit         : 192000
5) Output Format Type   : Default (IP-Eth II, IPX-802.3)
6) Ethernet 802.2 Pass Through : Yes
7) Admin, Operational Status : Enabled, inactive
8) Mirrored Port Status : Disabled, available
9) MAC address         : 000000:000000
```

Command {Item=Value/?/Help/Quit/Redraw/Next/Previous/Save} (Redraw) :

Descriptions for each of the fields in this display follow. To change any default value, enter the line number for item, an equal sign (=), and then the value for the parameter. Enter **save** to save all configured settings and move onto the next step in the group creation process.

1) *Vport*

The virtual port number for this port. The next virtual port number available in the switch is shown by default in this field.

2) *Description*

Enter a useful description for this virtual port using alphanumeric characters. The description may be up to 30 characters long.

3) *Bridge Mode*

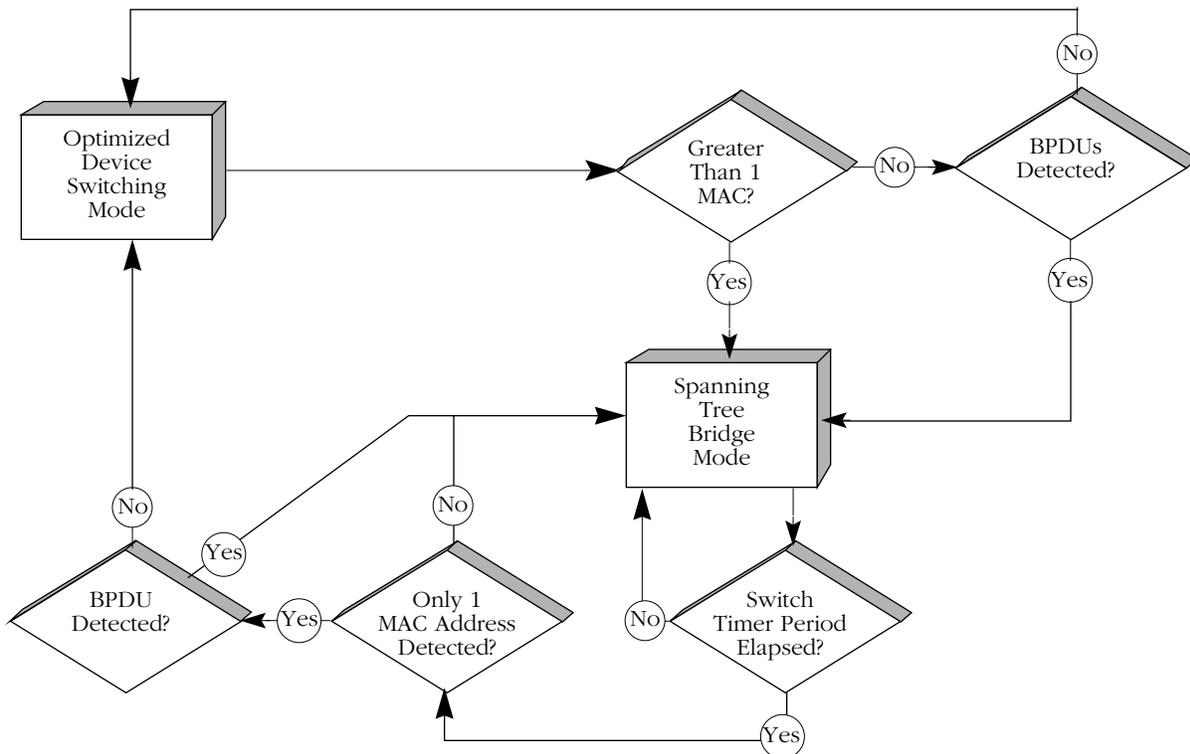
Select the bridge mode used by this port. The choices are:

Spanning Tree Bridge. The default setting for all non-Ethernet ports. This mode is appropriate for backbone and hub connections. The port acts as a standard 802.1d bridge port. It forwards BPDU frames out the port. When frames are received, Spanning Tree BPDUs are processed, and Spanning Tree dynamically controls the forwarding state. If flooding occurs, all frames destined for unknown MAC addresses, broadcast addresses, or multicast addresses will be sent to all ports in the same Group. Enter **3=b** and press **<Enter>** to select Spanning Tree Bridge mode.

Optimized Device Switching. This mode is appropriate for dedicated connections to a single workstation or server. Spanning Tree is turned off. No Spanning Tree BPDUs will be sent and the port will always be in the forwarding state. The port will stay in this mode even if a Spanning Tree BPDU is detected. In addition, all MACs learned will not be aged out (regardless of the Bridge Aging Timer setting) until the port is disconnected or configured to be administratively down. No flooding of packets with an unknown destination address is allowed after at least one MAC address has been learned. (An exception to this rule occurs on newer Mammoth-generation Ethernet modules, such as the ESM-100C-12, ESM-100F-8, and ESM-C-32. When these ports are in optimized mode, packets with unknown destination addresses will be flooded.) Packets with a broadcast or multicast destination will always be allowed. Enter **3=o** and press **<Enter>** to select Optimized Device Switching mode.

Auto-Switch. The default setting for all Ethernet ports. This mode is appropriate for dedicated connections requiring a switch-over to bridge mode when multiple devices are detected. A port in Auto-Switch mode will start in Optimized Device Switching mode (see description above). The port will remain in Optimized Device Switching mode until a Spanning Tree BPDU is detected or more than one MAC address transmits data. Once either of these conditions is met, the port will switch to Spanning Tree Bridge mode and Spanning Tree will start (if configured in the switch).

An Auto-Switch port will remain in Spanning Tree Bridge mode as long as there are BPDUs and multiple MACs. However, the port can revert back to Optimized Device Switching Mode if the time specified in the next field (**Switch Timer**) transpires without BPDUs and multiple MACs. Also, if the port is disconnected or configured to be administratively down, then an Auto-Switch port will revert back to Optimized Device Switching mode when it becomes operational again. Enter **3=a** and press **<Enter>** to select Auto-Switch mode.



How Auto-Switch Bridge Mode Works

31) Switch Timer

If you selected the Auto-Switch bridge mode, then you can configure this field. Enter the time-out period, in seconds, for an Auto-Switch port that has turned to Spanning Tree Bridge mode port to revert back to Optimized Switching mode. When in Auto-Switch mode, a port switches to Spanning Tree Bridge mode as soon as it detects a BPDU or more than one MAC address. The port will switch back to Optimized Switching mode after the time-out value you define here.

4) Flood Limit

The flood limit allows you to tune a virtual port to limit the flooding of broadcast, multi-cast, and unknown destination packets. This feature is useful for controlling broadcast storms on your network. While each network is different, in general the amount of flooded traffic represents a relatively small percentage of network traffic.

The flood limit is actually a “transmit credit” that is issued every five (5) seconds. When a packet is flooded on this port, the size of the packet, in bytes, is decremented from the current credit value. The credit value is the value you enter in this field multiplied by five. An additional credit, in the amount of the value you enter here multiplied by five, is allocated to each virtual port every five (5) seconds. If the credit value ever falls below zero, then all flooded packets are discarded until another credit is allocated. Flood limit checking is disabled if you enter a flood limit of zero (0). The flood limit default is 192,000 bytes per second, which equates to a transmit credit of 960,000 bytes every five seconds.

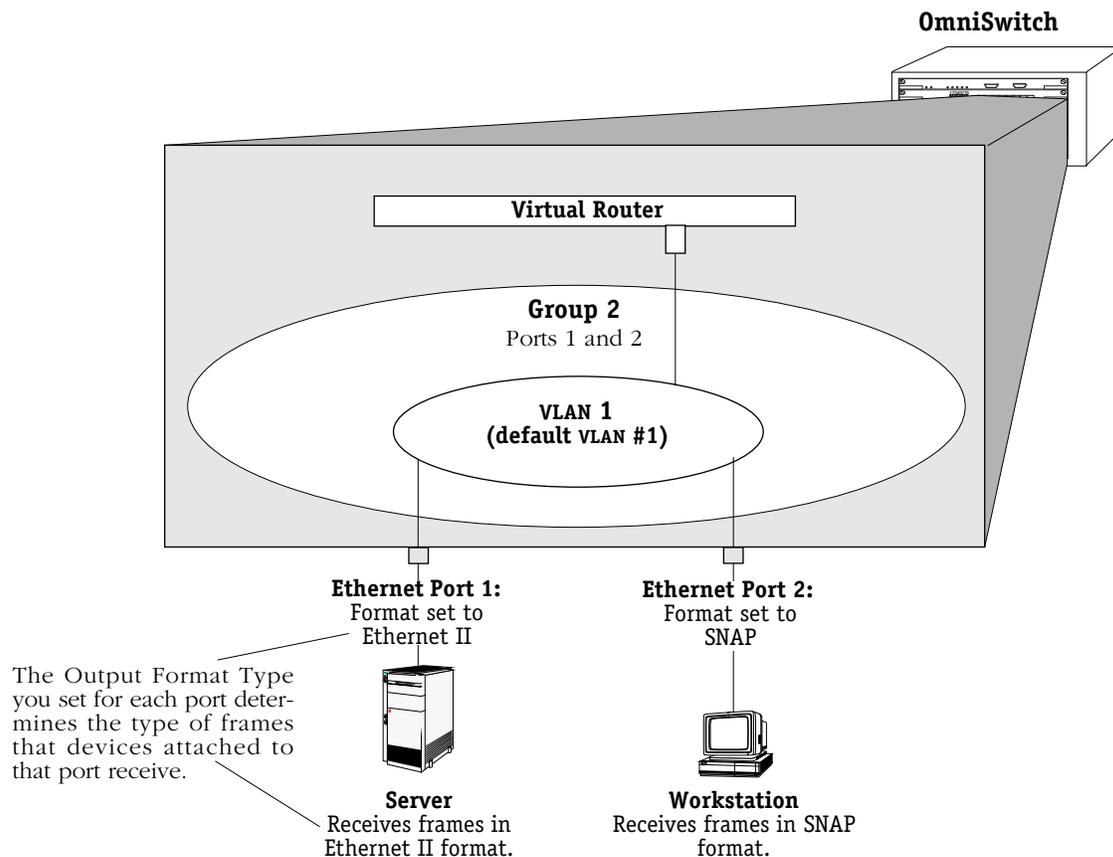
5) Output Format Type

The options will be different for Ethernet, Token Ring, and FDDI ports.

The output format setting determines the kind of frame that will be sent out this physical port. If translation is necessary, then incoming frames will be translated to this format before being sent out this port. For example, on an Ethernet port incoming FDDI frames need to be translated to Ethernet. However, there are four types of Ethernet frames—Ethernet II, IPX 802.3, SNAP, and LLC. The format type you select here would determine the frame format to which non-Ethernet frames would be translated. The following figure illustrates how a port’s framing type affects communication with attached devices.

◆ Note ◆

This parameter differs from the router framing type selected during the configuration of the virtual router port. The router framing type is the encapsulation done on a router port, whereas this output format type applies only to translations on this virtual port.



Output Framing Type on Physical Ports

Note that for Ethernet, the default output format option is Ethernet II for IP frames and 802.3 for IPX frames. On Token-Ring and FDDI, only SNAP and LLC are available as output format choices; FDDI ports may be configured to output 802.3 frames (i.e., "FDDI raw"), but that must be configured through the Switch menu.

You can customize your frame translation settings even further through the Switch menu. The Switch menu allows you to set translations at the frame format level (i.e., incoming SNAP frames could be translated one way, while incoming LLC frames could be translated another way) based on protocol type (IP or IPX). The Switch menu is explained in Chapter 23, "Configuring LAN Switch Translations."

6) *Ethernet 802.2 Pass Through*

For Ethernet ports only. If you answer **Yes** to this prompt, then frames received in the IEEE 802.2 format will not be translated according the Output Format Type chosen in line 5; they will be sent as is in their native IEEE 802.2 format. If you answer **No**, then 802.2 frames will be subject to the Output Format Type chosen in line 5.

7) *Admin, Operational Status*

Select whether to administratively enable or disable this port. When you enable the port, the port can transmit and receive data as long as a cable is connected and no physical or operational problems exist. When you disable a port, the port will not transmit or receive data even if a cable is connected and the physical connection is operational. If you disable the port at this point, you can enable it later through the **modvp** command (see *Modifying a Virtual Port* on page 24-53).

8) *Mirrored Port Status*

If the port you are configuring is Ethernet (10 or 10/100 Mbps) or Token Ring, you can set up port mirroring. You can mirror traffic on this port to another like port. Port mirroring is a useful feature for monitoring traffic on particular ports. It is discussed in more detail later in this chapter in *Port Mirroring* on page 24-65.

If you want to mirror this port, enter a **8=e**, press **<Enter>** and you will be prompted for the slot and port number of the “mirroring” port (i.e., the port that can “see” all traffic for this port):

Mirroring vport slot/port ? () :

Enter the mirroring port’s slot and port number and press **<Enter>**.

If port mirroring is not supported on this port, then the following prompt will display:

mirroring not supported on this port type

9) *MAC address*

Enter the MAC address for this virtual port if it is known.

After the MAC address prompt, the switch confirms the addition of the port to the group with a message similar to the following:

Adding port 2/8 to Group 6. . .

Make configuration changes to the port until you are satisfied. If you have completed the final virtual port, then your work is complete. You can always alter Group parameters (including virtual router parameters for the default VLAN) later through the **modvl** command (see *Modifying a Group or VLAN* on page 24-48) and modify virtual port parameters through the **modvp** command (see *Modifying a Virtual Port* on page 24-53).

Step 5. Configure Auto-Activated LANE Ports (Mobile Groups Only)

If you set up a mobile group in Step 3, you can configure LANE service ports as members of this group. Before release 3.2, LANE clients could only be set up through the **cas** command. Now, you can automatically insert these ports into a mobile group without any more configuration than the following steps.

- a. After you have completed configuring virtual ports, the following prompt displays:

Configure Auto-Activated LEC service ? [y/n] (y) :

To add a LANE service port to this mobile group, enter a **Y** and press **<enter>** at this prompt.

- b. The following prompt displays:

Enter the primary slot/interface for this service:

Enter the slot and port of the ATM access switch port that will be the primary port for this LANE service. The port should be an ATM access port (ASM or FCSM) as opposed to a cell switching, Ethernet, Token Ring, etc. port.

- c. The following prompt displays

Enter the secondary slot/interface for this service (hit enter for none):

Enter the slot and port of the ATM access switch port that will be used as the secondary port for this LANE service. This port will be used in case the primary port is not available; it will remain dormant until the primary port goes down. If you do not want to specify a secondary port (or if there is no other ATM access port in the switch), press **<Enter>**.

◆ **Note** ◆

If the port is an ATM RFM port, then do not specify a secondary port for this Auto-Activated LANE service.

- d. The following prompt displays

Enter E-LAN name:

Enter the name you want to use for this LANE service. Duplicate ELAN names cannot be used on the same port. It is possible to set up LANE services through the **cas** command, so make sure you are not using an ELAN name that has already been used. If you create a service through **cas** that uses the same name as a dormant auto-activated service, then the auto-activated service will not become operational.

- e. The following prompt displays

Enter the ELAN Type [Ethernet|Token Ring] (Ethernet):

Ethernet and Token Ring LANE clients are handled differently by switch software. Specify which type you want to configure.

- f. The following prompt displays:

Enable Translations for this service [y/n] (y):

If you want this service to perform translations, enter a **y**. Otherwise, enter **n**.

- g. The following prompt displays

Enable this service ? [y/n] (y):

Indicate whether or not you want to enable this service. If you enable this service it will remain operationally inactive until a device becomes a member of this ELAN. As soon as you enable the service, devices will be able register with this mobile group.

- h. The following prompt displays

Configure another service for this group ? [y/n] (n):

If you want to configure more auto-activated LANE service ports, enter a **Y** at this prompt. To begin configuring AutoTracker rules for this mobile group, enter an **N** and continue with Step 6.

Step 6. Configuring AutoTracker Policies (Mobile Groups Only)

When you have completed configuring mobile group and auto-activated LANE services, you can begin configuring AutoTracker policies for this mobile group. Instructions for configuring these rules can be found in Chapter 25, “Configuring Group and VLAN Policies.” Please refer to that chapter for instructions on configuring each policy type. After you configure AutoTracker policies, you are done configuring this mobile group and a prompt similar to the following displays:

VLAN 9: 1 created successfully

You can configure rules for this group later through the **modatvl** command. This command also works with mobile groups as long as you indicate you want to alter VLAN 1 in the mobile group (i.e., the command line would read **modatvl 3:1** to modify mobile group 3).

◆ Note ◆

If the mobile group is initially created without rules, the **modatvl** command cannot be used to add them later. You must turn off group mobility and then reinstate it to add the rules.

Creating a WAN Routing Group

After entering basic Group information as described in *Step 1. Entering Basic Group Information* on page 24-22, you should have answered Yes to the following prompt:

Enable WAN Routing? (n):

if you want to enable WAN Routing. WAN Routing Groups are treated differently than other Groups, as described earlier. The following steps complete the configuration of the WAN Routing Group.

- a. After answering **y** to the **Enable WAN Routing?** prompt, the following prompt displays:

Enable IP (y):

Press **<Enter>** if you want to enable IP Routing on the virtual router port for this Group. If you do not enable IP, then this WAN Group will not be able to route IP data. If you don't want to set up IP routing, enter **n**, press **<Enter>** and skip to Step g.

◆ **Note** ◆

You may enable routing of both IP and IPX traffic over a WAN connection. If you set up dual-protocol routing, you must fill out information for both IP and IPX parameters.

- b. The following prompt displays:

IP Address:

Enter the IP address for this virtual router port in dotted decimal notation or hexadecimal notation (e.g., 198.206.181.10). This IP address is assigned to the virtual router port of the default VLAN within this Group. After you enter the address, press **<Enter>**.

- c. The following prompt displays:

IP Subnet Mask (0xfffff00):

The default IP subnet mask (in parentheses) is automatically derived from the default VLAN IP address class. Press **<Enter>** to select the default subnet mask or enter a new subnet mask in dotted decimal notation or hexadecimal notation and press **<Enter>**.

- d. The following prompt displays:

IP Broadcast Address (198.200.10.255):

The default IP broadcast address (in parentheses) is automatically derived from the default VLAN IP address class. Press **<Enter>** to select the default IP broadcast address or enter a new broadcast address in dotted decimal notation or hexadecimal notation and press **<Enter>**.

- e. The following prompt displays:

Description (30 chars max):

Enter a useful description for this virtual IP router port using alphanumeric characters. The description may be up to 30 characters long. Press **<Enter>**.

- f. The following prompt displays:

```
IP RIP Mode {Deaf (d),  
Silent (s),  
Active (a),  
Inactive (i)} (s):
```

Define the RIP mode in which the virtual router port will operate. RIP (Router Information Protocol) is a network-layer protocol that enables the default VLAN in this Group to learn and advertise routes. The RIP mode can be set to one of the following:

Silent. The default setting shown in parentheses. RIP is active and receives routing information from other VLANs, but does not send out RIP updates. Other VLANs will not receive routing information concerning the default VLAN in this Group and will not include the VLAN in their routing tables. Simply press **<Enter>** to select Silent mode.

Deaf. RIP is active and sends routing information to other VLANs, but does not receive RIP updates from other VLANs. The default VLAN in this Group will not receive routing information from other VLANs and will not include other VLANs in its routing table. Enter **d** and press **<Enter>** to select Deaf mode.

Active. RIP is active and both sends and receives RIP updates. The default VLAN in this Group will receive routing information from other VLANs and will be included in the routing tables of other VLANs. Enter **a** and press **<Enter>** to select Active mode.

Inactive. RIP is inactive and neither sends nor receives RIP updates. The default VLAN in this Group will neither send nor receive routing information to/from other VLANs. Enter **i** and press **<Enter>** to select Inactive mode.

- g. You can now configure IPX routing on this port. The following message displays:

```
Enable IPX? (y) :
```

Press **<Enter>** if you want to enable IPX Routing on this virtual router port. If you do not enable IPX, then the default VLAN in this WAN Group will not be able to route IPX data. You can set up a virtual router port to route both IP and IPX traffic.

If you don't want to enable IPX routing for the default VLAN in this Group, enter **n** and press **<Enter>**. You can always set up IPX routing for other VLANs within this Group.

You are done configuring this WAN Routing Group. See the appropriate WAN interface chapter for further information on configuring this Routing service.

- h. After selecting to enable IPX, the following prompt displays:

```
IPX Network:
```

Enter the IPX network address. IPX addresses consist of eight hex digits and you can enter a minimum of one hex digits in this field. If you enter less than eight hex digits, the system prefixes your entry with zeros to create eight digits.

- i. The following prompt displays:

```
Description (30 chars max):
```

Enter a useful description for this virtual IPX router port using alphanumeric characters. The description may be up to 30 characters long. Press **<Enter>**.

- j. The following prompt displays:

```
IPX Delay in ticks (0):
```

Enter the number of ticks you want for the IPX network. A tick is about 1/18th of a second. The default is 0.

- k. After entering a description, the following prompt displays:

```

IPX RIP and SAP mode {RIP and SAP active (a)
RIP only active (r)
RIP and SAP inactive (i)}
RIP and SAP triggered (t)}           (a):
    
```

Select how you want the IPX protocols, RIP (router internet protocol) and SAP (service access protocol), to be configured for the default VLAN in this Group. RIP is a network-layer protocol that enables this VLAN to learn routes. SAP is also a network-layer protocol that allows network services, such as print and files services, to advertise themselves. The choices are:

RIP and SAP active. The default setting. The default VLAN to which this IPX router port is attached participates in both RIP and SAP updates. RIP and SAP updates are sent and received through this router port. Simply press **<Enter>** to select RIP and SAP active.

RIP only active. The default VLAN to which this IPX router port is attached participates in RIP updates only. RIP updates are sent and received through this router port. Enter an **r** and press **<Enter>** to select RIP only active.

RIP and SAP inactive. The IPX router port is active, but the default VLAN to which it is attached does not participate in either RIP nor SAP updates. Enter an **i** and press **<Enter>** to select RIP and SAP inactive.

RIP and SAP triggered. The IPX router port is active, but RIP and SAP information will be sent out on the port only when a network change has occurred. This option is more cost effective for WAN links and is best suited for smaller network environments that don't change often. Enter a **t** and press **<Enter>** to select RIP and SAP triggered.

When you are done entering Router parameters, a message similar to the following displays:

```

GROUP 5 has been added to the system
    
```

You should now follow the instructions for configuring a WAN Routing Service described in the appropriate WAN interface chapter.

Creating an ATM CIP Group

After entering basic Group information as described in *Step 1. Entering Basic Group Information* on page 24-22, you should have answered **Yes** to the following prompt:

Enable ATM CIP? (n):

if you want this Group to support ATM Classical IP (CIP). ATM CIP Groups are different from other Groups. CIP Groups must be created if there are devices in the ATM network that support only Classical IP or require CIP to communicate over ATM. The following steps complete the configuration of the ATM CIP Group.

- a. After answering **y** to the **Enable ATM CIP?** prompt, the following prompt displays:

IP Address:

Enter the IP address for this virtual router port in dotted decimal notation or hexadecimal notation (e.g., 198.206.181.10). This IP address is assigned to the virtual router port of the default VLAN within this Group. After you enter the address, press **<Enter>**.

- b. The following prompt displays:

IP Subnet Mask (0xfffff00):

The default IP subnet mask (in parentheses) is automatically derived from the default VLAN IP address class. Press **<Enter>** to select the default subnet mask or enter a new subnet mask in dotted decimal notation or hexadecimal notation and press **<Enter>**.

- c. The following prompt displays:

IP Broadcast Address (198.200.10.255):

The default IP broadcast address (in parentheses) is automatically derived from the default VLAN IP address class. Press **<Enter>** to select the default IP broadcast address or enter a new broadcast address in dotted decimal notation or hexadecimal notation and press **<Enter>**.

- d. The following prompt displays:

Description (30 chars max):

Enter a useful description for this Classical IP router port using alphanumeric characters. The description may be up to 30 characters long. Press **<Enter>**.

- e. The following prompt displays:

**IP RIP Mode {Deaf (d),
Silent (s),
Active (a),
Inactive (i)} (s):**

Define the RIP mode in which the virtual router port will operate. RIP (Router Information Protocol) is a network-layer protocol that enables the default VLAN in this Group to learn and advertise routes. The RIP mode can be set to one of the following:

Silent. The default setting shown in parentheses. RIP is active and receives routing information from other VLANs, but does not send out RIP updates. Other VLANs will not receive routing information concerning the default VLAN in this Group and will not include the VLAN in their routing tables. Simply press **<Enter>** to select Silent mode.

Deaf. RIP is active and sends routing information to other VLANs, but does not receive RIP updates from other VLANs. The default VLAN in this Group will not receive routing information from other VLANs and will not include other VLANs in its routing table. Enter **d** and press **<Enter>** to select Deaf mode.

Active. RIP is active and both sends and receives RIP updates. The default VLAN in this Group will receive routing information from other VLANs and will be included in the routing tables of other VLANs. Enter **a** and press **<Enter>** to select Active mode.

Inactive. RIP is inactive and neither sends nor receives RIP updates. The default VLAN in this Group will neither send nor receive routing information to/from other VLANs. Enter **i** and press **<Enter>** to select Inactive mode.

- f. The following prompt displays:

MTU Size(default value: 9180):

Set the Maximum Transmit Unit size for the group. The default is 9180 bits, but it can be anywhere between 0 and 18000.

When you are done entering Router parameters, a message similar to the following displays:

GROUP 6 has been added to the system

You should now follow the instructions for configuring an ATM Classical IP Service described in Chapter 36, "Configuring ATM Services."

IPX Routing Over ATM

IPX routing is not supported directly over ATM. IPX can be routed by the OmniSwitch and switched out one of the ATM services. See Chapter 36, "Configuring ATM Services," for more information.

Creating a 1483 Group

After entering basic Group information as described in *Step 1. Entering Basic Group Information* on page 24-22, you should have answered **Yes** to the following prompt:

Enable 1483 Routed Format? (n):

if you want this Group to support 1483 routed format groups. ATM 1483 Groups are different from other Groups. 1483 Groups must be created if there are devices in the ATM network that support only using RFC 1483 ATM method of routing. The following steps complete the configuration of the RFC 1483 ATM Group.

- a. After answering **y** to the **Enable 1483 Routed Format?** prompt, the following prompt displays:

IP Address:

Enter the IP address for this virtual router port in dotted decimal notation or hexadecimal notation (e.g., 198.206.181.10). This IP address is assigned to the virtual router port of the default VLAN within this Group. After you enter the address, press **<Enter>**.

- b. The following prompt displays:

IP Subnet Mask (0xfffff00):

The default IP subnet mask (in parentheses) is automatically derived from the default VLAN IP address class. Press **<Enter>** to select the default subnet mask or enter a new subnet mask in dotted decimal notation or hexadecimal notation and press **<Enter>**.

- c. The following prompt displays:

IP Broadcast Address (198.200.10.255):

The default IP broadcast address (in parentheses) is automatically derived from the default VLAN IP address class. Press **<Enter>** to select the default IP broadcast address or enter a new broadcast address in dotted decimal notation or hexadecimal notation and press **<Enter>**.

- d. The following prompt displays:

Description (30 chars max):

Enter a useful description for this Classical IP router port using alphanumeric characters. The description may be up to 30 characters long. Press **<Enter>**.

- e. The following prompt displays:

**IP RIP Mode {Deaf (d),
Silent (s),
Active (a),
Inactive (i)} (s):**

Define the RIP mode in which the virtual router port will operate. RIP (Router Information Protocol) is a network-layer protocol that enables the default VLAN in this Group to learn and advertise routes. The RIP mode can be set to one of the following:

Silent. The default setting shown in parentheses. RIP is active and receives routing information from other VLANs, but does not send out RIP updates. Other VLANs will not receive routing information concerning the default VLAN in this Group and will not include the VLAN in their routing tables. Simply press **<Enter>** to select Silent mode.

Deaf. RIP is active and sends routing information to other VLANs, but does not receive RIP updates from other VLANs. The default VLAN in this Group will not receive routing information from other VLANs and will not include other VLANs in its routing table. Enter **d** and press **<Enter>** to select Deaf mode.

Active. RIP is active and both sends and receives RIP updates. The default VLAN in this

Group will receive routing information from other VLANs and will be included in the routing tables of other VLANs. Enter **a** and press **<Enter>** to select Active mode.

Inactive. RIP is inactive and neither sends nor receives RIP updates. The default VLAN in this Group will neither send nor receive routing information to/from other VLANs. Enter **i** and press **<Enter>** to select Inactive mode.

- f. The following prompt displays:

MTU Size(default value: 9180):

Set the Maximum Transmit Unit size for the group. The default is 9180 bits, but it can be anywhere between 0 and 18000.

When you are done entering Router parameters, a message similar to the following displays:

GROUP 6 has been added to the system

You should now follow the instructions for configuring an ATM Classical IP Service described in Chapter 36, "Configuring ATM Services."

IPX Routing Over ATM

IPX routing is not supported directly over ATM. IPX can be routed by the OmniSwitch and switched out one of the ATM services. See Chapter 36, "Configuring ATM Services," for more information.

Viewing Current Groups

The **gp** command provides information on all currently defined Groups in a switch including Group number, network address, protocol type, and encapsulation type. You can obtain information on all groups in a switch by entering:

```
gp
```

A screen similar to the following displays:

Group ID (:VLAN ID)	Group Description	Network Address (IP Subnet Mask) or (IPX Node Addr)	Proto/ Encaps
1	Default GROUP (#1)	198.206.182.115 (ff.ff.ff.00)	IP / ETH2
2	New GROUP (#2)	198.206.101.12 (ff.ff.ff.00)	IP / SNAP
3	New GROUP (#3)	198.206.181.10 (ff.ff.ff.00)	IP/ 1490
4	New Group (#4)	198.206.183.44 (ff.ff.ff.00) 12314526 (0020da:020484)	IP / ETH2 IPX / 8023
5	New GROUP	198.206.143.11 (ff.ff.ff.00)	CIP / 1483

You can also get information on a specific Group by entering **gp** followed by the Group number. For example,

```
gp 3
```

displays information just on Group 3:

Group ID (:VLAN ID)	Group Description	Network Address (IP Subnet Mask) or (IPX Node Addr)	Proto/ Encaps
3	New GROUP (#3)	198.206.181.10 (ff.ff.ff.00)	IP / 1490

The following sections describe the columns in this table:

Group ID (:VLAN ID). The identification number assigned to this Group when it was created through the **crgp** command. The Group identifier is typically consistent network-wide (i.e., Group 3 in this switch should be the same Group as Group 3 configured in all other OmniSwitches in the network). If this Group contains any VLANs, then they will be listed below the Group number. If the default VLAN in the Group supports both IP and IPX routing, then information on both (network address, etc) will display. Group 4 in the screen sample above shows a case where both IP and IPX routing are supported.

Group Description. The textual description of this Group that was entered when the Group was created or modified. This description is limited to 30 characters.

Network Address (IP Subnet Mask) or (IPX Node Addr). For each virtual router port configured, two addresses are listed. Both of these addresses were configured when the Group was created or modified through **crgp** or **modvl**. The first address is the Network Address, which is the address of the virtual router port for the default VLAN (VLAN #1) in this Group. For an IP virtual router port, this address is the IP address, which is shown in dotted decimal format. For an IPX virtual router port, this address is the IPX network address, which is shown as eight hex characters.

A second address is displayed below the Network address. For IP, this address is the IP Subnet Mask, which is normally derived from the default VLAN IP address class. For IPX, this address is the IPX Node Address.

Proto/Encaps. For each Group or VLAN listed, the top field is the Protocol supported by this virtual router port. Possible values in the field are: **IP** (IP router), **IPX** (IPX router), and **CIP** (Classical IP Group with CIP router). If you configured an IP and an IPX router port, then two router entries will be listed—one with a Protocol of IP and the other with a Protocol of IPX.

The bottom field is the encapsulation used for outgoing frames on the router port. This encapsulation was configured when the router port was configured. Possible values for this field depend on the Protocol and type of Group.

Frame Relay WAN Groups will always display **1490** to indicate RFC 1490 encapsulation is performed on frames. ATM Classical IP (CIP) Groups will display **1483** to indicate RFC 1483 encapsulation is performed on frames.

IP and IPX routers have additional possible encapsulation types. For IP virtual router ports, the possible encapsulation types are as follows:

- **ETH2** Ethernet II
- **SNAP** Ethernet 802.3 SNAP
- **FDDI** FDDI
- **8025** Token Ring 802.5
- **TSRS** Token Ring Source Routing

For IPX virtual router ports, the possible encapsulation types are as follows:

- **ETH2** Ethernet II
- **LLC** Ethernet 802.3 LLC
- **SNAP** Ethernet 802.3 SNAP
- **8023** Ethernet 802.3 (Novell raw)
- **FDDI** FDDI SNAP
- **FSRS** FDDI Source Routing SNAP
- **FLLC** FDDI LLC
- **FSRL** FDDI Source Routing LLC
- **8025** Token Ring SNAP
- **TSRS** Token Ring Source Routing SNAP
- **TLLC** Token Ring LLC
- **TSRL** Token Ring Source Routing LLC

Modifying a Group or VLAN

After creating a Group (through **crgp**) or VLAN (through **cratvl**, see Chapters 25 and 27), you can change any of their parameters through the **modvl** command. In addition, if you did not set up a virtual router port (IP or IPX) during the initial Group or VLAN configuration, you can set one up with **modvl**. To use this command, enter **modvl** followed by the Group number and VLAN number to change. For example, to modify parameters in Group 2, VLAN 1, enter:

```
modvl 2
```

Note that you do not need to specify a VLAN number to modify the default VLAN within a Group. To modify parameters in Group 2, VLAN 2, you would enter:

```
modvl 2:2
```

A screen similar to the following displays.

Current values associated with GROUP 2.1 are as follows:

```
1) GROUP Number      - 2:1
2) Description       - New GROUP (#2)
IP Parameters:
3) IP enabled        - Y
4) IP Network Address - 198.206.101.12
5) IP Subnet Mask    - 255.255.255.0
6) IP Broadcast Address - 198.206.101.255
7) Router Description - Router Port #2
8) RIP Mode         - Silent
                    {Active (a), Inactive (i), Deaf (d), Silent (s)}
9) Routing disabled - N
11) Default Framing - Ethernet II
                    {Ethernet II(e), Ethernet 802.3 (8), fddi (f),
                    token ring (t), source route token ring (s)}
IPX parameters:
12) IPX enabled      - N

(save/quit/cancel)
:
```

The Group number at the top of this sample screen is followed by the number 1 (**GROUP 2.1**), meaning that the information applies to default VLAN #1 in this Group. If this screen displayed information on Group 2, VLAN 2, then this field would read **GROUP 2:2**.

The colon prompt (:) at the bottom of the screen is used to prompt for user input. To change a value, type the line number of the item you want to change, followed by an equal sign (=) and the new value. For example, to set a new description you could enter:

```
2=Engineering
```

All of the **modvl** parameters are described in the section for creating a new Group, *Creating a New Group* on page 24-21.

◆ Note ◆

Line numbering for the **modvl** command will vary depending on whether you have an IP or IPX router configured. Each type of router contains several parameters that require extra line numbers.

Viewing Your Changes

When you enter a change at the colon prompt, the **modvl** screen does not normally refresh. If you want to see the current Group or VLAN settings, including any changes you made, enter a question mark (?) at the colon prompt. The **modvl** screen will refresh.

Saving Your Changes

Once you have entered all your modifications and you want to save them, type **save** at the colon prompt. You will exit the **modvl** command and your changes will take effect.

Canceling Your Changes

You can also exit the **modvl** command without saving any changes you made in the current session. Simply enter **cancel** at the colon prompt or enter **<Ctrl>-d**. The **modvl** command will end and none of the changes you made will be saved.

Changing the IP Address

Changing the IP address can also affect the Subnet Mask and the Broadcast Address. The new IP address means that the Subnet Mask and Broadcast Address must be re-generated and the following message displays:

**New IP address generates new subnet and broadcast address
Enter '?' to view the changes**

The system automatically creates new Subnet Mask and Broadcast addresses based on the new IP address. If you enter a question mark (?) at this point you could view these changes.

If you remove the last IP address in the system, you will see a warning message that SNMP (and other applications) are now inoperational.

Changing the IP Subnet Mask

Changing the IP Subnet Mask can also affect the IP Broadcast Address. The new Subnet Mask means that the Broadcast Address must be re-generated and the following message displays:

New mask caused change in broadcast address

The system automatically created a new Broadcast address based on the new Subnet Mask. If you entered a question mark (?) at this point you could view these changes.

Enabling IP or IPX Routing

If you enable IP or IPX routing by setting the corresponding **modvl** lines from **N** to **Y**, then the screen automatically refreshes with additional lines for the new router port parameters. All lines are set to router defaults. The router defaults are as follows:

IP Router

IP Network Address	0.0.0.0
IP Subnet Mask	0.0.0.0
IP Broadcast Address	0.0.0.0
Router Description	(no description shown for default)
Routing Disabled	No
RIP Mode	Silent
Default Framing Type	Ethernet II

IPX Router

IPX Network Address	0x0
Router Description	(no description shown for default)
Delay in Ticks	0
RIP/SAP Mode	RIP and SAP are active
Default Framing Type	Ethernet II

You can change any of these defaults as you would any other **modvl** parameters: enter the line number, followed by an equal sign (=) and the new parameter.

◆ Note ◆

You must at least enter a Network Address for a new router or you will not be able to save the configuration.

Deleting a Group

You can delete a Group as long as it does not contain any virtual ports. The default Group, Group #1, cannot be deleted. To delete a Group, enter **rmgp** followed by the Group number you want to delete. For example, if you wanted to delete Group 5, you would enter:

```
rmgp 5
```

If the Group does not contain any virtual ports, then a confirmation message displays:

```
GROUP 5 removed.
```

If the Group still contains virtual ports, then a message similar to the following displays:

```
GROUP 5 has active entries, you must remove  
these prior to removing the GROUP (use rmvp for this).
```

You must first remove the Group's virtual ports before the Group can be removed. The **rmvp** command allows you to remove virtual ports. See *Deleting a Virtual Port* on page 24-54 for information on using this command.

◆ Note ◆

Some commands in the Bridge Management menu (described in Chapter 22, "Configuring Bridging Parameters") require you to select a Group before making configuration changes. If you delete the currently selected Group with **rmgp**, then the new currently selected Group reverts to the default Group, Group #1.

Adding Virtual Ports

You can add virtual ports to a Group at any time after the Group is created. The **addvp** command allows you to add one or more ports to a Group you specify. If you have used the **crgp** command to add virtual ports, then you will find the **addvp** command fields very familiar.

To use **addvp**, enter the command followed by the Group number to which you want to add the port. Next, specify the port or ports you want to add.

addvp <Group Number for port> <Module Slot>/<Port Number>

For example, if you wanted to add ports 4 through 6 on the module in slot 4 to Group #5, then you would specify:

addvp 5 4/4-6

The procedure for using **addvp** is as follows:

1. Enter **addvp** followed by the Group number where you want this port to reside, followed by the physical slot and port numbers you want to configure.
2. If you enter a port that is already assigned to another Group, then you will be prompted on whether or not you want to change its assignment. A message similar to the following displays for each port that you enter:

**4/4 - This interface has already been assigned to GROUP 1 -
(Default GROUP #1).
Do you wish to remove it from that GROUP and assign it (with
new configuration values) to this GROUP (n)?**

Simply enter a **y** at each port prompt to change its Group assignment and begin setting port parameters. You could also enter a **c** at this prompt to accept all default port parameters and skip port configuration questions. If you enter a **c**, *all* remaining ports are automatically added to the Group with default settings, and your work is complete.

3. The virtual port configuration menu displays:

Modify Ether/8 Vport 4/4 Configuration

1) Vport	: 9
2) Description	:
3) Bridge Mode	: Auto-Switched
31) Switch Timer	: 60
4) Flood Limit	: 192000
5) Output Format Type	: Default (IP-Eth II, IPX-802.3)
6) Ethernet 802.2 Pass Through	: Yes
7) Admin, Operational Status	: Enabled, inactive
8) Mirrored Port Status	: Disabled, available
9) MAC Address	: 000000:000000

Command {Item=Value/?/Help/Quit/Redraw/Next/Previous/Save} (Redraw) :

Descriptions for each of the fields in this display begin on page 24-32. To change any default value, enter the line number for the item, an equal sign (=), and then the value for the parameter. When you have completed the configuration for this port, enter **save** to save all configured settings.

Modifying a Virtual Port

You can modify a virtual port through the **modvp** command. The **modvp** command is very similar to the **addvp** command and the port configuration phase of the **crgp** command. To use **modvp**, enter the command, followed by the Group number for the port, and the physical slot and port number for the port:

```
modvp <Group Number for port> <Module Slot>/<Port Number>
```

You can specify only one port at a time. For example, if you wanted to modify the parameters for Port 7 on the module in Slot 4, and the Port currently resides in Group 6, then you would enter:

```
modvp 6 4/7
```

The procedure for using **modvp** is as follows:

1. Enter **modvp** followed by the Group number where the port currently resides, the physical slot and port number.
2. A prompt displays requesting your confirmation:

```
Modify local port 7 (Virtual port (#14)) ? (y) :
```

Simply press **<Enter>** if this is the correct virtual port. The Virtual Port number in parentheses (**Virtual Port #14** in this case) is the virtual port number within this entire OmniSwitch or Omni Switch/Router. Virtual ports are numbered sequentially within the switch, not within a Group or VLAN.

3. The virtual port configuration menu displays:

Modify Ether/8 Vport 4/7 Configuration

```
1) Vport                : 9
2) Description          :
3) Bridge Mode         : Auto-Switched
   31) Switch Timer     : 60
4) Flood Limit         : 192000
5) Output Format Type   : Default (IP-Eth II, IPX-802.3)
6) Ethernet 802.2 Pass Through : Yes
7) Admin, Operational Status : Enabled, inactive
8) Mirrored Port Status : Disabled, available
9) MAC Address         : 000000:000000
```

```
Command {Item=Value/?/Help/Quit/Redraw/Next/Previous/Save} (Redraw) :
```

Descriptions for each of the fields in this display begin on page 24-32. To change any default value, enter the line number for the item, an equal sign (=), and then the value for the parameter. When you have completed the configuration for this port, enter **save** to save all configured settings.

Deleting a Virtual Port

You can delete a virtual port from its existing Group by using the **rmvp** command. When you remove a virtual port, the port is moved to the default switch Group, Group #1, and all port parameters are reset to defaults except for the port name. For example, if you configured a port with a special flood limit and customized translation settings and you then removed the port, you would lose those port settings.

To remove a port, enter the **rmvp** command, followed by the Group number where the port currently resides and the physical slot and port number for the port:

```
rmvp <Group number> <Module Slot>/<Port Number>
```

For example, to delete Port 7 on the module in Slot 4, and the Port currently resides in Group 6, you would enter:

```
rmvp 6 4/7
```

A prompt displays requesting that you confirm the deletion:

```
Local port 7 (Virtual po...) is attached to this slot/interface - remove? (n):
```

Enter a **y** and press **<Enter>** to remove the port. Another message displays confirming the deletion:

```
BRIDGE port on 4/7 moved to GROUP 1.
```

If the port you specified did not exist in the Group you specified in the **rmvp** command, then a message similar to the following would display:

```
Specified port(s) not found on GROUP 6.
```

Viewing Information on Ports in a Group

The **via** command allows you to view port attachments associated with a specified Group or all Groups in a switch. Entering

```
via
```

displays summary information for all virtual ports in the switch. You can also display virtual interface attachments for a specific Group by specifying the Group ID after the **via** command. For example, to view ports for Group 2, you would enter

```
via 2
```

The same type of information is displayed for a single Group as is displayed for all Groups. The following screen shows a sample from the **via** command when specified without a Group ID.

GROUP Interface Attachments For All Interfaces

GROUP: Slot/Intf	Description	Service/ Instance	Protocol	Admin Status
1.1 : *	GROUP #1.0 IP router vport	Rtr / 1	IP	Enabled
2.1 : *	for group 2	Rtr / 2	IP	Enabled
1:2/1	Virtual port (#2)	Brg / 1	Tns	Enabled
1:2/2	Virtual port (#3)	Brg / 1	Tns	Enabled
1:2/3	Virtual port (#4)	Brg / 1	Tns	Enabled
2:2/4	finance server	Brg / 1	Tns	Enabled
1:2/5	Virtual port (#6)	Brg / 1	Tns	Enabled
1:2/6	Virtual port (#7)	Brg / 1	Tns	Enabled
1:2/7	Virtual port (#8)	Brg / 1	Tns	Enabled
1:2/8	Virtual port (#9)	Brg / 1	Tns	Enabled
1:3/1	Virtual port (#1)	Brg / 1	Tns	Enabled
1:4/1	Virtual port (#10)	Brg / 1	Tns	Enabled
1:4/2	Virtual port (#11)	Brg / 1	Tns	Enabled
1:4/3	Virtual port (#12)	Brg / 1	Tns	Enabled
1:4/4	Virtual port (#13)	Brg / 1	Tns	Enabled
1:4/5	Virtual port (#14)	Brg / 1	Tns	Enabled
1:4/6	Virtual port (#15)	Brg / 1	Tns	Enabled

GROUP: Slot/Intf. **GROUP** is the group number to which this port is assigned. When the Group displays as a Group number followed by a decimal and a 1 (1.1 and 2.1 in the above sample), it represents the router port on the default VLAN within that Group. **Slot** is the position in the chassis of the switching module where this port is located. **Intf** (Interface) is the physical port on the switching module. When the Slot and Interface are shown as an asterisk (*)—as the top two entries in the above table display—it represents as virtual router port that does not have a corresponding physical interface.

Description. The textual description entered for either the virtual router port or the virtual switch port. This description was entered through **crgp** or **modvl** for virtual router ports, or through **crgp**, **addvp**, or **modvp** for virtual switch ports.

Service/Instance. **Service** is the service type configured for this port. **Instance** is an identifier of this service type within the switch. For example, multiple virtual router ports within the switch will be labelled consecutively (1, 2, 3, etc.), and will each have a different **Instance** number.

Values for the service type are as follows:

- **Rtr** Virtual router port
- **Brg** Virtual bridge port
- **Tnk** Virtual trunk port (used for ATM, FDDI, and WAN)
- **T10** 802.10 FDDI service port
- **FRT** Frame Relay trunk port
- **Lne** LAN Emulation service port
- **CIP** Classical IP service port
- **Vlc** VLAN Clusters (X-LANE) service port

Protocol. The bridging protocol for virtual ports and services or the routing protocol for virtual router ports. Possible values are:

- **Tns** Transparent bridge. Bridges maintain a dynamic table of known MAC addresses on connected segments. The table is used to make forwarding decisions. When a frame is received that contains a destination address that matches an address in the table, it is forwarded to designated bridge ports that are in forwarding state.
- **SR** Source Routing Bridge. Normally used in Token Ring environments. Routing information is determined by looking at the Routing Information Field (RIF) in a frame. The RIF contains the segment and bridge numbers that create the path to the destination. Virtual ports are configured as Source Routing bridges through the **src** command, which is described in Chapter 21, "Managing Token Ring."
- **SRT** Source Routing Transparent. Normally used in Token Ring environments. Allows Source Routing and Transparent bridges to coexist. The Source Routing Transparent Bridge will form a Spanning Tree with other Transparent Bridges and Source Routing Transparent Bridges and will forward frames that do not contain a Routing Information Field (RIF) to destinations reachable by the Spanning Tree. If the bridge detects routing information in the RIF, it will forward it the same way Source Routing bridges do. Virtual ports are configured as Source Routing Transparent bridges through the **src** command, which is described in Chapter 21, "Managing Token Ring."
- **IP** IP Routing Protocol. Routing Information Protocol (RIP) used to learn routes from neighboring routers. You configure an IP router through the **crgp** or **modvl** commands. Other IP routing parameters can be set through the Networking menu commands, which are described in Chapter 30, "IP Routing."
- **IPX** IPX Routing Protocol. Uses RIP to learn routes from neighboring routers and the Service Advertising Protocol (SAP) to maintain a database of network services for requesting workstations. Other IPX routing parameters can be set through the Networking menu commands, which are described in Chapter 32, "IPX Routing."
- **CIP** Classical IP Routing (RFC 1577). Classical IP is necessary when an ATM network contains devices that support only CIP. This type of routing is configured when you initially create a Group through the **crgp** command.
- **FR** Frame Relay IP Routing. WAN Routing Groups are configured slightly different from other Groups. Frame Relay IP Routing is IP Routing with some enhancements to account for the Frame Relay network.

Admin Status. Indicates whether the port is administratively **Enabled** or **Disabled**. When **Enabled**, the port can transmit and receive data as long as a cable is connected and no physical or operational problems exist. When **Disabled**, the port will not transmit or receive data even if a cable is connected and the physical connection is operational. You can set the Admin Status during port configuration phase of the **crgp**, **addvp**, or **modvp** commands.

Viewing Detailed Information on Ports

The **vi** command displays detailed information about virtual ports. Entering

```
vi
```

displays information for all virtual ports in the switch. You can also display information for only ports in a specific Group by specifying the Group ID after the **vi** command. For example, to view information only for ports in Group 6, you would enter

```
vi 6
```

The same type of information is displayed for a single Group as is displayed for all Groups. The following screen shows a sample from the **vi** command when specified without a Group ID.

Virtual Interface Summary Information- For All Interfaces

Group	Intf	Slot/ Type/ Inst/Srvc	MAC Address	Prt	Encp	Admin	Status			
							Oper	Spn	Tr	Mode
1	All	Rtr/ 1	0020da:020d40	IP	ETH2	Enabl	Active	N/A	N/A	
2	All	Rtr/ 2	0020da:020d43	IP	ETH2	Enabl	Active	N/A	N/A	
2	All	Rtr/ 3	0020da:020d44	IP	ETH2	Enabl	Active	N/A	N/A	
1	3/1	Brg/ 1/ 1	0020da:048730	Tns	DFLT	Enabl	Inactv	Disabl	Bridged	
1	4/1	Brg/ 1/ na	0020da:030990	Tns	DFLT	Enabl	Active	Fwdng	Bridged	
1	4/2	Brg/ 1/ na	0020da:030991	Tns	DFLT	Enabl	Inactv	Disabl	Bridged	
1	4/3	Brg/ 1/ na	0020da:030992	Tns	DFLT	Enabl	Inactv	Disabl	Bridged	
1	4/4	Brg/ 1/ na	0020da:030993	Tns	DFLT	Enabl	Inactv	Disabl	Bridged	
1	4/5	Brg/ 1/ na	0020da:030994	Tns	DFLT	Enabl	Inactv	Disabl	Bridged	
1	4/6	Brg/ 1/ na	0020da:030995	Tns	DFLT	Enabl	Inactv	Disabl	Bridged	
1	4/7	Brg/ 1/ na	0020da:030996	Tns	DFLT	Enabl	Inactv	Disabl	Bridged	
2	4/8	Brg/ 1/ na	0020da:030997	Tns	DFLT	Enabl	Inactv	Disabl	Bridged	
1	5/1	Brg/ 1/ na	0020da:022860	Tns	DFLT	Enabl	Inactv	Disabl	Bridged	

Group. The Group number to which this port is currently assigned.

Slot/Intf. The slot (**Slot**) is the position in the chassis of the switching module where this port is located. The interface (**Intf**) is the physical port on the switching module. If this column reads **All**, then this port is a router port that supports all virtual ports in the Group.

Type/Inst/Srvc. The Service Type (**Type**), Instance (**Inst**) of this Service Type in the switch, and service number (**Srvc**) for this virtual port. Service Type values are as follows:

- **Rtr** Virtual router port
- **Brg** Virtual bridge port
- **Tnk** Virtual trunk port (used for ATM, FDDI, and WAN)
- **T10** 802.10 FDDI service port
- **FRT** Frame Relay trunk port
- **Lne** LAN Emulation service port
- **Vlc** VLAN clusters (X-LANE) service port
- **CIP** Classical IP service port

The Instance (**Inst**) is an identifier of this type of service within the switch. For example, if more than one virtual router port is configured in the switch, then each “instance” of a router will be given a different number. The service number (**Srv**) is port-specific. If a port has more than one service configured on it, then each service will be identified by a different service number.

MAC Address. The MAC address for this virtual port. Each virtual port is allocated a MAC address.

Prt. The bridging or routing protocol supported by this virtual port. Descriptions of these protocol types are provided on page 24-56. Possible values are:

- **Tns** Transparent Bridge
- **SR** Source Routing Bridge
- **SRT** Source Routing Transparent Bridge
- **IP** IP Routing Protocol
- **IPX** IPX Routing Protocol
- **CIP** Classical IP Routing (RFC 1577)
- **FR** Frame Relay IP Routing

Encp. Encapsulation used for outgoing packets on this virtual router or switch port. Possible encapsulation values are:

- **DFLT** Default format for this switch port (differs for each interface type)
- **SWCH** Frame translations have been customized through the Switch menu
- **ETH2** Ethernet II
- **ESNP** Ethernet 802.3 SNAP (virtual router ports)
- **ELLC** Ethernet 802.3 LLC (IPX router ports only)
- **8023** Ethernet 802.3, Novell Raw (IPX router ports only)
- **8025** Token Ring 802.5 SNAP (virtual router ports)
- **TSRS** Token Ring Source Routing SNAP (virtual router ports)
- **TLLC** Token Ring LLC (IPX router ports only)
- **TSRL** Token Ring Source Routing LLC (IPX router ports only)
- **FDDI** FDDI SNAP (virtual router ports)
- **FSRS** FDDI Source Routing SNAP (IPX router ports only)
- **FLLC** FDDI LLC (IPX router ports only)
- **FSRL** FDDI Source Routing LLC (IPX router ports only)
- **1490** Frame Relay Routing (RFC 1490)
- **1483** Classical IP Routing (RFC 1483)
- **SNAP** SNAP (switch ports only)
- **LLC** LLC (switch ports only)

Admin. Indicates whether the port is administratively Enabled or Disabled. When **Enabld**, the port can transmit and receive data as long as a cable is connected and no physical or operational problems exist. When **Disabld**, the port will not transmit or receive data even if a cable is connected and the physical connection is operational. You can set the Administrative Status during the port configuration phase of the **crjgp** command, the **addvp** command, or the **modvp** command. A port can have an Administrative Status of Enabled, but still be operationally Inactive. See the description of the **Oper** column below.

Oper. Indicates the current Operational Status of the port. The port will be Active (**Active**) or Inactive (**Inactv**). If the port is Active, then the port can pass data and has a good physical connection. If it is Inactive, then it may not have a good physical connection and it is not capable of passing data at this time.

Spn Tr. The port's current state as defined by the Spanning Tree Protocol. The possible Spanning Tree States are: Disabled, Blocking, Listening, Learning, and Forwarding. This state controls the action a port takes when it receives and transmits a frame. For ports which are Administratively disabled or Operationally Inactive, this state will be Disabled (**Disabl**), meaning the Spanning Tree algorithm is not active on this port. If the state is **Blocking**, then only BPDUs will be transmitted and received. If the state is **Forwarding**, then both data and BPDU frames will be transmitted and received. This Spanning Tree Protocol state is not applicable to virtual router ports and will read **N/A** for those ports.

Mode. The Bridge Mode currently in use on this port. This mode is chosen during the port configuration phase of the **crgp** command, through the **addvp** command, or through the **modvp** command. It is not applicable to virtual router ports and will read **N/A** for those ports. Possible values are:

- **Bridged** Spanning Tree Bridge.
- **AutoSw** Auto Switch.
- **Optimzd** Optimized Device Switching.

See page 24-32 for a description of these bridge modes.

Viewing Port Statistics

The **vs** command displays transmit and receive statistics for ports in the switch. Entering

```
vs
```

displays statistics for all virtual ports in the switch. You can also display statistics for only ports in a specific Group by specifying the Group ID after the **vs** command. For example, to view statistics only for ports in Group 6, you would enter

```
vs 6
```

You can also display statistics for a specific port by entering the slot and port number after the **vs** command. For example, to view statistics only for Port 1 on the module in Slot 4, you would enter

```
vs 4/1
```

The same type of information is displayed for a single Group or port as is displayed for all ports in a switch. The following screen shows a sample from the **vs** command when specified without any Group or port parameters.

Virtual Interface Statistical Information- For All Interfaces

Slot/ Group	Intf	Service/ Instance	Frames In Out	Octets In Out	UcastPkts In Out	NUcastPkts In Out
1	All	Rtr/ 1				
2	All	Rtr/ 2				
3	All	Rtr/ 3				
1	3/1	Tnk/ 1	0	0	0	0
			0	0	0	0
1	4/1	Brg/ 1	17774	1739560	1707	16067
			684	103048	681	3
1	4/2	Brg/ 1	0	0	0	0
			0	0	0	0
1	4/3	Brg/ 1	0	0	0	0
			0	0	0	0
1	4/4	Brg/ 1	0	0	0	0
			0	0	0	0
1	4/5	Brg/ 1	0	0	0	0
			0	0	0	0
1	4/6	Brg/ 1	0	0	0	0
			0	0	0	0
1	4/7	Brg/ 1	0	0	0	0
			0	0	0	0
1	4/8	Brg/ 1	0	0	0	0
			0	0	0	0
1	5/1	Brg/ 1	0	0	0	0
			0	0	0	0

Group, Slot/Intf. These columns are described for the **vi** command on page 24-58.

Service/Instance. The Service Type (**Service**) and Instance (**Instance**) of this Service Type in the switch.

Service Type values are as follows:

- **Rtr** Virtual router port
- **Brg** Virtual bridge port
- **Tnk** Virtual trunk port (used for ATM, FDDI, and WAN)
- **T10** 802.10 FDDI service port
- **FRT** Frame Relay trunk port
- **Lne** LAN Emulation service port
- **Vlc** VLAN clusters (X-LANE) service port
- **CIP** Classical IP service port

The Instance (**Inst**) is an identifier of this type of service within the switch. For example, if more than one virtual router port is configured in the switch, then each “instance” of a router will be given a different number.

Frames In/Out. The number of frames received or sent from this port. The top number for each port row is the number of frames received, and the bottom number is the number of frames sent. Statistics are not provided for virtual router ports in this display, but they are provided through Networking menu commands. See Chapters 30 and 32 for further information on router port statistics.

Octets In/Out. The number of octets, or bytes, received or sent from this port. The top number for each port row is the number of octets received, and the bottom number is the number of octets sent. Statistics are not provided for virtual router ports, but they are provided through Networking menu commands. See Chapters 30 and 32 for further information on router port statistics.

Ucast Pkts In/Out. The total number of unicast packets received or sent from this port. The top number for each port row is the number of unicast packets received, and the bottom number is the number of unicast packets sent. Statistics are not provided for virtual router ports, but they are provided through Networking menu commands. See Chapters 30 and 32 for further information on router port statistics.

Non Ucast Pkts In/Out. The total number of non-unicast packets received or sent from this port. Non-unicast frames include multicast and broadcast frames. The top number for each port row is the number of non-unicast packets received, and the bottom number is the number of non-unicast packets sent. Statistics are not provided for virtual router ports, but they are provided through Networking menu commands. See Chapters 30 and 32 for further information on router port statistics.

Viewing Port Errors

The **ve** command displays port error statistics for ports in the switch. Entering

```
ve
```

displays error statistics for all virtual ports in the switch. You can also display errors statistics for only ports in a specific Group by specifying the Group ID after the **ve** command. For example, to view errors only for ports in Group 6, you would enter

```
ve 6
```

You can also display error statistics for a specific port by entering the slot and port number after the **ve** command. For example, to view errors only for Port 1 on the module in Slot 4, you would enter

```
ve 4/1
```

The same type of information is displayed for a single Group or port as is displayed for all ports in a switch. The following screen shows a sample from the **ve** command when specified without any Group or port parameters.

Virtual Interface Error Information- For All Interfaces

Group	Slot/ Intf	Service/ Instance	Buffer Discards		Error Discards	
			In	Out	In	Out
2	All	Rtr/ 1				
3	All	Rtr/ 2				
1	All	Rtr/ 1				
1	3/1	Tnk/ 1	0	0	0	0
1	4/1	Brg/ 1	0	0	0	0
1	4/2	Brg/ 1	0	0	0	0
1	4/3	Brg/ 1	0	0	0	0
1	4/4	Brg/ 1	0	0	0	0
1	4/5	Brg/ 1	0	0	0	0
1	4/6	Brg/ 1	0	0	0	0
1	4/7	Brg/ 1	0	0	0	0
1	4/8	Brg/ 1	0	0	0	0
1	5/1	Brg/ 1	0	0	0	0

Group, Slot/Intf. These columns are described for the **vi** command on page 24-58.

Service/Instance. The Service Type (**Service**) and Instance (**Instance**) of this Service Type in the switch. Service Type values are as follows:

- **Rtr** Virtual router port
- **Brg** Virtual bridge port
- **Tnk** Virtual trunk port (used for ATM, FDDI, and WAN)
- **T10** 802.10 FDDI service port
- **FRT** Frame Relay trunk port
- **Lne** LAN Emulation service port
- **Vlc** VLAN clusters (X-LANE) service port
- **CIP** Classical IP service port

Viewing Port Errors

The Instance (**Inst**) is an identifier of this type of service within the switch. For example, if more than one virtual router port is configured in the switch, then each “instance” of a router will be given a different number.

Buffer Discards In/Out. For transmit (**Out**) and receive (**In**), the number of frames discarded due to a lack of buffer space. Buffer discard information is not provided for virtual router ports.

Error Discards In/Out. For transmit (**Out**) and receive (**In**), the number of frames discarded due to errors. Error discard information is not provided for virtual router ports.

Port Mirroring

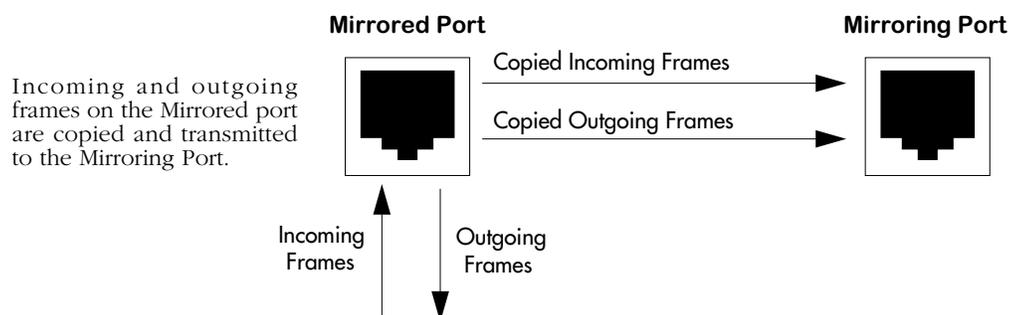
You can set up Port Mirroring for any pair of Ethernet (10 or 10/100 Mbps) or Token Ring within the same switch chassis. Ethernet ports supporting port mirroring include 10BaseT (RJ-45), 10BaseFL (fiber), 10Base2 (BNC), and 10Base5 (AUI) connectors. When you enable port mirroring, the active, or “mirrored,” port transmits and receives network traffic normally, and the “mirroring” port receives a copy of all transmit and receive traffic to the active port. You can connect an RMON probe or network analysis device to the mirroring port to see an exact duplication of traffic on the mirrored port without disrupting network traffic to and from the mirrored port.

Port mirroring is supported on OmniSwitch and Omni Switch/Router chassis for Ethernet (10 or 10/100 Mbps) and Token Ring ports only. An Ethernet port can only be mirrored by one other Ethernet port; a Token Ring Port can only be mirrored by another Token Ring port. A mirroring port can only mirror one port at a time. Up to five (5) mirroring sessions (mirrored-mirroring port pairs) are supported in a single switch chassis. The mirrored and mirroring ports can be in different Groups and different VLANs.

How Port Mirroring Works

When a frame is received on a Mirrored Port it is copied and sent to the Mirroring Port. The received frame is actually transmitted twice across the switch backplane—once for normal bridging and then again to the Mirroring Port.

When a frame is transmitted by the mirrored port, a copy of the frame is made, tagged with the mirroring port as the destination, and sent back over the switch backplane to the mirroring port. The following diagram illustrates the data flow for a Mirrored-Mirroring port pair.



Relationship Between Mirrored and Mirroring Port

When port mirroring is enabled, there may be some performance degradation since all frames received and transmitted by the Mirrored port need to be copied and sent to the Mirroring port.

What Happens to the Mirroring Port

Once you set up port mirroring and attach cables to the Mirrored and Mirroring ports, the Mirroring port is administratively disabled and no longer a part of the Bridging Spanning Tree. The Mirroring port does not transmit or receive any traffic on its own. In addition, the Admin Status of the mirroring port displays in switch software commands, such as **vi**, as

```
M <slot> <port>
```

where **<slot>** is the slot number of the module containing the mirrored port, and **<port>** is the port number of the mirrored port. For example, if the Admin Status of a port displayed as

M 3 02

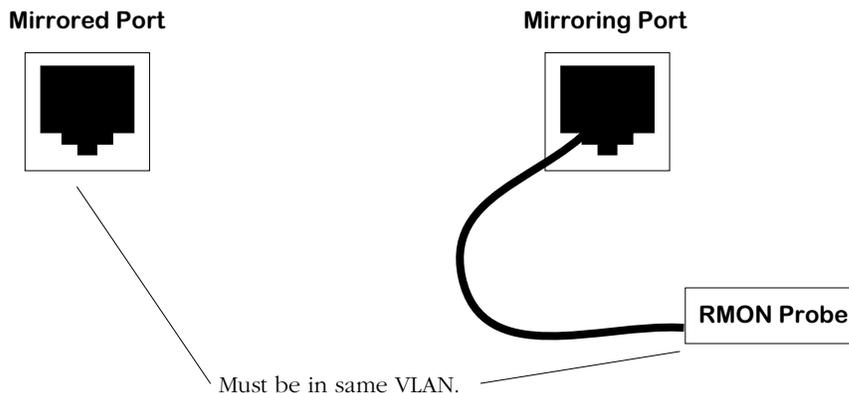
then you would know this port is mirroring traffic for Port 2 on the module in Slot 3.

If a cable is not attached to the Mirrored port, port mirroring will not take place. In this case, the Mirroring Port reverts back to its normally operational state and will bridge frames as if port mirroring were disabled.

Using Port Mirroring With External RMON Probes

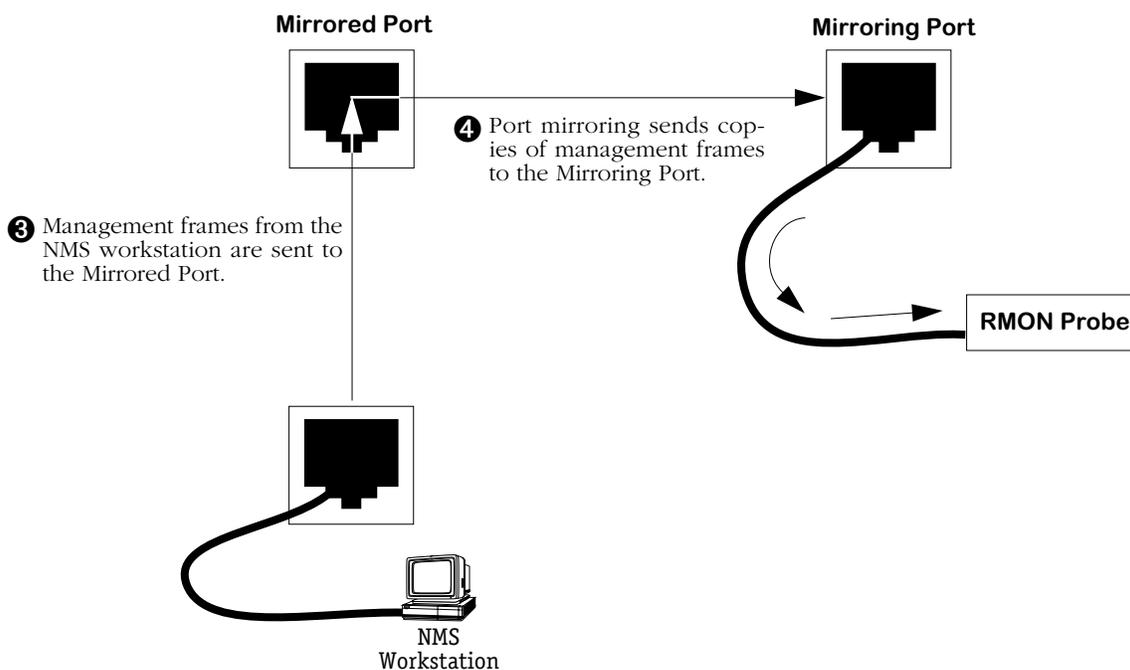
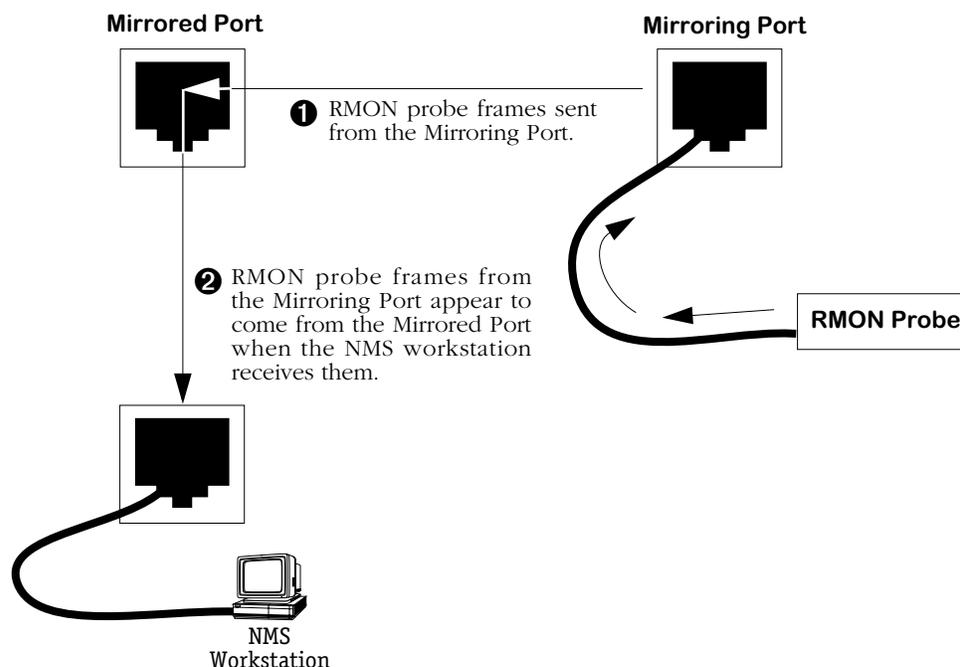
Port mirroring is a helpful monitoring tool when used in conjunction with an external RMON probe. Once you set up port mirroring, the probe can collect all relevant RMON statistics for traffic on the mirrored port. You can also move the Mirrored Port so that the Mirroring Port receives data from different ports. In this way, you can roam the switch and monitor traffic at various ports.

If you attach an external RMON probe to a mirroring port, that probe must have an IP address that places it in the same VLAN as the mirrored port. In addition if you change the mirrored port, then you must again make sure that the RMON probe is in the same VLAN as that new mirrored port.



Mirrored and Mirroring Ports in Same VLAN

Frames received from an RMON probe attached to the Mirroring Port can be seen as being received by the Mirrored Port. These frames from the Mirroring Port are marked *as if they are received on the Mirrored Port* before being sent over the switch backplane to an NMS station. Therefore, management frames from an NMS station that are destined for the RMON probe are first forwarded out the Mirrored Port. After being received on the Mirrored Port, copies of the frames are mirrored out the Mirroring Port—the probe attached to the Mirroring Port receives the management frames. The illustration on the following page shows this data flow.



Port Mirroring Using an External RMON Probe

◆ Important Note ◆

The Mirroring Port is not accessible from the NMS device. From the NMS station, the Mirroring Port will appear disabled or down.

Setting Up Port Mirroring

You set up port mirroring when you add or modify a port through the **addvp** or **modvp** commands. The switch software senses the type of port you are configuring, so it will only prompt you for port mirroring when configuring an Ethernet or Token Ring port. Follow the steps below to set up port mirroring.

1. Start the **addvp** or **modvp** command for the virtual port that you want to mirror.
2. At the **Command** prompt enter **8=e**, press **<Enter>** and you will be prompted for the slot and port number of the “mirroring” port (i.e., the port that can “see” all traffic for this port):

Mirroring vport slot/port ? () :

3. Enter the mirroring port’s slot, a slash (/), the port number, and then press **<Enter>**. The port that you indicate here will be disabled and only capable of receiving duplicate traffic from the mirrored port. If port mirroring is not supported on this port, then the following prompt will display:

mirroring not supported on this port type

After entering the Mirroring slot and port number, the **addvp** or **modvp** screen of options re-displays with the changes you entered. If you are done modifying or adding the port, enter **save** at the **Command** prompt. If using the **addvp** command a message indicating that you have successfully set up the port displays. Port mirroring takes place immediately, so you could now connect a probe or network analyzer to the Mirroring port.

Disabling Port Mirroring

You can disable port mirroring through the **modvp** command. Follow these steps to disable port mirroring.

1. Start the **modvp** command for the virtual port on which you want to disable port mirroring.
2. At the **Command** prompt enter **8=d**, press **<Enter>**. The **modvp** screen re-displays. The **Mirrored Port Status** field should read **Disabled, available**.

Port Monitoring

An essential tool of the network engineer is a network packet capture device. A packet capture device is usually a PC-based computer, such as the Sniffer®, that provides a means for understanding and measuring data traffic of a network. Understanding data flow in a VLAN-based switch presents unique challenges primarily because traffic takes place *inside* the switch, especially on dedicated devices.

The port monitoring feature built into OmniSwitch software allows the network engineer to examine packets to and from a specific Ethernet 10BaseT or Token Ring port. Port monitoring has the following features:

- Software commands to enable and display captured port data.
- Captures data in Network General® file format.
- Limited protocol parsing (basic IP protocols and IPX) in console dump display.
- Data packets time stamped.
- One port monitored at a time.
- RAM-based file system.
- Memory buffer space from 1 MB to 8 MB.
- Statistics gathering and display
- Monitors only Ethernet 10BaseT and Token Ring ports
- Filtering limited to basic packet type—broadcast, multicast or unicast.

You can select to dump real-time packets to the terminal screen, or send captured data to a file. Once a file is captured, you can FTP it to a Sniffer for viewing.

Port Mirroring

An alternate method of monitoring ports is Port Mirroring, which allows a network engineer to attach a Sniffer to one Ethernet or Token Ring port and mirror traffic to and from any other Ethernet or Token Ring port. Port mirroring is described in *Port Mirroring* on page 24-65.

Port Monitoring Menu

The port monitoring commands are contained on the port monitoring menu, which is a sub-menu of the Networking menu. The port monitoring menu displays as follows:

<u>Command</u>	<u>Port Monitoring Menu</u>				
pmon	Port monitor utility				
pmcfg	Configure port monitor parameters				
pmstat	View port monitor statistics				
pmd	Port monitor disable				
pmp	Port monitor pause				
		Main	File	Summary	VLAN
		Interface	Security	System	Services
		/Networking/Monitor %			Networking Help

The commands in this menu are described in the following sections.

RAM Disk System for Data Capture Files

Port monitoring uses a RAM disk for fast temporary storage of data capture files. The RAM disk has a separate directory designation of **/ram**. RAM-based files are created in DOS-FAT format and they are displayed in UPPERCASE.

You can copy files between the **/ram** disk system and the standard **/flash** file system. In addition, files in the RAM disk system are retrievable via FTP. Both the **/ram** file system and the **/flash** file system are accessible by using the UNIX/DOS-style change directory (**cd**) command.

◆ Note ◆

The RAM drive is part of DRAM memory. If you power off or reboot the switch, any files saved in the RAM drive will be lost.

Configuring RAM Drive Resources (pmcfg)

The **pmcfg** command allows you to select the size of the RAM disk file system or to delete the RAM disk. In addition, it allows you to configure the amount of data collected for each packet capture. To begin configuring RAM drive resources, enter

```
pmcfg
```

A screen similar to the following displays:

```
RAM disk size : 1000 Kilobytes
Lines displayed: 1
Change any of the above (y/n)? (n)
```

To change one of the settings, enter a **Y** and press **<enter>**. You will be prompted for a new RAM drive size. Select a size in kilobytes between 1000 and 8000. You can also delete the RAM drive by entering a size of zero (0). Changing the RAM disk size also requires that you reboot the system.

The **Lines displayed** controls the amount of data displayed to the terminal when you choose to dump session data to the computer screen. You can specify the number of lines to display while viewing port monitor data on the screen.

Changing the Default System Directory (cd)

After a port monitoring session is enabled the default directory is the RAM disk system (**/ram**). To switch back to the standard default flash file system (**/flash**) use the **cd** command. To switch back to the default directory, enter

```
cd /flash
```

To switch back to the RAM disk directory, enter

```
cd /ram
```

Starting a Port Monitoring Session (pmon)

You enable a port monitoring session through the **pmon** command. To start a session, enter **pmon** followed by the slot and port number that you want to monitor. For example, to monitor a port that is the first port in the fourth slot of the switch, you would enter

```
pmon 4/1
```

You can only monitor Ethernet 10BaseT and Token Ring ports. If a port is already being mirrored (enabled through the **advp** or **modvp** command) you cannot monitor it. Also, you cannot set up more than one monitoring session on the same port.

If the port is currently being monitored, or mirrored, the following message displays:

```
Port 4/1 is being monitored.  
Disable monitoring? (y)
```

If the port is not being monitored, or mirrored, the following message displays:

```
Port 4/1 is not being monitored, or mirrored.  
Enable monitoring? (y)
```

Enter a **Y** and press **<enter>** at this prompt. The following screen of options displays:

```
Slot/Port : 5/1  
RAM disk size : 1000 Kilobytes  
Capture to filename : y  
Capture filename : PMONITOR.ENC  
Dump to screen : y  
Broadcast frames : y  
Multicast frames : y  
Unicast frames : y  
Change any of the above (y/n)? (n) :
```

If you want to change any of the values, enter a **Y** and press **<enter>**. You will be prompted for all of the values in the screen except the **RAM disk size**, which you must change through the **pmcfg** command before starting the session. The information selected in this screen will be saved in flash configuration memory.

Enter any new values as prompted. The above screen re-displays to show the new values. Press **<enter>** to accept the updated values. Messages similar to the following display:

```
1048576 byte RAM drive /ram already initialized.  
Bytes remaining on RAM disk = 1040384
```

The port monitoring session has begun. What happens at this point depends on whether you chose the **Dump to screen** option. The sections below describe what happens in each case.

◆ Note ◆

If you change the capture filename from the default, you must specify **/ram**. Otherwise, the file will be saved in the flash directory.

If You Chose *Dump to Screen*

If you selected the **Dump to screen** option, then a real-time synopsis of the session displays on your terminal screen. The following shows an example of this data

```
Enter 'p' to pause, 'q' to quit.
Destination      | Source          | Type | Data
-----|-----|-----|-----
00:20:DA:04:01:02 | 00:20:DA:04:01:01 | ICMP | 01:02:03:04:05:06:07:08
00:20:DA:04:01:02 | 00:20:DA:04:01:01 | ICMP | 01:02:03:04:05:06:07:08
FF:FF:FF:FF:FF:FF | 00:20:DA:02:10:E3 | ARP-C | 08:06:00:01:08:00:06:04
FF:FF:FF:FF:FF:FF | 00:20:DA:6F:97:A3 | RIP  | 08:00:45:00:00:34:22:30
```

Each line in the display represents a packet. The destination MAC address, source MAC address, protocol type and actual packet data are shown. The amount of data shown is configured through the **pmcfg** command. The above sample shows 16 bytes of data per packet. You can stop the data dump to the screen at anytime by pressing **q** to quit. You can also pause the data dump by pressing **p** to pause.

If You Did Not Choose *Dump to Screen*

If you did not select the **Dump to screen** option, then the system prompt will return and port monitoring occurs in the background. You can continue using other UI commands. The port monitoring session data is saved in the file you indicated through the **pmmon** screen. You can monitor the session at anytime by using the **pmstats** command. You can also end or pause an in-progress session using the **pmdelete** or **pmpause** commands, respectively. The following sections describes **pmdelete** and **pmpause**.

Ending a Port Monitoring Session (**pmdelete**)

The **pmdelete** command ends a port monitoring data capture session that is being saved to file but not being dumped to the console screen. To end the session, enter:

```
pmd
```

A message similar to the following displays:

```
Port monitoring session terminated, data file is xxxxx.ENC.
```

If a port monitoring session was not in progress then the following message displays:

```
No ports being monitored.
```

Pausing a Port Monitoring Session (**pmpause**)

The **pmpause** command pauses a port monitoring data capture session that is being saved to file but not being dumped to the console screen. To pause the session, enter:

```
pmmp
```

The following message displays

```
Pausing monitor data capture/display.
```

To resume the port monitoring session, enter **pmmp** again. The following message displays:

```
Resuming monitor data capture.
```

If a port monitoring session was not in progress, then the following message would display:

```
No ports being monitored.
```

Ending a Port Monitoring Session

After you quit a port monitoring session, the default directory changes to **/ram** and the current files on the RAM drive are listed. The screen below shows an example of the display at the completion of a monitoring session.

```
Port monitoring capture done. Current capture files listed:
Current working directory '/ram'.
```

```
PM0302.ENC    65536  10/20/96 12:12
PM0303.ENC    32768  10/20/96 11:15
```

```
950272 bytes free
```

Viewing Port Monitoring Statistics (pmstat)

The **pmstat** command displays the statistics gathered for the current or most recent port monitoring session. If a port monitoring session is currently in progress, then it displays the results of the in-progress session. If a port monitoring session is not in progress, then it displays results of the most recently completed session. To view session statistics, enter

```
pmstat
```

A screen similar to the following displays:

```
Viewing capture statistics:
Percent RAM available: 96%
Frame type           #Frames
-----
Broadcast            108
Multicast             253
Unicast               301
```

The **Percent RAM available** indicates how much of the configured RAM disk has been used by this port monitoring session. You can configure the size of the RAM disk through the **pmcfg** command; the default size is 1 MB. The remaining items in the display show the number of packets passed on the port broken down into broadcast, multicast, and unicast frames.

Port Mapping

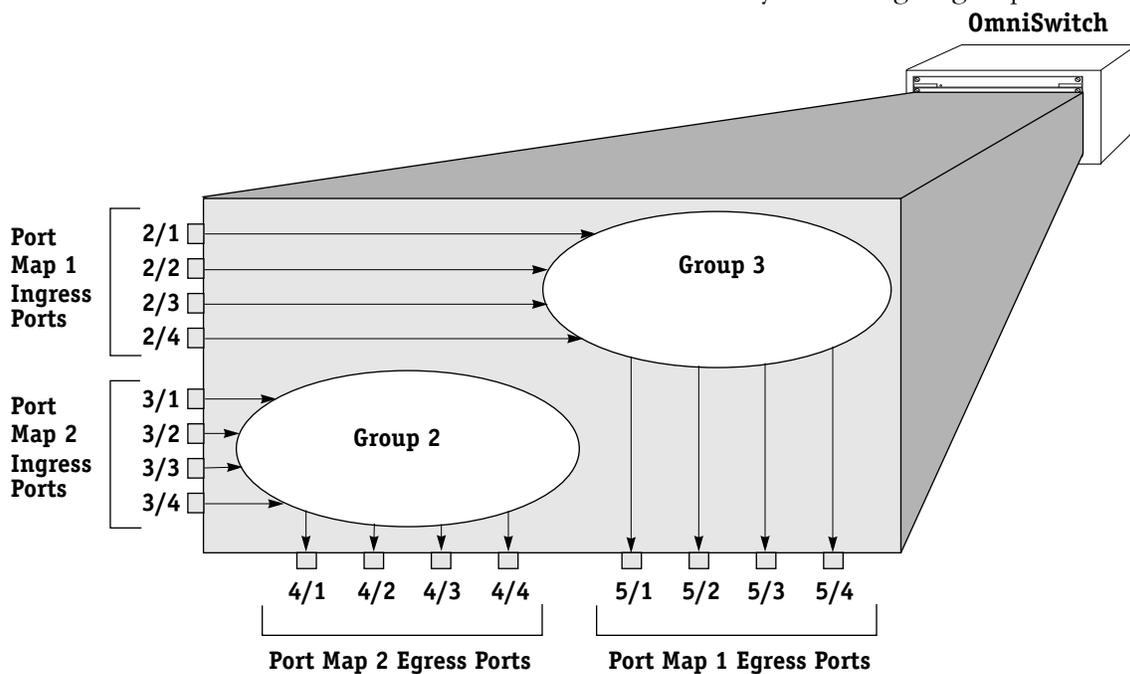
The OmniSwitch began as an any-to-any switching device, connecting different LAN interfaces, such as Ethernet, Token Ring, and FDDI. As networks grew and the traffic on them increased, a need arose for controlling some traffic, such as broadcasts. Virtual LANs, or VLANs, were introduced to segment traffic such that devices could only engage in switched communication with other devices in the same VLAN.

Some applications today require a further degree of traffic segmentation than that provided by VLANs. The port mapping feature allows you to further segment traffic *within* a VLAN or group by isolating a set of ports.

Groups/VLANs and Port Mapping

Port mapping does *not* affect existing group or AutoTracker VLAN operations in a switch. Group and VLAN membership are checked and applied before port mapping constraints are applied. Therefore, any constraints applied by port mapping only limit traffic flow *within* a group or VLAN; port mapping parameters do not provide any additional connectivity to a port. So if you add a port to a port mapping set, that port will be first subject to the constraints of its Group/VLAN and then the restrictions imposed by port mapping. Up to 128 port mapping sets can be configured per switch.

The illustration below helps show how group and port mapping constraints interact. The ports in slot 2 and 5 (2/1—2/4 and 5/1—5/4) are part of group 3. By group membership, all of these ports have switched communication with each other. Likewise, the ports in slot 3 and slot 4 have switched communication with each other as they all belong to group 2.



Groups and Port Mapping

Once a port mapping set is constructed, communication within each of the groups becomes more restricted. A port mapping set consists of *ingress* and *egress* ports; ingress ports can only send traffic to egress ports. In the above figure, all ports on slots 2 and 3 are ingress ports and ports on slots 4 and 5 are egress ports.

Port communication is uni-directional. A mapping between an ingress port and an egress port can only pass data from the ingress port to the egress port. To allow traffic to flow from the egress port to the ingress port, it is necessary to create a new mapping.

This configuration restricts each port to communication *only with the other four ports in the opposite port mapping subset within the same group*. For example, port 2/1 can only send traffic to ports 5/1, 5/2, 5/3, and 5/4. It can no longer communicate with ports 2/2, 2/3, and 2/4 even though they are part of the same group. Port mapping restricts ports from communicating with other ports within the same subset.

Port mapping does not affect other ports in the group that are not part of the port mapping set.

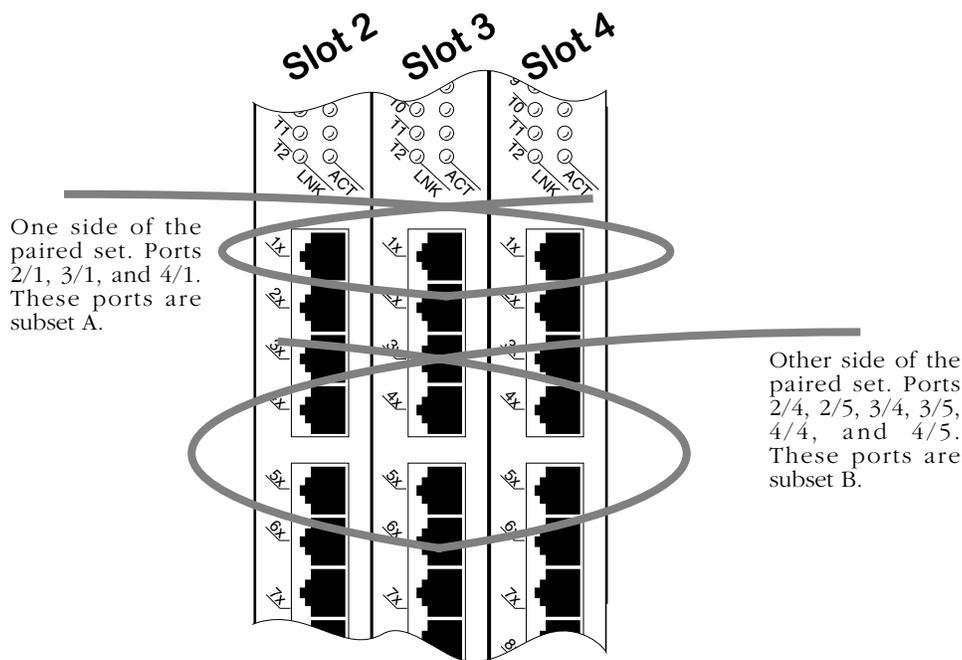
The Details of Port Mapping

Port mapping can be thought of as special rule that is applied after standard group and VLAN rules are applied. This rule statically assigns a port as either an ingress or egress port. Ingress ports can only communicate with egress ports. In this sense, one subset of ports is “mapped” to another subset of ports. Ports within the same subset can not communicate with each other or with another switch port that is not a member of the opposite port mapping subset.

◆ Note ◆

Port mapping restrictions are only applied to ports on 10/100 Ethernet modules (e.g., ESM-100F-8, ESM-C-32, ESM-FM-16W, ESM-100C-12).

As an illustration, see the diagram of three Ethernet modules below. The modules are in slots 2, 3, and 4. The ports that are circled are included in a port mapping subset. The three ports at the top—2/1, 3/1, and 4/1—are ingress ports. The six ports below—2/4, 2/5, 3/4, 3/5, 4/4, and 4/5—are egress ports in the port mapping set.



Port Subsets in the Port Mapping Set

Who Can Talk to Whom?

The following matrix outlines which ports can communicate with each other in the example shown on the previous page *assuming all ports are part of the same group or VLAN*. A port can only communicate with ports in the opposite subset within the port mapping set.

Switch Ports That May Communicate*

	2/1	2/4	2/5	3/1	3/4	3/5	4/1	4/4	4/5
2/1	N/A	Yes	Yes	No	Yes	Yes	No	Yes	Yes
2/4	No	N/A	No						
2/5	No	No	N/A	No	No	No	Yes	No	No
3/1	No	Yes	Yes	N/A	Yes	Yes	No	Yes	Yes
3/4	No	No	No	No	N/A	No	No	No	No
3/5	No	No	No	No	No	N/A	No	No	No
4/1	No	Yes	Yes	No	Yes	Yes	N/A	Yes	Yes
4/4	Yes	No	No	Yes	No	No	Yes	N/A	No
4/5	Yes	No	No	Yes	No	No	Yes	No	N/A

***Read table from right (ingress ports) to left only.**

Port communication is uni-directional. A mapping between an ingress port and an egress port can only pass data from the ingress port to the egress port. To allow traffic to flow from the egress port to the ingress port, it is necessary to create a new mapping.

It's important to remember that the port mapping configuration is affected by existing group/VLAN rules. If the ports in the above example belonged to three groups based on IP network rules, then they would be restricted by group membership and port mapping.

Port mappings can be created between switch ports and uplink ports, but not between uplink ports. For example, you could map ethernet ports 3/1-12 to an ATM uplink port 4/1. This is useful when there is no traffic between ethernet ports, but all ports are to be forced to the uplink module. You *cannot*, however, map uplink port 4/1 to uplink port 4/2.

Port Mapping Limitations

The following are restrictions to the use of the port mapping feature:

- Port mapping cannot be used with ports assigned to an 802.1Q group.
- Port mapping cannot be used with an OmniChannel unless all ports in the OmniChannel are included in the port mapping (on either the ingress or egress list). For example, if ports 3/1-3/4 are an OmniChannel, all four ports must be in the ingress or egress list. You could not just map port 3/1.

Creating a Port Mapping Set

Use the **pmapcr** command to create a port mapping set. Follow these steps:

1. Enter **pmapcr** at a system prompt.
2. The following screen displays:

Port Map Configuration

```
1. Ingress List  :
2. Egress List   :
```

Enter the ingress ports and egress ports for this map set. This is done by entering the line number, an equal sign, and the port (or ports) to be added. For example, if you want to create a map set with an ingress port of 3/6 and an egress port of 4/6, you would enter the following at the prompt:

```
1=3/6
2=4/6
```

This must be done in two separate operations, one for the ingress and one for the egress lists. You can add more than one port to a list by using a comma (,) between slot/port designations, or a dash (-) between port numbers. For example, if you wanted to make ports 4/1, 4/6, 4/7, 4/8, and 4/9 egress ports for this map set, you would enter the following:

```
2=4/1, 4/6-9
```

A switch port in the ingress list can only communicate with switch ports in the egress list. Switch ports in the same list cannot communicate with each other or any other ports in the switch. For example, if you enter:

```
1=2/1, 3/1
2=2/2, 3/2
```

then you are creating a paired set of four ports. Port 2/1 can only communicate with ports 2/2 or 3/2. It cannot communicate with any other ports in the switch, including port 3/1. Port 3/1 also can only communicate with ports 2/2 and 3/2, but no others.

Any port type may be added to a port mapping set. However, only Mammoth-generation Ethernet ports will be restricted by port mapping limitations. For example, you could add a non-Ethernet port to the set, but traffic from that port would not be restricted.

3. You will want to save your configuration, so enter an **s** at the **port-mapping** prompt. Your configuration will be saved. A prompt similar to the following appears to confirm the creation of the port map:

```
Port Map 7 created.
```

The port map number is used when modifying the map set.

It is important to remember that port communication is uni-directional. A mapping between an ingress port and an egress port can only pass data from the ingress port to the egress port. To allow traffic to flow from the egress port to the ingress port, it is necessary to create a new mapping.

Adding Ports to a Port Mapping Set

You can add ports to a port map set once it has been created using the **pmapmod** command. Follow these steps:

1. Enter the **pmapmod** command at a system prompt, as shown:

```
pmapmod <pmap id>
```

where **<pmap id>** is the map set number shown when the map set was created. (To view a list of all existing map sets, see *Viewing a Port Mapping Set* on page 24-80.) For example, to modify map set 5, you would enter the following:

```
pmapmod 5
```

2. The following screen displays:

```

Port Mapping Configuration
=====
Port Map Id      Ingress Ports      Egress Ports
-----
5                3/1, 3/2, 3/3     4/1, 4/2, 4/3

Modify Port Map 5

1. Add Ports to Ingress List      :
2. Add Ports to Egress List      :
3. Delete Ports from Ingress List :
4. Delete Ports from Egress List  :
5. View Port Map Configuration   :
```

Note that the current ports in the port mapping set are displayed. Use this information to make decisions on the ports you want to add or remove from the set.

Enter the line number for the operation you want to perform (a **1** for the ingress list or a **2** for the egress list), an equal sign (=), and the ports to be added. For example, add port 3/2 to the ingress list and the egress list, enter the following (in two separate operations):

```
1=3/2
```

```
2=3/2
```

You can add more than one port to a list by using a comma (,) between slot/port designations, or a dash (-) between port numbers. For example, if you wanted to make ports 4/1, 4/6, 4/7, 4/8, and 4/9 egress ports for this map set, you would enter the following:

```
2=4/1, 4/6-9
```

3. To view the changes, enter a **5 (View Port Map Configuration)**, and equal sign (=), and a **y**, as shown:

```
5=y
```

This will refresh the Port Mapping Configuration screen and display any changes you have made.

4. Quit the session by entering a **q** at the prompt.

Removing Ports from a Port Mapping Set

You can remove ports to a port map set once it has been created using the **pmapmod** command. Follow these steps:

1. Enter the **modpmap** command at a system prompt, as shown:

```
pmapmod <pmap id>
```

where **<pmap id>** is the map set number shown when the map set was created. (To view a list of all existing map sets, see *Viewing a Port Mapping Set* on page 24-80.) For example, to modify map set 5, you would enter the following:

```
pmapmod 5
```

2. The Port Mapping Configuration screen displays (as shown above in *Adding Ports to a Port Mapping Set* on page 24-78).

Enter the line number for the operation you want to perform (a **3** for the ingress list or a **4** for the egress list), an equal sign (=), and the ports to be added. For example, remove port 3/2 to the ingress list and the egress list, enter the following (in two separate operations):

```
3=3/2  
4=3/2
```

You can remove more than one port to a list by using a comma (,) between slot/port designations, or a dash (-) between port numbers. For example, if you wanted to remove ports 4/1, 4/6, 4/7, 4/8, and 4/9 from the egress list of this map set, you would enter the following:

```
4=4/1, 4/6-9
```

3. To view the changes, enter a **5** (view port map configuration), an equal sign (=), and a **y**, as shown:

```
5=y
```

This will refresh the Port Mapping Configuration screen and display any changes you have made.

4. Quit the session by entering a **q** at the prompt.

Viewing a Port Mapping Set

You can view a port mapping set using the **vpmap** command. Enter the **pmapv** command as shown:

```
pmapv <pmap id>
```

where **<pmap id>** is the map set number shown when the map set was created. For example, to modify map set 5, you would enter the following:

```
pmapv 5
```

The following screen is shown:

```
Port Mapping Configuration
=====
Port Map Id      Ingress Ports      Egress Ports
-----
5                3/1, 3/2, 3/3     4/1, 4/2, 4/3
```

As a variation of this command, enter the **vpmap** command with no port map identification. This will display all port mapping sets configured for this switch.

Port Map Id. An identification number for the port map set, generated when the set is created.

Ingress Ports. The switch ports designated as ingress ports for this port map set. Ingress ports can only communicate with egress ports.

Egress Ports. The switch ports designated as egress ports for this port map set. Egress ports can only communicate with ingress ports.

Deleting a Port Mapping Set

You can delete a port mapping set after it is created. Enter **pmapdel** at a prompt as shown:

```
pmapdel <pmap id>
```

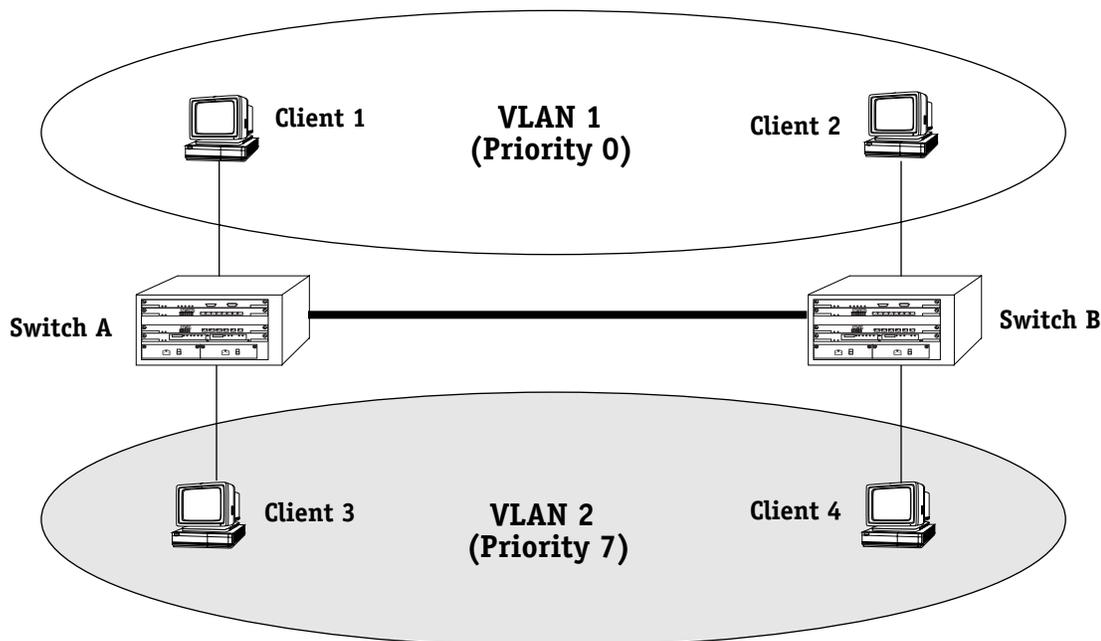
where **<pmap id>** is the map set number shown when the map set was created. (To view a list of all existing map sets, see *Viewing a Port Mapping Set* on page 24-80.) For example, to modify map set 5, you would enter the following:

```
pmapdel 5
```

Priority VLANs

Prioritizing VLANs allows you to set a value for traffic based on the destination VLAN of packets. Traffic with the higher priority destination will be delivered first. VLAN priority can be set from 0 to 7, with 7 being the level with the most priority.

The following diagram illustrates this idea:



In the above diagram, traffic from Client 3 in VLAN 2 (with a priority of 7) to Client 2 takes precedence over traffic from Client 1 in VLAN 1 (with a priority of 0) to Client 4.

Group priority can be set when creating a group using the `crgrp` command. For more information on the `crgrp` command, see *Creating a New Group* on page 24-21.

Group priority can be modified or viewed using the `prty_mod` and `prty_disp` commands, detailed below.

Mammoth vs. Kodiak Priority VLANs

Although the range of VLAN priority is 0-7, the Mammoth based modules only supports two levels of priority. In other words, 0-3 is one level and 4-7 is another. Future releases will expand the number of priority levels.

Kodiak based modules support up to 4 levels of priority (0-1, 2-3, 4-5, 6-7). **These two different implementations of the VLAN priority are not compatible.** Kodiak based priority VLANs can be used with other Kodiak based priority VLANs. This is true for Mammoth based VLANs as well.

Configuring VLAN Priority

To configure the priority of a VLAN:

1. Enter the **prty_mod** command at the system prompt, as shown:

```
prty_mod <groupId>
```

where **<groupId>** is the group number associated with the VLAN whose priority is being set. For example, to modify the priority of the VLAN for Group 2, you would enter the following:

```
prty_mod 2
```

The following prompt is shown:

```
Enter a priority value which is between 0 and 7: 0
```

2. Enter the number value that is to be the new priority level for this VLAN. The highest (most important) value is 7.
3. Press **<enter>**. A message similar to the following is displayed:

```
Priority for VLAN 2 has been set as 7
```

Viewing VLAN Priority

The priority level for all configured VLANs can be viewed by using the **prty_disp** command. Enter the **prty_disp** at the system prompt, as shown:

```
prty_disp <groupId>
```

where **<groupId>** is the group number associated with the VLAN whose priority is being viewed. For example, to view the priority of the VLAN for Group 2, you would enter the following:

```
prty_disp 2
```

A display similar to the following is shown:

```
The priority of group 2 is 7
```

As a variation of this command, you can enter **prty_disp** at the system prompt without a group number. This will display the priority of all VLANs.

25 Configuring Group and VLAN Policies

AutoTracker policies subdivide network traffic based on specific criteria. AutoTracker policies can be defined by port, MAC address, protocol, network address, user-defined, port binding, DHCP port, or DHCP MAC address policy. You can define multiple policies—also referred to as “rules”—for a mobile Group or an AutoTracker VLAN. A port or device is included in a mobile Group or AutoTracker VLAN if it matches any one AutoTracker rule. For example, you can define rules based on MAC address and rules based on protocol in the same mobile group or AutoTracker VLAN.

This chapter provides an overview of AutoTracker Policies as well as instructions for configuring these policies. AutoTracker policies may be applied to mobile groups (including authenticated groups) and to VLANs within standard groups. All policy types may be used with mobile groups and VLANs within standard Groups. However, only the Binding Rule may be used with authenticated groups.

◆ Note ◆

This chapter contains instructions for configuring AutoTracker policies for mobile groups or AutoTracker VLANs. Instructions for configuring groups (mobile and non-mobile) can be found in Chapter 24. More detailed overview and instructions for AutoTracker VLANs (created within non-mobile groups) can be found in Chapter 27.

AutoTracker policies enable you to control communications between end stations in your network. You define policies that determine membership in the mobile group or AutoTracker VLAN and AutoTracker automatically locates ports or devices that fit the policies and places them into the mobile group or AutoTracker VLAN.

You can define physical policies or logical policies (or combinations thereof) to determine membership. Physical policies consist of port rules: you define the members as one or more specific ports and membership is limited to the ports defined and the MAC addresses of devices connected to those ports.

Logical VLAN policies can consist of MAC address rules, protocol rules, network address rules, user-defined, or port binding rules. Ports are assigned to mobile groups or AutoTracker VLANs that have logical rules when the MPM module examines frames that originate from devices connected to the switch. If a frame is received that matches a logical rule, the source device's MAC address and the port to which the source device is connected are both made members.

The members of a mobile group or AutoTracker VLAN thus consist of source devices originating frames that fit the AutoTracker policies and the ports to which those source devices are connected.

AutoTracker Policy Types

You can define a maximum of 32 AutoTracker policies of each type per Group. There is no restriction on the number of rules you can define per AutoTracker VLAN, as long as the maximum number of policies for the Group is not exceeded. A port or device is included in a mobile group or AutoTracker VLAN if it matches any one rule.

You can define the following types of rules:

Port Policies. Port policies enable you to define membership on the basis of ports. Members of the mobile group or AutoTracker VLAN will consist of devices connected to specific ports on one switch or on multiple switches in the Group.

MAC Address Policies. MAC address policies enable you to define membership on the basis of devices' MAC addresses. This is the simplest type of rule and provides the maximum degree of control and security. Members of the mobile group or AutoTracker VLAN will consist of devices with specific MAC addresses. These devices may all be connected to one switch or they may be connected to different switches in the Group. A maximum of 1024 MAC addresses are supported per MAC address policy.

Protocol Policies. Protocol policies enable you to define membership on the basis of the protocol that devices use to communicate. All devices that communicate with the specified protocol become members of the mobile group or AutoTracker VLAN.

You can specify membership according to the following protocols: IP, IPX, AppleTalk, or DECNet. In addition, you can specify membership according to Ethernet type, source and destination SAP (service access protocol) header values, or SNAP (sub-network access protocol) type.

Network Address Policies. Network address policies enable you to define membership on the basis of network address criteria.

For example, you can specify that all IP users with a specific subnet mask be included in the mobile group or AutoTracker VLAN. Or, you can specify that all IPX users in a specific network address area using a certain encapsulation type be included.

If you define network address and port or protocol rules in the same VLAN, the network address rules will take precedence over the port and protocol rules should any conflict arise. To reverse this precedence (i.e., port and protocol rules take precedence over network address rules) you must add the following line to the switch's **mpm.cmd** file:

Precedence=0

User-Defined Policies. User-defined policies enable you to define membership on the basis of a specific pattern within a frame. All devices that originate frames containing this pattern are assigned to the mobile group or AutoTracker VLAN. The pattern is specified by defining an offset, a value, and a mask.

Port Binding Policies. A port binding policy specifies a particular device to be included in the mobile group or AutoTracker VLAN. There are six types of Port Binding Rules that can be created:

- Bind IP Address to a Port and a MAC address
- Bind MAC Address to a Protocol and a Port
- Bind Port to a Protocol
- Bind IP Address to a MAC Address
- Bind IP Address to a Port
- Bind MAC Address to a Port

You must specify a separate binding policy for each device, but you can specify an unlimited number of such policies. Binding policies take precedence over all other AutoTracker policies.

DHCP Port Policies. These policies are similar to standard port policies, but apply to switch ports to which DHCP client workstations are attached.

DHCP MAC Address Policies. These policies are similar to standard MAC address policies, but apply to the MAC addresses of DHCP client workstations only.

Defining and Configuring AutoTracker Policies

You can define AutoTracker policies by port, MAC address, protocol, network address, user definition, or port binding. You can define multiple policies for a mobile group or AutoTracker VLAN if you wish. A port or device is included in a mobile group or AutoTracker VLAN if it matches any one rule. For example, you can define rules based on ports, rules based on MAC address, and rules based on protocol in the same mobile group or AutoTracker VLAN. However, defining multiple rules is not trivial – exercise extreme care when you do so and make sure that you understand the consequences of your definitions. In most situations, it is advisable to use one of AutoTracker's predefined rules.

The sections below provide directions for setting up each type of AutoTracker policy. Follow the directions for the policy you wish to set up.

Port Policy	See <i>Defining a Port Policy</i> on page 25-5.
MAC Address Policy	See <i>Defining a MAC Address Policy</i> on page 25-6.
Protocol Policy	See <i>Defining a Protocol Policy</i> on page 25-8.
Network Address Policy	See <i>Defining a Network Address Policy</i> on page 25-11.
User-defined Policy	See <i>Defining Your Own Rules</i> on page 25-13.
Binding Policy	See <i>Defining a Port Binding Policy</i> on page 25-15.
DHCP Port Policy	See <i>Defining a DHCP Port Policy</i> on page 25-20.
DHCP MAC Address Policy	See <i>Defining a DHCP MAC Address Policy</i> on page 25-21.

Where These Procedures Start

These policy configuration sections start in the middle of a sequence of steps with the **crgp** or **modatvl** commands. During the **crgp** command prompt sequence you can configure policies for mobile groups or for VLANs within non-mobile groups. The **modatvl** command contains an option for adding policies (option #3). The procedures in these sections pick up at the point after you choose to either to configure AutoTracker rules (**crgp**) or add more rules (**modatvl**).

Defining a Port Policy

After you enter the Administrative Status, the following menu displays:

- Select rule type:
1. Port Rule
 2. MAC Address Rule
 - 21) MAC Address Range Rule
 3. Protocol Rule
 4. Network Address Rule
 5. User Defined Rule
 6. Binding Rule
 7. DHCP PORT Rule
 8. DHCP MAC Rule
 - 81) DHCP MAC Range Rule

Enter rule type (1):

1. Press **<Return>**. If this is a VLAN in a non-mobile Group refer to Chapter 24 for a detailed explanation of the two ways port policies may be configured.

◆ **Note** ◆

As of the current release, the MAC Address Range Rule and DHCP MAC Range are not supported.

2. The following prompt displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the VLAN as it controls only to this specific rule within this specific VLAN. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

Enter the list of ports in Slot/Int/Service/Instance format:

Enter the physical ports that you want included in this VLAN. You may enter multiple ports at a time. Use the **<slot>/<port>** format. For example, to include port 7 from the module in slot 2, you would enter **2/7**. (The service and instance numbers are not necessary for specifying physical LAN ports. They are only necessary when specifying logical ports used over ATM, FDDI, and Frame Relay.)

4. The following prompt displays:

Configure more rules for this vlan (y/n):

You can set up multiple rules for the same VLAN. Enter a **Y** here if you want to set up more rules in addition to the port rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up on this VLAN. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

VLAN 1:2 created successfully

You are done setting up rules.

Defining a MAC Address Policy

After you enter the Administrative Status, the following menu displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
   21) MAC Address Range Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule
   81) DHCP MAC Range Rule
```

Enter rule type (1):

1. Enter **2** and press **<Enter>**.
2. The following prompt displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for this mobile group or AutoTracker VLAN as it controls only to this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

Enter the list of MAC addresses (Enter save to end):

Enter the MAC addresses that you want to include in this VLAN. Separate addresses by a space. When you have entered the final MAC address, leave a space and type **save**.

4. The following prompt displays:

Configure more rules for this vlan (y/n):

You can set up multiple rules. Enter a **Y** here if you want to set up more rules in addition to the MAC Address rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the mobile group or AutoTracker VLAN was set up.

VLAN 1:2 created successfully

You are done setting up rules.

Defining a MAC Address Range Policy

After you enter the Administrative Status, the following menu displays:

```

Select rule type:
1. Port Rule
2. MAC Address Rule
   21) MAC Address Range Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule
   81) DHCP MAC Range Rule
  
```

Enter rule type (1):

1. Enter **21** and press **<Enter>**.
2. The following prompt displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for this mobile group or AutoTracker VLAN as it controls only to this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

Enter the lower end MAC addresses (AABBCC:DDEEFF) in canonical form followed by the higher end:

Enter the low end MAC address followed by the high end MAC address. Separate addresses by a space. The range is specified using the last two bytes of the MAC address.

When you have entered the high end MAC address press **<enter>**.

4. The following prompt displays:

Configure more rules for this vlan (y/n):

You can set up multiple rules. Enter a **Y** here if you want to set up more rules in addition to the MAC Address rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the mobile group or AutoTracker VLAN was set up.

VLAN 1:2 created successfully

You are done setting up rules.

◆ Note ◆

MAC range rules only apply to mobile groups. They cannot be configured for AutoTracker VLANs.

Defining a Protocol Policy

After you enter the Administrative Status for this mobile group or AutoTracker VLAN, the following menu displays:

- Select rule type:**
1. Port Rule
 2. MAC Address Rule
 - 21) MAC Address Range Rule
 3. Protocol Rule
 4. Network Address Rule
 5. User Defined Rule
 6. Binding Rule
 7. DHCP PORT Rule
 8. DHCP MAC Rule
 - 81) DHCP MAC Range Rule

Enter rule type (1):

1. Press **3** and press **<Enter>**.
2. The following prompt displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Indicate whether or not you want to enable this rule. Type **e** to enable or **d** to disable. If you enable the rule, the mobile group or AutoTracker VLAN will use it to determine membership of devices. If you disable the rule, then this rule will not be used in assigning devices, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the mobile group or AutoTracker VLAN as it controls only to this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

- Select Protocol:**
1. IP
 2. IPX
 3. DECNET
 4. APPLETALK
 5. Protocol specified by ether-type
 6. Protocol specified by DSAP and SSAP
 7. Protocol specified by SNAP

Enter protocol type (1):

Enter the number for the protocol that will be used to define this mobile group or AutoTracker VLAN. Numbers are listed next to the protocol names. By selecting a specific protocol, you are indicating that all traffic originating from network devices using that protocol will be assigned to this mobile group or AutoTracker VLAN. You can select the IP, IPX, DECNET, and APPLETALK protocols by entering 1, 2, 3, or 4, respectively.

◆ Please Take Note ◆

ARP (address resolution protocol) is included as IP. DDP (datagram delivery protocol) and AARP (AppleTalk ARP) are included as AppleTalk. DECNET is DECNET Phase IV traffic only.

If you want to define a protocol other than IP, IPX, AppleTalk, or DECNet, you can do so by specifying an Ethernet type, or by specifying source and destination SAP (service access protocol) header values, or by specifying a SNAP (sub-network access protocol) type. The following three sections describe how to specify these protocol types. If you are not specifying one of these special protocol types, continue with Step 4 below.

Protocol Specified by Ether-Type

- a. To specify a protocol by Ethernet type, enter **5** at the **Select Protocol:** menu. The following prompt displays:

Enter the Ether-type value in hex:

- b. Enter the desired Ethernet type in hex. You must enter two bytes of data. For example, enter 0800 to specify IP or enter 0806 to specify ARP. All devices that use the specified Ethernet type will be members of the mobile group or AutoTracker VLAN.
- c. Go on to Step 4 below.

Protocol Specified by DSAP and SSAP

- a. To specify a protocol by SAP (service access protocol) header, enter **6** at the **Select Protocol:** menu. The following prompt displays:

Enter the DSAP value in hex:

- b. Enter the destination service access protocol (DSAP) value in hex and press **<Enter>**. The following prompt displays:

Enter the SSAP value in hex:

- c. Enter the source service access protocol (SSAP) value in hex. Each entry must consist of one byte of data. All devices that use the specified source and destination SAP types will be members of the mobile group or AutoTracker VLAN.
- d. Go on to Step 4 below.

Protocol Specified by SNAP

- a. To specify a protocol by SNAP (sub-network access protocol) type, enter **7** at the **Select Protocol:** menu. The following prompt displays:

Enter the SNAP value in hex

- b. Enter the desired SNAP value in hex. You must enter five bytes of data. For example, enter 0000008137 to specify IPX SNAP or enter 00000080F3 to specify AppleTalk ARP SNAP. All devices that use the specified SNAP type will be members of the mobile group or AutoTracker VLAN.
- c. Go on to Step 4 below.

4. The following prompt displays:

Configure more rules for this vlan (y/n):

You can set up multiple rules for the same mobile group or AutoTracker VLAN. Enter a **Y** here if you want to set up more rules in addition to the protocol rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

VLAN 1:2 created successfully

You are done setting up rules for this mobile group or AutoTracker VLAN.

Defining a Network Address Policy

After you enter the Administrative Status for this mobile group or AutoTracker VLAN, the following menu displays:

```

Select rule type:
1. Port Rule
2. MAC Address Rule
   21) MAC Address Range Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule
   81) DHCP MAC Range Rule
  
```

Enter rule type (1):

1. Press **4** and press **<Enter>**.
2. The following prompt displays:

```
Set Rule Admin Status to ((e)nable/(d)isable):
```

Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the mobile group or AutoTrackerVLAN as it controls only to this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

```

Select the Network Protocol:
1. IP
2. IPX
  
```

```
Enter the protocol type:
```

Enter the protocol for which you want to define this network address rule. Enter a **1** for IP and a **2** for IPX. The prompts that follow are different for IP and IPX. These differences are due to the different conventions used by the protocols for network address formats. Follow the procedure below the network protocol you are setting up.

Set Up an IP Address

- a. To specify an IP address, enter a **1** at the **Select the Network Protocol:** prompt.
- b. The following prompt displays:

```
Enter the IP address:
```

Enter the IP address that you want to include in this mobile group or AutoTracker VLAN. Enter the address in dotted decimal notation or hexadecimal notation (e.g., 198.206.181.10).

- c. The following prompt displays:

```
Enter the IP Mask (0xfffff00):
```

Enter the IP Subnet mask for this address. The default subnet mask is shown in parentheses and is automatically derived from the IP address class entered in Step b.

- d. Go on to Step 4 below.

Set Up an IPX Address

- a. To specify an IPX address, enter a **2** at the **Select the Network Protocol:** prompt.
- b. The following prompt displays:

Enter the IPX Network Number:

Enter an IPX network number to define the network devices you want included in the mobile group or AutoTracker VLAN. IPX addresses consist of eight hex digits and you can enter a minimum of one hex digit in this field. If you enter less than eight hex digits, the system prefixes your entry with zeros to create eight digits. All devices with the specified network number will be included in the mobile group or AutoTracker VLAN.

- c. The following prompt displays:

Select the IPX Network Encapsulation

1. Ethernet-II
2. IEEE 802.2 LLC
3. IEEE SNAP
4. IPX Proprietary

Enter the IPX Network Encapsulation (1):

Select the encapsulation type from the list. IPX devices do not know their network number at bootup. Typically, IPX servers assign different network numbers to devices using different encapsulation types within the same physical network. When an encapsulation type is specified here, an IPX device that does not know its network number at bootup will be assigned to the mobile group or AutoTracker VLAN as long as the device uses the encapsulation type you specify here.

- d. Go on to Step 4 below.

4. The following prompt displays:

Configure more rules for this vlan (y/n):

You can set up multiple rules for the same mobile group or AutoTracker VLAN. Enter a **Y** here if you want to set up more rules in addition to the Network Address rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up on this mobile group or AutoTracker VLAN. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

VLAN 1:2 created successfully

You are done setting up rules for this mobile group or AutoTracker VLAN.

Defining Your Own Rules

A user-defined rule enables you to include all devices in the mobile group or AutoTracker VLAN that originate frames containing a specified pattern at a specified location. Each user-defined rule requires an Offset, a Value, and a Mask; you will be prompted for each of these values. The Offset specifies the location of the pattern within the frame. The Value specifies the pattern. The Mask specifies the bits that you care about within the Value pattern.

After you enter the Administrative Status for this mobile group or AutoTracker VLAN, the following menu displays:

```

Select rule type:
1. Port Rule
2. MAC Address Rule
   21) MAC Address Range Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule
   81) DHCP MAC Range Rule
  
```

Enter rule type (1):

1. Enter **5** and press **<Return>**.
2. The following prompt displays:

```
Set Rule Admin Status to ((e)nable/(d)isable):
```

Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the mobile group or AutoTracker VLAN as it controls only to this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

```
Enter the Offset into the frame ( < 64 ) :
```

Enter an **Offset** value, in number of bytes, to define the location where the **Value** – or pattern – is found. The offset value can be any number from 0 – 63. The first byte of the frame's MAC header is considered byte 1. An offset of 0 specifies that the pattern begins in byte 1 of the frame.

As an example, enter an offset value of **14** if you want to specify the pattern that defines NETBIOS, because that pattern begins in the 21st byte of the frame.

4. The following prompt displays:

```
Enter the value of the pattern to match:
```

Enter a **Value**, in hex, to specify the pattern itself. The value can be a maximum of eight bytes. For example, enter **FOFO** to specify the pattern that identifies NETBIOS.

5. The following prompt displays:

```
Enter the mask for the pattern to match:
```

Enter a **Mask** value, in hex, to specify the bits within the **Value** that you care about. The mask can be a maximum of eight bytes, but must be the same length as the **Value** you entered. The mask value is ANDed with the **Value** and frames are searched for the result.

Defining and Configuring AutoTracker Policies

For example, if you enter **FFEF** as the value and **FFFF** as the mask:

	<u>Hex</u>		<u>Binary</u>
Value=	FFEF	=	1111 1111 1110 1111
Mask=	FFFF	=	1111 1111 1111 1111

When a bit in the mask is set to 1, the corresponding bit of the value must be literal. When a bit in the mask is set to 0, the corresponding bit in the value is ignored and can be either a 0 or a 1. In the example above, since the mask is FFFF, all bits in the value must be literal and the actual pattern searched for is the binary value 1111 1111 1110 1111. Only devices that originate frames containing this binary value beginning at the 21st byte will be included in the mobile group or AutoTracker VLAN.

As a second example, if you enter FFEF as the pattern and FFF7 as the mask:

	<u>Hex</u>		<u>Binary</u>
Value=	FFEF	=	1111 1111 1110 1111
Mask=	FFF7	=	1111 1111 1111 0111

In this example, bits 0–2 and bits 4–15 of the value must be literal, since the corresponding bits in the mask are 1s. However, since bit 3 of the mask is a 0, bit 3 of the value can be either a 0 or a 1. Therefore, in this example, two actual binary patterns are searched for:

1111 1111 1110 1111 **or** 1111 1111 1110 0111

Devices originating frames containing either one of these binary values beginning at the 21st byte of the frame will be included in the mobile group or AutoTracker VLAN.

6. The following prompt displays:

Configure more rules for this vlan (y/n):

You can set up multiple rules for the same mobile group or AutoTracker VLAN. Enter a **Y** here if you want to set up more rules in addition to the Network Address rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up on this mobile group or AutoTracker VLAN. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

VLAN 1:2 created successfully

You are done setting up rules for this mobile group or AutoTracker VLAN.

Defining a Port Binding Policy

Port binding policies require devices to match two or three criteria. The criteria can be one of six combinations:

1. The device can attach to a specific switch port *and* use a specific MAC address *and* use a specific protocol (IP or IPX).
2. The device can attach to a specific switch port *and* use a specific MAC address *and* use a specific IP network address
3. The device can attach to a specific switch port and use a specific protocol (IP or IPX)
4. The device can use a specific IP address *and* use a specific MAC address
5. The device can use a specific port *and* a specific IP address
6. The device can use a specific port *and* a specific MAC address.

A device must match all values in the criteria set.

Port binding policies have two additional features. First, if a policy violation is detected, an SNMP trap is generated to alert the network manager which rule was violated. Secondly, if you attempt to configure a port binding rule that creates a conflict with another binding rule, an error message is generated to alert the user of the problem.

For example, if a port binding rule is created with a policy that links IP address 1.1.1.1 and MAC address aabbcc:ddeeff, and you attempt to create a port binding rule for the same IP address with a policy that links it to port 3/1, an error message will appear as shown:

This IP address has already been assigned to a different rule

In this example the second port binding rule is not created because the purpose of the first rule is to provide mobility for the IP address 1.1.1.1 (i.e., it is not restricted to a port), while the second rule specifically limits the mobility of IP address 1.1.1.1 to port 3/1.

A general rule for port binding policies is that once an address has been assigned (MAC or IP), it cannot be assigned to another policy until it is removed from the first policy. The following table is a reference for policy conflicts:

Limitations for Port Policies

	IP Address	MAC Address	Port	Protocol
IP Address	N/A	IP and MAC address cannot be used again	IP address cannot be used again	N/A
MAC Address	IP and MAC address cannot be used again	N/A	MAC address cannot be used again	MAC address cannot be used again
Port	IP address cannot be used again	MAC address cannot be used again	N/A	None
Protocol	N/A	MAC address cannot be used again	None	N/A

Defining and Configuring AutoTracker Policies

After you indicate you want to set up rules for this mobile Group or AutoTracker VLAN (using the **cratvl** command), the following menu displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
   21) MAC Address Range Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule
   81) DHCP MAC Range Rule
```

Enter rule type (1):

1. Enter a 6 and press **<Return>**.
2. The following prompt displays:

```
Set Rule Admin Status to [(e)nable/(d)isable] (d) :
```

Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the mobile group or AutoTracker VLAN as it applies only to this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

```
Please select one of the following bindings:
1. Bind IP Address to a Port and a MAC Address.
2. Bind MAC Address to a Protocol and a Port
3. Bind Port to a Protocol
4. Bind IP Address to a MAC Address
5. Bind IP Address to a Port
6. Bind MAC Address to a Port
Enter the type of binding (1) :
```

Enter the type of binding you want to use for this policy. Each binding policy specifies a particular device to be included in the mobile group or AutoTracker VLAN. Therefore, you must set up a separate binding policy for each device you want included in this mobile Group or AutoTracker VLAN.

You can bind a device's IP address to a switch port and a MAC address (select option 1), bind a device's MAC address to a protocol and a switch port (select option 2), bind a switch port to a specific protocol (select option 3), bind an IP address to a MAC address (select option 4), bind an IP address to a switch port (select option 5), or bind a MAC address to a switch port (select option 6).

◆ Note ◆

It is important to remember the line number of the binding policy you chose in order to follow the correct sequence for the remainder of these steps.

If you select option 1, 2, 3, 5, or 6, go to step 4. If you select option 4, go to step 5.

- The following prompt displays:

Enter the port in the form of slot/interface:

Enter the switch port to which this device must be attached. If the device is not attached to this port, it will not be included in this mobile Group or AutoTracker VLAN. You should first enter the slot for the module, then a slash (/), then the port number.

If you selected binding policy 1 or 5, then continue with step 5. If you selected binding policy 2 or 6, then continue with step 6. If you selected binding policy 3, then continue on with step 7.

- The following prompt displays:

Enter the IP address:

Enter the IP address for the device. If the device does not have this IP address, it will not be included in this mobile Group or AutoTracker VLAN.

If you selected binding policy 1 or 4, continue with step 6. If you selected binding policy 5, continue with step 8.

- The following prompt displays:

Enter the Canonical MAC address in AABBC:DDEEFF format:

Enter the MAC address for the device. If the device does not have this MAC address, it will not be included in this mobile Group or AutoTracker VLAN.

If you selected binding policy 1, 4, or 6, then continue with step 8. If you selected binding policy 2, then continue with step 7.

- The following prompt displays:

Select Protocol:

1. IP
2. IPX
3. DECNET
4. APPLETALK
5. Protocol specified by ether-type
6. Protocol specified by DSAP and SSAP
7. Protocol specified by SNAP

Enter protocol type (1):

Enter the number for the protocol that will be used to define this binding policy. Numbers are listed next to the protocol names. By selecting a specific protocol, you are indicating that a device with the MAC address you specified previously that are attached to the switch port you specified previously, and with traffic using this protocol will be assigned to this mobile group or AutoTracker VLAN. You can select the IP, IPX, DECNET, and APPLE-TALK protocols by entering 1, 2, 3, or 4, respectively.

◆ **Note** ◆

ARP (address resolution protocol) is included as IP. DDP (datagram delivery protocol) and AARP (Apple-Talk ARP) are included as AppleTalk. DECNET is DECNET Phase IV traffic only.

Defining and Configuring AutoTracker Policies

If you want to define a protocol other than IP, IPX, AppleTalk, or DECNet, you can do so by specifying an Ethernet type, or by specifying source and destination SAP (service access protocol) header values, or by specifying a SNAP (sub-network access protocol) type. The following three sections describe how to specify these protocol types. If you are not specifying one of these special protocol types, continue with Step 8 below.

Protocol Specified by Ether-Type

- a. To specify a protocol by Ethernet type, enter **5** at the **Select Protocol:** menu. The following prompt displays:

Enter the Ether-type value in hex:

- b. Enter the desired Ethernet type in hex. You must enter two bytes of data. For example, enter 0800 to specify IP or enter 0806 to specify ARP. All devices that use the specified Ethernet type will be members of the mobile group or AutoTracker VLAN.
- c. Go on to Step 8 below.

Protocol Specified by DSAP and SSAP

- a. To specify a protocol by SAP (service access protocol) header, enter **6** at the **Select Protocol:** menu. The following prompt displays:

Enter the DSAP value in hex:

- b. Enter the destination service access protocol (DSAP) value in hex and press **<Enter>**. The following prompt displays:

Enter the SSAP value in hex:

- c. Enter the source service access protocol (SSAP) value in hex. Each entry must consist of one byte of data. All devices that use the specified source and destination SAP types will be members of the mobile group or AutoTracker VLAN.
- d. Go on to Step 8 below.

Protocol Specified by SNAP

- a. To specify a protocol by SNAP (sub-network access protocol) type, enter **7** at the **Select Protocol:** menu. The following prompt displays:

Enter the SNAP value in hex

- b. Enter the desired SNAP value in hex. You must enter five bytes of data. For example, enter 0000008137 to specify IPX SNAP or enter 00000080F3 to specify AppleTalk ARP SNAP. All devices that use the specified SNAP type will be members of the mobile group or AutoTracker VLAN.
- c. Go on to Step 8 below.

8. The following prompt displays:

Configure more rules for this vlan (y/n):

You can set up more devices for this binding policy group. Enter a **Y** here if you want to set up more devices. If you enter **Y**, you will be prompted for the next rule that you want to set up. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

VLAN 2:1 created successfully

You are done setting up rules for this mobile group or AutoTracker VLAN.

Defining a DHCP Port Policy

DHCP port polices simplify network configurations requiring DHCP clients and servers to be in the same mobile group or AutoTracker VLAN. You can see how DHCP port policies were used in an application example on page 25-27.

DHCP port policies differ fundamentally from standard port policies. In a standard port policy, the port is placed in the mobile group or AutoTracker VLAN as soon as the port rule is configured; no traffic on the port is required. A DHCP port rule *requires* traffic on the port in the form of a DHCP request packet before the port gains membership.

After you indicate you want to set up rules for this mobile Group or AutoTracker VLAN, the following menu displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
   21) MAC Address Range Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule
   81) DHCP MAC Range Rule
```

Enter rule type (1):

1. Enter a 7 and press <Enter>.
2. The following prompt displays:

```
Set Rule Admin Status to [(e)nable/(d)isable] (d) :
```

Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the mobile group or AutoTracker VLAN as it applies only to this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

```
Enter the list of ports in Slot/Int/Service/Instance format:
```

Enter the physical switch ports that you want included in this mobile Group or AutoTracker VLAN. You may enter multiple ports at a time. Use the <slot>/<port> format. For example, to include port 7 from the module in slot 2, you would enter **2/7**. (The service and instance numbers are not necessary for specifying physical LAN ports. They are only necessary when specifying logical ports used over ATM, FDDI, and Frame Relay.)

4. The following prompt displays:

```
Configure more rules for this vlan [y/n] (n) :
```

You can set up multiple rules for the same mobile group or AutoTracker VLAN. Enter a **Y** here if you want to set up more rules in addition to the port rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up. Follow the directions in the appropriate section to configure that rule. If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

```
VLAN 1:2 created successfully
```

You are done setting up rules for this mobile group or AutoTracker VLAN.

Defining a DHCP MAC Address Policy

You can see how DHCP MAC address policies were used in an application example on page 25-27.

After you enter the Administrative Status for this mobile group or AutoTracker VLAN, the following menu displays:

```

Select rule type:
1. Port Rule
2. MAC Address Rule
   21) MAC Address Range Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule
   81) DHCP MAC Range Rule
  
```

Enter rule type (1):

1. Enter **8** and press **<Enter>**.
2. The following prompt displays:

```
Set Rule Admin Status to ((e)nable/(d)isable):
```

Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the mobile group or AutoTracker VLAN as it applies only this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

```
Enter the list of MAC addresses (AABBCC:DDEEFF) in Canonical format
(Enter save to end):
```

Enter the MAC addresses that you want to include in this mobile group or AutoTracker VLAN. Separate addresses by a space. When you have entered the final MAC address, leave a space and type **save**.

4. The following prompt displays:

```
Configure more rules for this vlan (y/n):
```

You can set up multiple rules for the same mobile group or AutoTracker VLAN. Enter a **Y** here if you want to set up more rules in addition to the port rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

```
VLAN 1:2 created successfully
```

You are done setting up rules for this mobile group or AutoTracker VLAN.

Defining a DHCP MAC Address Range Policy

You can see how DHCP MAC address policies were used in an application example on page 25-27.

After you enter the Administrative Status for this mobile group or AutoTracker VLAN, the following menu displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
   21) MAC Address Range Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule
   81) DHCP MAC Range Rule
```

Enter rule type (1):

1. Enter **81** and press **<Enter>**.
2. The following prompt displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the mobile group or AutoTracker VLAN as it applies only this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

Enter the lower end DHCP MAC addresses (AABBCC:DDEEFF) in canonical form followed by the higher end:

Enter the low end DHCP MAC address followed by the high end DHCP MAC address. Separate addresses by a space. The range is specified using the last two bytes of the MAC address.

When you have entered the high end MAC address press **<Enter>**.

4. The following prompt displays:

Configure more rules for this vlan (y/n):

You can set up multiple rules for the same mobile group or AutoTracker VLAN. Enter a **Y** here if you want to set up more rules in addition to the port rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

VLAN 1:2 created successfully

You are done setting up rules for this mobile group or AutoTracker VLAN.

◆ Note ◆

MAC range rules only apply to mobile groups. They cannot be configured for AutoTracker VLANs.

Viewing Mobile Groups and AutoTracker VLANs

You can view the current status of all mobile groups or AutoTracker VLANs in the switch using the **atvl** command. Enter **atvl** and a table similar to the following displays.

VLAN Group :	VLAN Id	VLAN Description	Admin Status	Operational Status
	6	New Mobile Group 6	Enabled	Active
	8	New Mobile Group 8	Enabled	Active

VLAN Group. The Group to which this AutoTracker VLAN is assigned. The Group is specified when first creating an AutoTracker VLAN.

VLAN ID. An identification number that you assigned when you created this VLAN. A value will not display in this column for mobile groups.

VLAN Description. A textual description that you entered to describe a VLAN when you created or modified it through **cratvl** or **modatvl**. This description is limited to 30 characters.

Admin Status. The Administrative Status for the VLAN may be enabled or disabled. You enable or disable the Administrative Status for a VLAN when you create or modify it. If the VLAN is enabled, the switch will use the policies you configured to filter traffic to the devices in this VLAN. If you disable the rule, then policies will not be used, but the parameters you set up for the VLAN will be saved.

Oper Status. The VLAN is shown as **Active** or **Inactive**. In order for an enabled VLAN to become “active” it must be able to assign a switch port to the VLAN. If the port rule is used for a VLAN, then the VLAN automatically becomes active. If any other rule is used (MAC address, protocol, etc.), then a frame matching the VLAN rule must first be received by a switch port before the VLAN is active. So, an Active VLAN requires the following:

- Admin Status must be enabled.
- A port must be assigned to the VLAN through either a port-based rule or by a device transmitting data that matches the VLAN policy.

Viewing Policy Configurations

Typing **viatr1** brings up the Policy Configuration Table, which shows the policies defined for the mobile Group or VLAN specified.

VLAN Group :	VLAN Id	Rule Num	Rule Type	Rule Status	Rule Definition
3:	5	1	PORT RULE	Disabled	2/7/Brg/1
3:	11	1	NET ADDR RULE	Enabled	IPX Addr = 11223344 IPX Encapsulation = Ethernet
3:	12	1	NET ADDR RULE	Enabled	DECNET Area = 13579
3:	22	1	PORT RULE	Enabled	2/7/Brg/1
3:	23	1	PORT RULE	Enabled	2/7/Brg/1
3:	24	1	MAC RULE	Enabled	082008:003002 082009:803728
3:	25	1	PROTOCOL RULE	Enabled	Protocol = IP
3:	26	1	NET ADDR RULE	Enabled	IP Addr = 131.1.2.3 IP Mask = 255.255.0.0
3:	27	1	USER RULE	Enabled	Offset = 64 Length = 2 Value = FFFF Mask = FFFF
3:	31	1	PROTOCOL RULE	Enabled	Protocol = IP
3:	32	1	NET ADDR RULE	Enabled	IPX Addr = 00000001 IPX Encapsulation = Ethernet

VLAN Group. The Group to which this AutoTracker VLAN is assigned. The Group number is specified when first creating the VLAN.

VLAN ID. An identification number that you assigned when you created this virtual LAN. A value will not display in this column for mobile groups.

Rule Num. The number of the policy within the VLAN definition. Each rule defined for a VLAN is numbered sequentially in the order of creation. The rule number is needed when you want to modify or delete a rule definition.

Rule Type. The type of VLAN policy. The Rule Type can be a port policy (PORT RULE), MAC Address policy (MAC RULE), network address policy (NET ADDR RULE), Protocol policy (PROTOCOL RULE), a user-defined policy (USER RULE), port-binding policy (BIND RULE), DHCP Port policy (DHCP PORT RULE), or a DHCP MAC address policy (DHCP MAC RULE). You set up VLAN policies when you create or modify the VLAN.

Rule Status. Indicates whether the rule for this row is Enabled or Disabled. If the rule is enabled, then the VLAN is using the rule definition to determine VLAN membership. If Disabled, then the VLAN is not using this rule to determine membership. Note that this Rule Status is different from the Admin Status for the VLAN since it controls only this specific rule within this specific VLAN. You can enable or disable the rule using the **modatvl** command.

Rule Definition. Details of this rule. For a Port Rule, this column lists the virtual interface for the Port included in the VLAN as

<slot>/<port>/<service>/<instance>

For example, the port defined for the first row in the table applies to the first bridge instance on port 7 on the module in slot 2 of the switch. For a MAC address rule, this column lists the MAC address for the device in the VLAN. For a Network Address Rule, the column will list the address (IP or IPX) and the IP Mask (IP) or the Encapsulation type (IPX). For a Protocol policy, the column list the protocol used to determine membership. And in a User-Defined rule, the offset, length, value, and mask are listed.

Viewing Virtual Ports' Group/VLAN Membership

You can view the VLAN membership of each virtual interface in the switch. For physical LAN ports, the virtual interface is the same as a virtual port. However, when multiple services are set up for a physical port, then each service has a virtual port.

Type **viol** and a Virtual Interface Table displays similar to the one that follows. You can also specify just the slot and port number to narrow the range of ports displayed.

Virtual Interface VLAN Membership

Slot/Intf/Service/Instance	Group	Member of VLAN#
1 /1 /Rtr /1	1	1
1 /1 /Rtr /2	3	1
1 /1 /Rtr /3	3	23
1 /1 /Rtr /4	3	24
1 /1 /Rtr /5	3	25
1 /1 /Rtr /6	3	5
2 /1 /Brg /1	1	1
2 /2 /Brg /1	1	1
2 /3 /Brg /1	1	1
2 /4 /Brg /1	1	1
2 /5 /Brg /1	1	1
2 /6 /Brg /1	1	1
2 /7 /Brg /1	1	1 22
2 /8 /Brg /1	1	1
3 /1 /Brg /1	1	1
4 /1 /Brg /1	1	1
4 /2 /Brg /1	1	1
4 /3 /Brg /1	1	1
4 /4 /Brg /1	1	1
4 /5 /Brg /1	1	1
4 /6 /Brg /1	1	1
5 /1 /Brg /1	1	1

Slot/Intf/Service/Instance. Specifies the virtual interface for which AutoTracker VLAN information will be displayed. The **Slot** is the physical slot location to which the virtual interface maps. The **Intf** is the physical port to which the virtual interface maps. The **Service** is the service type for this interface. The service type may be a Router (**Rtr**), Bridge (**Brg**), Classical IP (**CIP**), FDDI Trunk (**Trk**), or an 802.10 Trunk (**T10**). **Instance** is the specific instance of this service type. These different instances are identified numerically. The first instance of a service type belonging to a physical port is identified as 1, the second instance is identified as 2, etc.

Group. The Group to which this virtual interface is assigned. The Group is specified when first creating an AutoTracker VLAN.

Member of VLAN #. The AutoTracker VLANs to which this virtual interface belongs. An interface may belong to more than one VLAN. For example, a port may contain devices using the IP Protocol and could match the Port policy of one AutoTracker VLAN and the Protocol policy of another AutoTracker VLAN. Also, physical ports always remain members of the default VLAN #1.

View VLAN Membership of MAC Devices

The **fwtl** command displays a table of learned MAC addresses and the VLAN membership of those MAC addresses. Follow these steps to view this table.

1. Enter **fwtl**.
2. The following prompt displays:

Enter Slot/Interface (return for all ports) :

Enter the slot and port for which you want to view MAC Address/VLAN information. You can also press **<Enter>** to view information on all ports in the switch.

3. The following message and prompt displays:

Total number of MAC addresses learned for Group 1: 4
Maximum number of entries to display [20] :

The top line displays the number of MAC addresses learned on this switch. This number indicates the potential number of entries you can display in the Learned MAC Address Table. The second line allows you to indicate how many of these MAC addresses you want to display. Enter the number of MAC entries you want to display or press **<Enter>** to select the default in brackets [20].

4. The Learned MAC Address/VLAN Membership Table displays as follows:

MAC Address	Slot/Intf/Service/Instance	AT VLAN Membership
0020DA:05F623	4/ /1 /Brg 1	1
0020DA:021533	4/ /1 /Brg 1	1
0020DA:0205B3	4/ /1 /Brg 1	1
0020DA:06BAD3	4/ /1 /Brg 1	1
0020DA:05F610	4/ /1 /Brg 1	1

MAC Address. The MAC address for which virtual interface and VLAN membership information will be displayed.

Slot/Intf/Service/Instance. Specifies the virtual port for which AutoTracker VLAN information will be displayed. The **Slot** is the physical slot location to which the MAC address maps. The **Intf** is the physical port to which the MAC address maps. The **Service** is the service type for this MAC address. The service type may be a Router (**Rtr**), Bridge (**Brg**), Classical IP (**CIP**), FDDI Trunk (**Trk**), or an 802.10 Trunk (**T10**). **Instance** is the specific instance of this service type. These different instances are identified numerically. The first instance of a service type belonging to a physical port is identified as 1, the second instance is identified as 2, etc.

AT VLAN Membership. The AutoTracker VLANs to which this MAC Address belongs. An MAC address may belong to more than one VLAN. For example, let's say a MAC device runs on an IPX network. It could be included in a MAC Address policy for one AutoTracker VLAN and the IPX Protocol Policy of another VLAN.

Application Example: DHCP Policies

This application example shows how Dynamic Host Configuration Protocol (DHCP) port and MAC address policies can be used in a DHCP-based network. DHCP is built on a client-server model in which a designated DHCP server allocates network addresses and delivers configuration parameters to dynamically configured clients.

Since DHCP clients initially have no IP address, placement of these clients in an AutoTracker VLAN presents a problem. AutoTracker determines VLAN membership by looking at traffic from source devices. Since the first traffic transmitted from a source DHCP client does not contain the actual address for the client (because the server has not allocated the address yet), the client may not be placed in the same VLAN as its server.

Before the introduction of DHCP port and MAC address rules, various strategies were deployed to use DHCP with Groups and VLANs. Typically these strategies involved IP protocol and network rules along with Bootp relay functionality. (See Chapter 29 for some application examples of these strategies.) These solutions required that all DHCP clients in a particular mobile group or VLAN be grouped together through a common IP policy.

DHCP port and MAC address rules simplify the configuration of DHCP networks. Instead of relying on IP-based policies to group all DHCP clients in the same network as a DHCP server, you can manually place each individual DHCP client in the VLAN or mobile group of your choice. DHCP port and MAC address policies operate the same way as standard port and MAC address policies except these new rules have been enhanced for use with DHCP clients.

The VLANs

This application example contains three (3) AutoTracker VLANs within a single non-mobile group. These VLANs are called Test, Production, and Branch.

The Test VLAN connects to the main network, the Production VLAN, through an external router. This VLAN is intended to be self-contained such that copies of it could be made and attached to the Production VLAN in the same way this VLAN does. The Test VLAN contains its own DHCP server and DHCP clients. The clients gain membership to the VLAN through DHCP port rules.

The Production VLAN carries most of the traffic in this network. It does not contain a DHCP server, but does contain DHCP clients that gain membership through DHCP port rules. Two external routers connect this VLAN to the Test VLAN and a Branch VLAN. One of the external routers—the one connected to the Branch VLAN—has Bootp relay functionality enabled. It is through this router that the DHCP clients in the Production VLAN access the DHCP server in the Branch VLAN.

The Branch VLAN contains a number of DHCP client stations and its own DHCP server. The DHCP clients gain membership to the VLAN through both DHCP port and MAC address rules. The DHCP server allocates IP addresses to all clients in this VLAN as well as the DHCP clients in the Production VLAN.

DHCP Servers and Clients

DHCP clients must be able to communicate with a DHCP server at initialization. The most reliable way to ensure this communication is for the server and its associated clients to share the same VLAN or mobile group. However, if the network configuration does not lend itself to this solution (as the Production VLAN does not in this application example), then the server and clients can communicate through a router with Bootp relay enabled.

The DHCP servers and clients in this example are either in the same VLAN or are connected through a router with Bootp relay. All clients in the Test VLAN receive IP addresses from the server in their VLAN (Server 1). Likewise, all clients in the Branch VLAN receive IP addresses from their local server (Server 2). The DHCP clients in the Production VLAN do not have a local DHCP server, so they must rely on the Bootp relay functionality in external Router 2 to obtain their IP addresses from the DHCP server in the Branch VLAN.

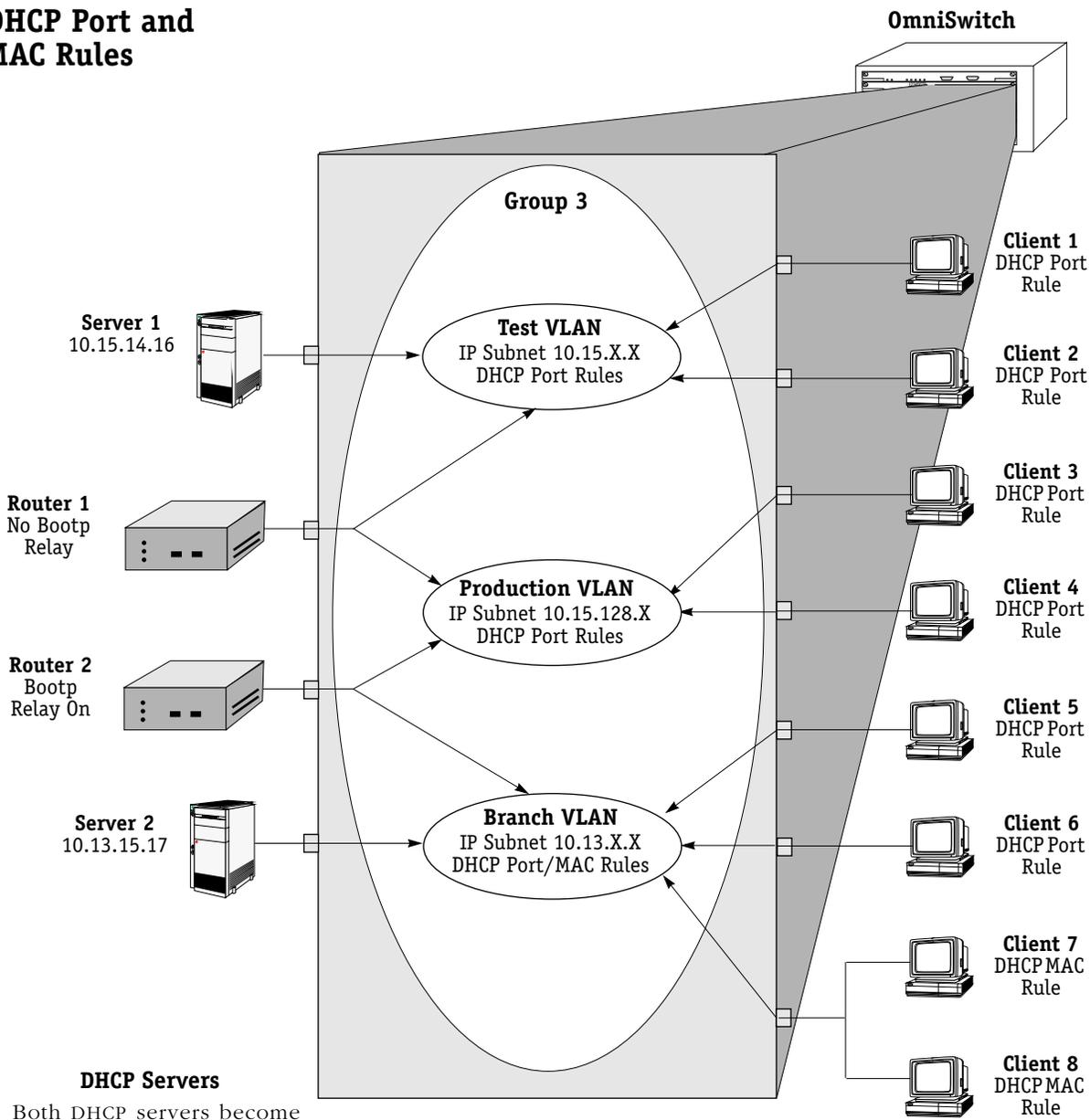
Both DHCP servers gain membership to their VLANs through IP network address policies.

The following table summarizes the VLAN architecture and policies for all devices in this network configuration. The diagram on the following page illustrates this network configuration.

Devices and VLAN Membership

Device	VLAN Membership	Policy Used/Router Role
DHCP Server 1	Test VLAN	IP subnetwork rule=10.15.X.X
DHCP Server 2	Branch VLAN	IP subnetwork rule=10.13.X.X
External Router 1	Test VLAN Production VLAN	Connects Test VLAN to Production VLAN
External Router 2	Production VLAN Branch VLAN	Bootp relay provides access to DHCP server in Branch VLAN for clients in Production VLAN.
DHCP Client 1	Test VLAN	DHCP Port Rule
DHCP Client 2	Test VLAN	DHCP Port Rule
DHCP Client 3	Production VLAN	DHCP Port Rule
DHCP Client 4	Production VLAN	DHCP Port Rule
DHCP Client 5	Branch VLAN	DHCP Port Rule
DHCP Client 6	Branch VLAN	DHCP Port Rule
DHCP Client 7	Branch VLAN	DHCP MAC Address Rule
DHCP Client 8	Branch VLAN	DHCP MAC Address Rule

DHCP Port and MAC Rules



Both DHCP servers become members in their respective VLANs via IP subnet rules.

Routers

Router 1 provides connectivity between the Test VLAN and the Production VLAN. It does not have Bootp functionality enabled so it cannot connect DHCP servers and clients from different VLANs.

Router 2 connects the Production VLAN and the Branch VLAN. With Bootp relay enabled, this router can provide connectivity between the DHCP server in the Branch VLAN and the DHCP clients in the Production VLAN.

DHCP Clients

Clients 1 to 6 are assigned to their respective VLANs through DHCP port rules. Clients 3 and 4 are not in a VLAN with a DHCP server so they must rely on the server in the Branch VLAN for initial addressing information. Clients 7 and 8 share a port with other devices, so they are assigned to the Branch VLAN via DHCP MAC address rules.

26 Interswitch Protocols

This chapter describes Interswitch Protocols, which are used to discover adjacent switches, and track VLAN membership and retain mobile group information across switches. They include two new protocols and one existing protocol that is updated for release 4.0:

- Mapping Adjacency Protocol (XMAP), a new protocol used to discover the topology of OmniSwitches and OmniSwitch/Routers (Omni S/Rs)
- Group Mobility Advertisement Protocol (GMAP), a new protocol used to retain learned mobile group and protocol information
- VLAN Advertisement Protocol (VAP), an existing interswitch protocol used to exchange VLAN information between switches

The protocols are independent of each other and perform separate functions. Each protocol is described in detail in separate sections of this chapter.

Interswitch Protocol Commands

There is an Interswitch Protocol (XIP) submenu. Select **XIP** from the AutoTracker submenu, and the submenu displays as follows:

<u>Command</u>	<u>XIP Menu</u>
gmapst	Turn Group Mobility Advertisement Protocol (GMAP) ON or OFF
gmapgaptime	Set GMAP inter-message gap time in milliseconds
gmapholdtime	Set GMAP hold time interval time in minutes
gmapupdtime	Set GMAP update interval time in seconds
vlap	Turn VLAN Advertisement Protocol (VAP) ON or OFF
xmapst	Turn the Xylan Mapping Adjacency Protocol (XMAP) ON or OFF
xmapls	List adjacent switches found using the XMAP protocol
xmapdisctime	Set XMAP message interval for discovery phase in seconds
xmapcmntime	Set XMAP message interval for common phase in seconds

Main File Summary VLAN Networking
Interface Security System Services Help

These commands are described in this chapter.

XMAP

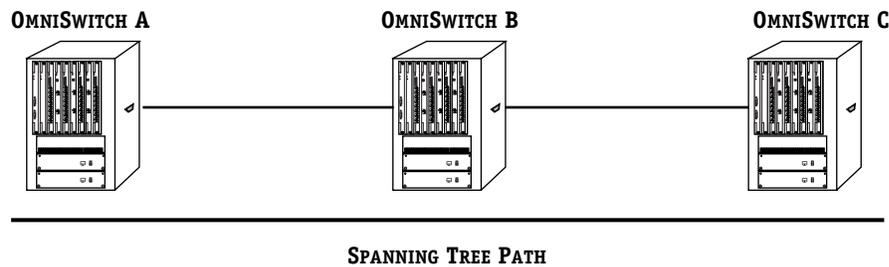
The Mapping Adjacency Protocol (XMAP) is used to discover the topology of OmniSwitches or OmniS/Rs in a particular installation. Using this protocol, each switch determines which OmniSwitches or OmniS/Rs are adjacent to it by sending and responding to Hello update packets. For the purposes of XMAP, *adjacent* switches are those that:

- have a Spanning Tree path between them
- do not have any switch between them on the Spanning Tree path that has XMAP enabled

◆ **Note** ◆

XMAP replaces the Adjacency Only mode of earlier versions of VAP.

In the illustration here, all switches are on the Spanning Tree path. OmniSwitch A and OmniSwitch C have XMAP enabled. OmniSwitch B does not. OmniSwitch A is adjacent to OmniSwitch C and vice versa. If OmniSwitch B enables XMAP, the adjacency changes. A would be adjacent to B, B would be adjacent to both A and C, and C would be adjacent to B.



XMAP Adjacency

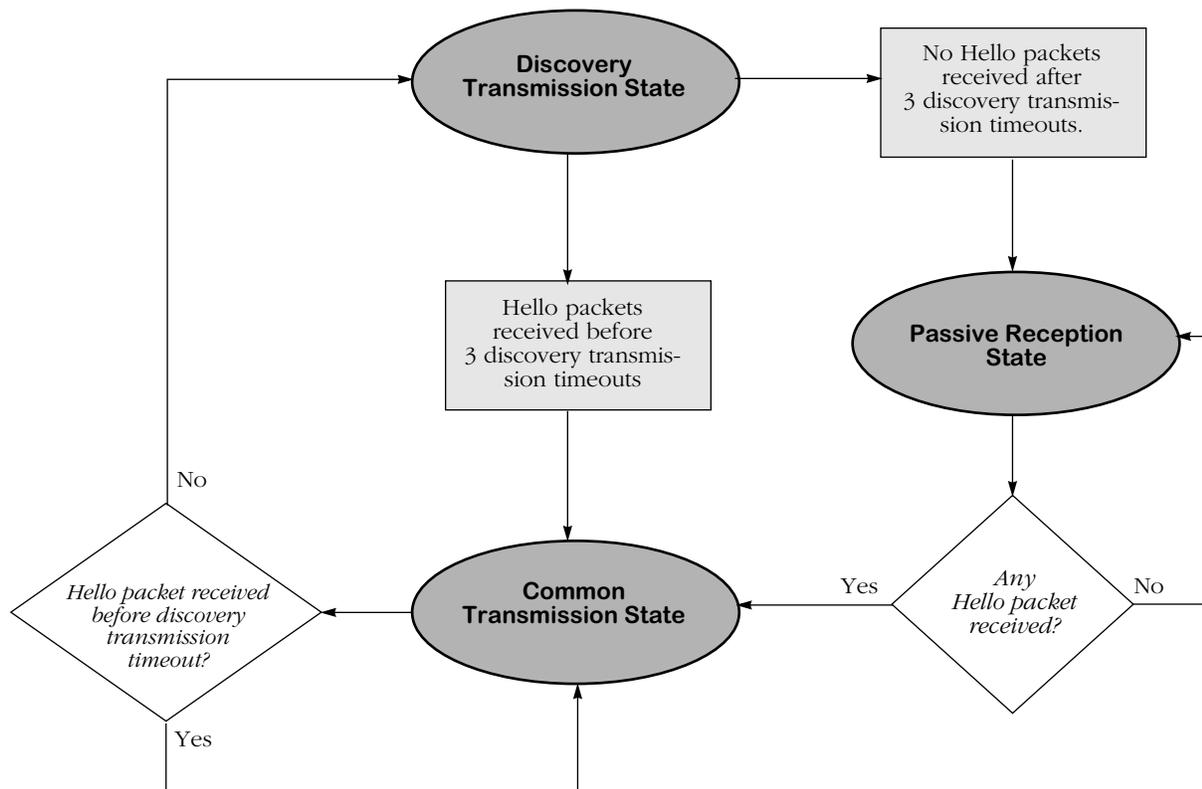
XMAP Transmission States

XMAP switch ports are either in the *discovery transmission state*, *common transmission state*, or *passive reception state*. Ports transition to these states depending on whether or not they receive Hello responses from adjacent switches.

◆ Note ◆

All Hello packet transmissions are sent to a well-known MAC address (0020DA000003).

The transmission states are illustrated here.



XMAP State Transitions

Discovery Transmission State

When XMAP is active, at startup all active switch ports are in the discovery transmission state. In this state ports send out Hello packets and wait for Hello responses. Ports send out Hello packets at a configurable interval called the *discovery transmission time*. The discovery transmission time is configurable; 30 seconds is the default. The ports send out Hello packets up to *three* timeouts of this interval trying to discover adjacent switches.

Any switch ports that receive Hello packets before three discovery transmission times expire send a Hello reply and transition to the common transmission state. Any switch ports that do not receive a Hello response before three discovery transmission times have expired are placed in the passive reception state.

Common Transmission State

In the common transmission state, ports detect adjacent switch failures or disconnects by sending Hello packets and waiting for Hello responses. Ports in this state send out Hello packets at a configurable interval (the default is 5 minutes) called the *common transmission time*. To avoid synchronization with adjacent switches, the common transmission time is jittered randomly by plus or minus ten percent.

Ports wait for Hello responses using the *discovery transmission time* (the default is 30 seconds). If Hello responses are detected within one discovery transmission time, the port remains in the common transmission state. If Hello responses are not detected within one discovery transmission time, the port reverts to the discovery state.

Passive Reception State

In the passive reception state, switch ports are in receive-only mode. Hello packets are not sent out from these ports, and there is no timer on waiting for Hello responses. If the port receives a Hello packet at any time, it enters the common transmission state and transmits a Hello packet in reply.

If a port transitions to the passive reception state, any remote switch entries for that port are deleted.

Common Transmission and Remote Switches

If an XMAP switch is connected to multiple XMAP switches via a hub, the switch sends and receives Hello traffic to and from the remote switches through the same port. If one of the remote switches stops sending Hello packets and other remote switches continue to send Hello packets, the ports in the common transmission state will remain in the common transmission state.

The inactive switch will eventually be aged out of the switch's XMAP database because each remote switch entry has a "last seen" field that is updated when Hello packets are received. The switch checks the "last seen" field at least once every common transmission interval. Switch ports that are no longer "seen" may still retain an entry for up to three common transmission intervals. The slow aging out prevents the port from sending Hello packets right away to the inactive switch and creating additional unnecessary traffic.

Configuring XMAP

XMAP is active by default. In addition to disabling or enabling XMAP, you can view a list of adjacent switches or configure the timeout intervals for Hello packet transmission/reception.

Enabling or Disabling XMAP

To display whether or not XMAP is active or inactive, or to activate or deactivate XMAP, enter the following command:

```
xmapst
```

A screen displays similar to the following:

```
XMAP is currently ACTIVE. (a)ctivate, (d)e-activate : (a) :
```

Enter **a** or **d** to change the current state, or press **<Enter>** to keep the current value. A message similar to the following displays:

```
XMAP is ACTIVE.
```

To change the state of XMAP without displaying the current state first, enter the command with the desired value. For example:

```
xmapst d
```

A message similar to the following displays:

```
XMAP is INACTIVE.
```

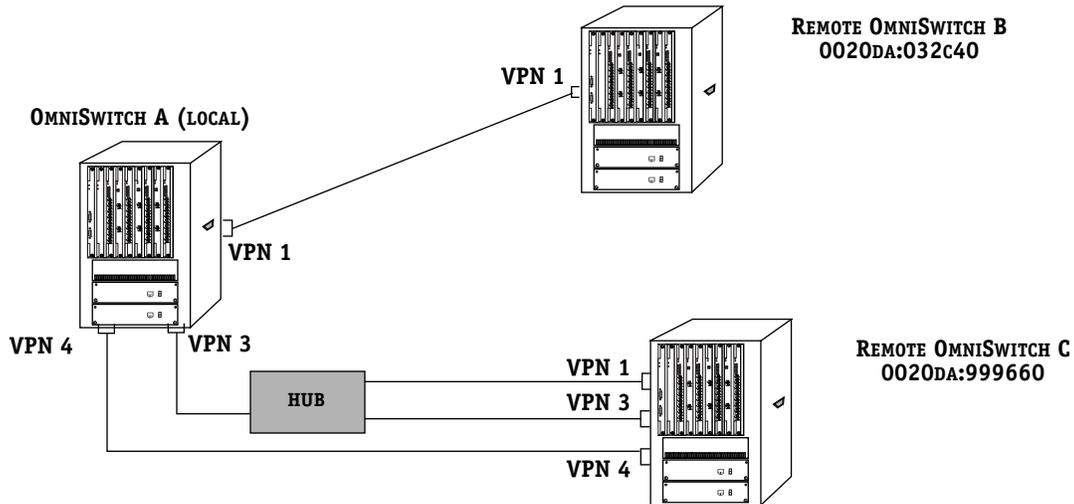
Viewing a List of Adjacent Switches

Use the **xmapls** command to view a list of adjacent switches and their associated MAC addresses, ports, groups, and IP addresses. For remote switches that stop sending Hello packets *and* are connected via a hub, entries may take up to three times the common transmission interval to age out of this table.

The example display shows three virtual ports on a local XMAP switch connected to remote virtual ports on two switches. VPN 3 is connected to a remote switch through a hub.

VPN	Rem Switch ID	Rem VPN	Pri Group	IP Addresses
=====	=====	=====	=====	=====
1	0020da:032c40	1	2	18.1.1.1 27.0.0.2 192.168.10.1 198.206.184.40
3	0020da:999660	1	2	192.168.10.1
		3	7	198.206.184.177
4	0020da:999660	4	9	192.168.10.1 198.206.184.177

A visual illustration of these connections is shown here:



XMAP Network Example

The fields in `xmapls` table are defined as follows:

VPN. The local virtual port number which is connected to an adjacent switch.

Rem Switch ID. The MAC address of the MPM in the adjacent switch.

Rem VPN. The remote virtual port number in the adjacent switch.

Pri Group. The primary group associated with the remote port. The primary group is the group upon which Spanning Tree converges. For more information about primary groups, see Chapter 24, “Managing Groups and Ports.”

IP Addresses. All IP addresses associated with the adjacent switch.

Configuring the Discovery Transmission Time

The discovery transmission time is used in both the discovery transmission state *and* the common transmission state to determine how long the port will wait for Hello packets. For ports in the discovery transmission state, this timer is also used as the interval between sending out Hello packets.

◆ Note ◆

Ports in the common transmission state send out Hello packets based on the common transmission time as described in the next section.

Use the `xmapdisctime` command to view or update the discovery transmission time.

To view the current discovery transmission time, enter the following command:

```
xmapdisctime
```

A message similar to the following displays:

XMAP Discovery Phase Timeout Interval is 30 seconds.

To change the interval, enter the command with the desired value (any value between 1 and 65535). For example:

xmapdisctime 20

A message similar to the following displays:

XMAP Discovery Phase Timeout Interval is 20 seconds.

Configuring the Common Transmission Time

Use the **xmapcmntime** command to view or change the time between sending Hello update packets in the common transmission state. (This timer is only used in the common transmission state.) A switch sends an update for a port just before or after the common transmission time expires.

◆ Note ◆

The switches avoid synchronization by jittering the common transmission time by plus or minus ten percent of the configured value. For example, if the default common transmission time is used (300 seconds), the jitter is plus or minus 30 seconds.

When a Hello packet is received from an adjacent switch before the common transmission time expires, the switch sends a Hello reply and restarts the common transmission timer.

To view the current common transmission time, enter the following:

xmapcmntime

A message similar to the following displays:

XMAP Common Phase Timeout Interval is 300 seconds.

To change the interval, enter the command with the desired value (the value must be between 1 and 65535):

xmapcmntime 200

A message similar to the following displays:

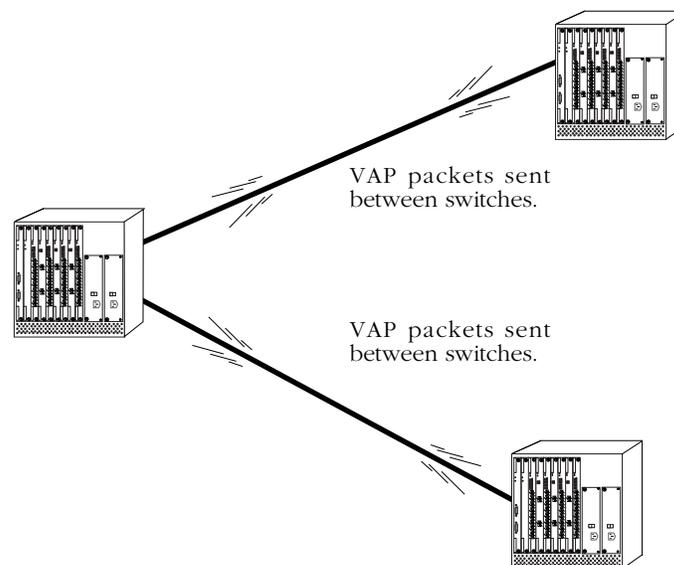
XMAP Common Phase Timeout Interval is 200 seconds.

VLAN Advertisement Protocol (VAP)

The VLAN Advertisement Protocol (VAP) is an interswitch protocol that keeps the VLAN membership databases stored on switches in sync and enables the auto-discovery of network nodes. VAP is useful when you want all VLANs to communicate over a backbone, but do not want locally connected devices to receive all backbone traffic.

In order for a switch to participate in VAP exchanges, VAP must be enabled through a software configuration command. The switch does not need to have attached devices that are a part of all groups and VLANs for which VAP information is exchanged; however, all groups and VLANs must be defined on each switch.

Each switch in a network maintains an AutoTracker database. This database is built by observing traffic that matches user-configured policies. The VAP protocol reads this database on all switches and then advertises entries in the database to all other switches in the network.



VAP Exchanges Between Switches

VAP updates nodes on any new entries in AutoTracker databases every 60 seconds.

VAP also stores information in its own database. Currently this information is used by SNMP-based network management software. The database contains information on VLAN membership; it maps each learned MAC address to a group and to any associated VLANs. This database can contain information on up to 40,000 MAC addresses.

VAP and Port Policies

One of the main purposes of VAP is to advertise the connectivity of devices attached to the switch via AutoTracker port policies. VAP eliminates the need to apply port policies to backbones to ensure that connectivity is established and maintained. When you use port policies, all devices heard through a port will become a member of the VLAN. Using port policies across backbones is not efficient because all devices learned over the backbone would be placed in the same VLAN since they would be attached to the same port.

For this reason, port policies should not be used to interconnect switches because these policies classify MAC addresses on VLANs. Backbone ports should be left in the default VLAN, and only learned devices should be segregated into VLANs by port policies.

There are two types of port policies (or rules), regular port rules and port forwarding rules. Only one can be active at a time. The type of port rule is determined by a command line in the `mpm.cmd` or `mpx.cmd` file. See *Port Policy Functionality* in Chapter 27, “Managing AutoTracker VLANs,” for a detailed explanation of the two port rules settings.

Regular port policy places frames received on a particular port into a VLAN; VLAN membership is based on the port. The current version of VAP supports regular port rules only.

If you set up VAP in its full mode (VLAN membership exchanges and auto-discovery), the switch will automatically set the port policy to *regular* mode.

◆ Note ◆

Earlier versions of VAP include an Adjacency Only mode. If an earlier version of VAP is running on the switch in Adjacency Only mode, when new code is loaded and the switch is rebooted, VAP will be set to off. If an earlier version of VAP is set to Full mode, VAP remains in Full mode when the new code is loaded and the switch is rebooted.

Configuring VAP

There are two settings for the VLAN advertisement protocol, off or full mode. These modes are defined as follows:

- *Full mode*—VLAN membership information exchanged between switches and auto-discovery of network nodes is enabled. This option automatically sets the port policy to regular mode.
- *Off*—Disables VAP exchanges. Nodes will not be auto-discovered and VLAN information will not be exchanged between switches.

To change the VAP mode, at a UI command prompt, enter `vlap` and select the mode in which you want VAP to run. A screen similar to the following displays:

```
The VLAN advertisement protocol is currently not running
To change the mode type: F - full mode, O - off : ( ) :
```

Or, enter the `vlap` command with the desired mode. For example:

```
vlap f
```

A message similar to the following displays:

```
The VLAN advertisement protocol is currently running.
```

The new mode takes effect immediately. You do not need to reboot the switch.

GMAP

The Group Mobility Advertisement Protocol (GMAP) enables workstation users to move from port to port among interconnected switches and still retain all learned mobile group and protocol information. Using GMAP the switch sends a complete list of learned MAC addresses and associated group/protocol information to all interconnected switches in the network. Update and retention times are configurable. A switch that receives a GMAP update packet updates its internal GMAP tables and queries the forwarding database to make any necessary updates.

At startup time and for three successive update intervals, GMAP sends update packets on all virtual ports that are active non-leaf ports (that is, ports that are running Spanning Tree). GMAP packets are sent using the VAP multicast address. After startup and three transmissions, interval packets will only be sent on virtual ports that are active and are known to have an OmniSwitch or OmniS/R running GMAP connected to them.

GMAP will send updates only for MAC addresses that are learned on leaf ports (ports that are not running Spanning Tree). It does not advertise MAC addresses for groups assigned by authentication, and it does not advertise group 1 entries or nonmobile group entries. If conflicting information is received for a MAC address, the last packet received for that address will take precedence.

When AutoTracker learns a new MAC address on a leaf port it attempts to assign it to a mobile group. It consults GMAP tables and any appropriate group membership entries are added to the forwarding database.

GMAP Updating Rules

Upon receiving a packet, GMAP updates its internal tables and queries the forwarding database. When GMAP reviews the forwarding database to update it with new information, it uses the following rules:

- GMAP will only update information for leaf ports.
- GMAP does not add a new MAC address to a port.
- GMAP will only overwrite group 1 entries. If there is no group 1 entry, it will add a new entry, provided that it will not create a conflict with existing entries in the forwarding database.
- GMAP will not add an entry for an authenticated group.
- GMAP will not add an entry that is in conflict or potential conflict with a binding rule. A potential conflict would be a binding rule that requires the IP address be known for the MAC address. GMAP does not have access to IP information.
- GMAP will not add an entry for a group/protocol pair when there is an existing entry for that protocol on the requested port.
- When GMAP finds an entry for the desired group already on the switch but not on the requested port, it will move it to the requested port.
- When GMAP finds an entry with the appropriate group but a protocol value of 0 (indicating all protocols), it will update the protocol value in that entry to that in its database.

Configuring GMAP

GMAP is inactive by default. In addition to enabling and disabling GMAP, you can configure the time between packet transmissions (when multiple packets are required for an update), the time between updates, and the length of time GMAP will retain its current information.

Enabling and Disabling GMAP

Use the **gmapst** command to display or change the state of GMAP. A prompt similar to the following displays:

```
GMAP is currently INACTIVE. (a)ctivate, (d)e-activate: (d)
```

Enter **a** or **d** or press **<Enter>** to keep the current value. A message similar to the following displays:

```
GMAP is ACTIVE.
```

To change the state of GMAP without displaying the current state first, enter the command with the desired value. For example:

```
gmapst d
```

The following message displays:

```
GMAP is INACTIVE.
```

Configuring the Gap Time

Use the **gmappgptime** command to display or change the interpacket gap time used when multiple packets are required for an update. When there are many MAC addresses on mobile ports, more than one GMAP packet is required for an update. Typically the gap time does not have to be changed, but you may want to modify it if traffic spikes are occurring in the network.

To view the current gap time, enter the following command:

```
gmappgptime
```

A message similar to the following displays:

```
GMAP Gap Time is 133 milliseconds.
```

To change the gap time, enter the command with the desired value (any value between 0 and 65535). For example:

```
gmappgptime 100
```

A message displays similar to the following:

```
GMAP Gap Time is 100 milliseconds.
```

The switch approximates the gap time because its internal clock does not use milliseconds. For any value shorter than one second, the switch uses 1/60 second increments called “ticks.” The default for gap time is 8 ticks or approximately 133 milliseconds. Any value you enter will be rounded to the nearest tick.

Configuring the Interpacket Update Time

Use the **gmapupdtime** command to display or change the time between sending updates.

◆ **Note** ◆

The switches avoid synchronization by jittering the update time by plus or minus one quarter of the configured interval. For example, if the default of 300 seconds is used, the jitter is plus or minus 75 seconds.

To view the current update time, enter the following:

```
gmapupdtime
```

A message similar to the following displays:

```
GMAP Update Time is 300 seconds.
```

To change the update time, enter the command and the desired time (any value between 1 and 65535). For example:

```
gmapupdtime 100
```

A message similar to the following displays:

```
GMAP Update Time is 100 seconds.
```

Configuring the Hold Time

Use the **gmapholdtime** command to display or change the length of time for which GMAP will retain information it has learned.

To view the current hold time, enter the following:

```
gmapholdtime
```

A message similar to the following displays:

```
GMAP Hold Time is 4320 minutes.
```

The default is 4320 minutes (72 hours). To change the current hold time, enter the command followed by the desired value (any value between 1 and 65535). For example:

```
gmapholdtime 2880
```

A message similar to the following displays:

```
GMAP Hold Time is 2880 minutes.
```

Displaying GMAP Statistics by MAC Address

To display GMAP statistics for all MAC addresses, use the **gmapls** command. The screen displays similar to the following:

GMAP Table						
MAC Address	Protocol	Group	Src Switch ID	Flags	Timeout(sec)	
000502:C07F11	1809B	12	0020DA:ECC770	00:00:00:00	3536	
	800	12	0020DA:ECC770	00:00:00:00	3536	
00105A:1873B9	1809B	12	0020DA:ECC770	00:00:00:00	3536	
	800	23	0020DA:ECC770	00:00:00:00	3536	

To limit the display, specify the MAC address. For example:

```
gmapls 00105A:C07F11
```

Fields in this table are defined as follows:

MAC Address. The MAC address of the local end station.

Group. The group(s) to which the MAC address belongs.

Protocol. The protocol associated with the group on the switch from which the information was received. Protocol values are defined as follows:

- e0e0 or ffff — IPX over 802.3
- 8137 — IPX over Ethernet II
- 18137 — IPX over SNAP
- 28137 — any IPX encapsulation
- 800 — IP
- 809b — AppleTalk
- 1809b — AppleTalk over SNAP
- 6003 — DECNET

Src Switch ID. The MAC address of the switch from which the entry was received.

Flags. The first two bytes are not used. The third byte displays the AutoTracker flags associated with the entry on the source switch. The last byte displays the router flags associated with this entry on the source switch.

Timeout (sec). The number of seconds remaining until this entry is deleted (unless another GMAP message is received and then the entry is refreshed).

27 Managing AutoTracker VLANs

In a large, flat, switched network, broadcast traffic can overload a network based primarily on port-based Groups. Through the use of AutoTracker VLANs, you can control broadcast traffic such that it is forwarded only to those VLANs where it needs to be sent.

VLANs are created within a Group to subdivide network traffic based on specific criteria. The criteria you use to define a VLAN are called AutoTracker policies. AutoTracker policies can be defined by port, MAC address, protocol, network address, a user-defined policy, or a multicast policy. You can also define multiple policies—also referred to as “rules”—for a VLAN if you wish. A port or device is included in a VLAN if it matches any one VLAN rule. For example, you can define rules based on MAC address and rules based on protocol in the same VLAN.

A Group defines a physical space within the network—a set of ports. The policies that you define for VLAN membership are applied to all traffic on those ports, but not to traffic on ports outside the Group.

You can create two types of policy-based VLANs: AutoTracker VLANs and multicast VLANs. You can create up to 31 AutoTracker VLANs and up to 32 multicast VLANs in any one Group. AutoTracker VLANs and multicast VLANs operate independently of one another: the policies you establish for AutoTracker VLANs neither conflict nor interfere with the policies you establish for multicast VLANs, even when those policies involve the same ports or MAC addresses.

This chapter provides an overview of AutoTracker VLANs and multicast VLANs as well as instructions for managing and monitoring each type of VLAN. Instructions for configuring AutoTracker policies can be found in Chapter 25, “Configuring Group and VLAN Policies.”

The AutoTracker Menu

All software commands for configuring AutoTracker policies and AutoTracker/multicast VLANs are in the AutoTracker menu. This menu is a submenu of the VLAN menu. You can access the AutoTracker menu by typing **at** any prompt. The menu displays as follows:

Command	Auto-Tracker Management Menu
cratvl	Create an Auto-Tracker VLAN
atvl	View definition of Auto-Tracker VLAN
viatrl	View Auto-Tracker Rule Configuration
rmatvl	Delete an Auto-Tracker VLAN
modatvl	Modify definition of an Auto-Tracker VLAN
vivl	View list of Active Auto-Tracker VLANs on an interface
fwtvvl	View VLAN assignment of learned MAC addresses
defvl	Enable or disable membership in default VLAN
crmcvl	Create a Multicast VLAN
mcvl	View definition of Multicast VLAN
vimcrl	View Multicast VLAN Rule Configuration
rmmcvl	Delete a Multicast VLAN
modmcvl	Modify definition of a Multicast VLAN
vimcvl	View list of Active Multicast VLANs on an interface
gmstat	Turn Group Mobility Status ON or OFF
vpl	View Virtual Ports in a Mobile Group
vigl	View Mobile Group List for a Virtual Port
cats	Create Auto-Activated Services
data	Delete Auto-Activated Services
vats	View Auto-Activated Services
vag	View Authenticated Groups
gmcfg	Configure Group Mobility Parameters
mag	Modify Authenticated Group
xip	Enter the Xylan Inter-switch Protocol (XIP) sub-menu

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

The commands on the AutoTracker menu can be roughly divided into two halves. The first half of commands—listed from **cratvl** to **vimcvl**—apply mainly to AutoTracker VLANs (i.e., VLANs created inside non-mobile groups). An exception to this rule is the **modatvl** command, which can be used to modify AutoTracker policies for VLANs or mobile groups. In addition many of the informational commands apply to both VLANs and mobile groups. The commands that apply to AutoTracker VLANs are described in this chapter. Multicast VLANs are described in Chapter 28, “Multicast VLANs.” The mag command is described in the *Switched Network Services User Manual*. The XIP sub-menu is described in Chapter 26, “Inter-switch Protocols.”

The commands from **gmstat** to **gmcfg** apply strictly to mobile groups. All of the commands in this second set are described in Chapter 24, “Managing Groups and Ports.”

AutoTracker VLANs

AutoTracker VLANs enable you to control communications between end stations in your network. You define policies that determine membership in the VLAN and AutoTracker automatically locates ports or devices within the Group that fit the policies and places them into the VLAN.

You can define physical policies or logical policies (or combinations thereof) to determine membership in AutoTracker VLANs. Physical policies consist of port rules: you define the VLAN members as one or more specific ports and VLAN membership is limited to the ports defined and the MAC addresses of devices connected to those ports.

Logical VLAN policies can consist of MAC address rules, protocol rules, network address rules, or user-defined rules. Ports are assigned to VLANs that have logical rules when the MPM examines frames that originate from devices connected to the Group's set of ports. If a frame is received that matches a logical VLAN rule, the source device's MAC address and the port to which the source device is connected are both made VLAN members.

The members of an AutoTracker VLAN thus consist of source devices originating frames that fit the VLAN's policies and the ports to which those source devices are connected. Instructions for creating AutoTracker VLANs begin on page 27-16.

AutoTracker VLAN Policies

You can define a maximum of 32 AutoTracker policies of each type per Group. There is no restriction on the number of rules you can define per VLAN, as long as the maximum number of policies for the Group is not exceeded.

A switch port – or a device connected to a switch port – can belong to more than one VLAN simultaneously, as determined by the rules the port or device matches. A port or device is included in a VLAN if it matches any one rule.

You can define the following types of rules:

Port Policies. Port policies enable you to define membership in the VLAN on the basis of ports. Members of the VLAN will consist of devices connected to specific ports on one switch or on multiple switches in the Group.

MAC Address Policies. MAC address policies enable you to define membership in the VLAN on the basis of devices' MAC addresses. This is the simplest type of rule and provides the maximum degree of control and security. Members of the VLAN will consist of devices with specific MAC addresses. These devices may all be connected to one switch or they may be connected to different switches in the Group. A maximum of 10,240 MAC addresses are supported per policy.

Protocol Policies. Protocol policies enable you to define membership in the VLAN on the basis of the protocol that devices use to communicate. All devices that communicate with the specified protocol become members of the VLAN.

You can specify VLAN membership according to the following protocols: IP, IPX, AppleTalk, or DECNet. In addition, you can specify membership according to Ethernet type, source and destination SAP (service access protocol) header values, or SNAP (sub-network access protocol) type.

Network Address Policies. Network address policies enable you to define membership in the VLAN on the basis of network address criteria.

For example, you can specify that all IP users with a specific subnet mask be included in the VLAN. Or, you can specify that all IPX users in a specific network address area using a certain encapsulation type be included in the VLAN.

If you define network address and port or protocol rules in the same VLAN, the network address rules will take precedence over the port and protocol rules should any conflict arise. To reverse this precedence (i.e., port and protocol rules take precedence over network address rules) you must add the following line to the switch's **mpm.cmd** or **mpx.cmd** file:

Precedence=0

User-Defined Policies. User-defined policies enable you to define membership in the VLAN on the basis of a specific pattern within a frame. All devices that originate frames containing this pattern are assigned to the VLAN. The pattern is specified by defining an offset, a value, and a mask.

Port Binding Policies. A port binding policy specifies a particular device to be included in the mobile group or AutoTracker VLAN. You can bind a device's IP address to a switch port and a MAC address, or bind a device's MAC address to a protocol and a switch port.

DHCP Port Policies. These policies are similar to standard port policies, but apply to switch ports to which DHCP client workstations are attached.

DHCP MAC Address Policies. These policies are similar to standard MAC address policies, but apply to the MAC addresses of DHCP client workstations only.

The Default VLAN

The default AutoTracker VLAN, also referred to as VLAN #1, is different from other AutoTracker VLANs. The following list outlines some of these differences.

1. The default VLAN is automatically created when you create a new Group. Non-default VLANs must be created through the **cratvl** command.
2. The default VLAN cannot be removed. Other VLANs can be removed through the **rmatvl** command.
3. You cannot apply AutoTracker policies to the default VLAN. Other non-default AutoTracker VLANs allow you to apply any policy to them.

You can enable routing on the default VLAN. You enable the default VLAN virtual router through the **crgp** or **modvl** command. See Chapter 24, "Managing Groups and Ports," for further information on the virtual router port on the default VLAN.

All ports and devices in a Group initially belong to default VLAN #1. All physical switch ports always remain members of the default VLAN, but they can also become members of other VLANs. It is not possible to delete a physical switch port from VLAN #1. Individual network devices, however, can move out of VLAN #1. All MAC devices are also initially part of default VLAN #1. However, when a MAC device is removed from default VLAN #1 and moved into a non-default VLAN, it is deleted from default VLAN #1.

The default VLAN is explained further in other sections of this chapter. See *How Devices are Assigned to AutoTracker VLANs* on page 27-5 for a discussion of default VLAN membership issues and the **defvl** command. Also, see *Application Example 4* in Chapter 29, "AutoTracker VLAN Application Examples," for discussions of routing issues and the default VLAN.

How Devices are Assigned to AutoTracker VLANs

When a broadcast frame, a multicast frame, or a unicast frame from an unknown device is received at a switching module, the frame is forwarded to the MPM for processing. Source learning logic on the MPM module examines the entire frame to determine the VLAN or VLANs in which the originating device should be a member. If the frame matches any one policy defined for a VLAN, the originating device (and the port to which it is connected) are made members of that VLAN. If the frame does *not* match any VLAN policy, one of the following occurs:

- If the **defvl** command is on, the source device is made a member of Default VLAN #1 in the Group of which the source port is a member. The **defvl** command determines whether traffic from devices that do not match any policies is assigned to the default VLAN or dropped. (See “The defvl Command” below for more information on this command.)
- If the **defvl** command is off, all traffic from the source device is dropped.

Please Take Note

A broadcast or multicast frame is processed to determine the source device’s VLAN membership each time it is received. A unicast frame is processed to determine the source device’s VLAN membership only the first time it is received.

When the MPM module has determined the VLAN or VLANs in which the originating device belongs, it relays this information to the switching module. The switching module updates a VLAN membership flag attached to the frame’s source MAC address in the CAM (content-addressable memory). The frame is then switched based on this membership flag.

Refer to Chapter 29, “AutoTracker VLAN Application Examples,” for information on AutoTracker VLAN assignments in specific network situations.

The defvl Command

You can turn the **defvl** command on and off simply by entering **defvl on** or **defvl off**. If you enter the command without any parameters, it displays the current setting for the Default VLAN. For example, if source devices are automatically placed in the Default VLAN when they do not match any VLAN policy rule, the following message would display:

membership in default vlan is currently on

If source devices are automatically dropped when they do not match any VLAN policy, the following message would display:

membership in default vlan is currently off

The **defvl** command applies to all Groups in an OmniSwitch and it is only applicable if there is at least one AutoTracker rule configured.

Devices that Generate a Secondary Traffic Type

Source devices sometimes generate more than one traffic type; for example, a device could generate IP traffic primarily but also generate a secondary stream of AppleTalk. When a device generates secondary traffic that does not match any existing VLAN policy, that traffic is grouped into the primary VLAN of which the device is a member.

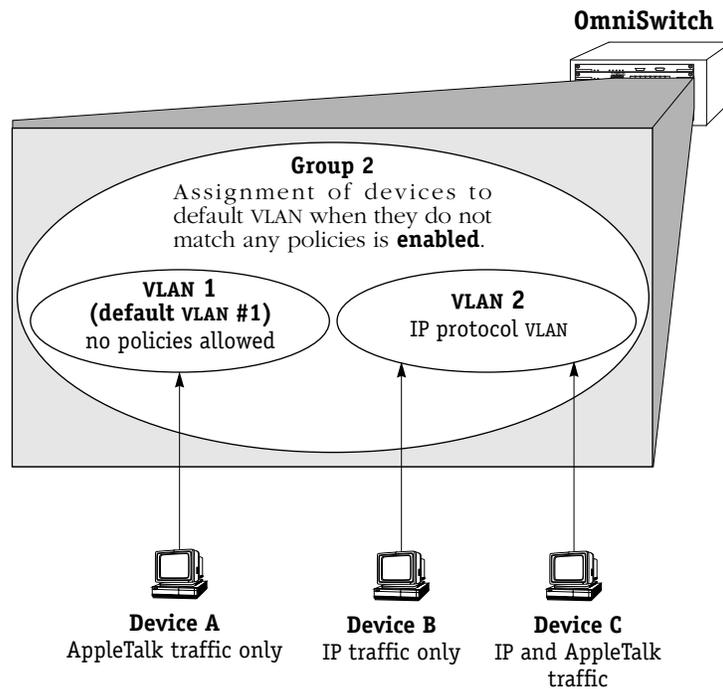
To continue the example, if a device generates both IP and AppleTalk, and both an IP VLAN and an AppleTalk VLAN exist, that device is made a member of both VLANs and no problem occurs. If, however, an AppleTalk VLAN does not exist, all traffic from that device is grouped into the existing VLAN of which the device is a member – in this example, the IP VLAN. This can cause communication problems, as explained below. **For this reason, it is advisable to create VLANs that accommodate all known network traffic.**

In this example Device A is assigned to default VLAN #1 because it does not match any existing VLAN policy.

Devices B and C are assigned to VLAN 2 because they generate IP traffic. The secondary AppleTalk traffic Device C generates is also grouped into VLAN 2, since the AppleTalk traffic does not match any existing VLAN policy.

The result is that Devices A and C are unable to communicate.

Creation of an AppleTalk protocol VLAN solves this problem. If an AppleTalk VLAN exists, Device A will be assigned to it and removed from Default VLAN #1. Device C will be assigned to both the IP VLAN and the AppleTalk VLAN. Devices A and C can then communicate.



How Devices are Assigned to AutoTracker VLANs (*continued*)

Router Traffic in IP and IPX Network Address VLANs

Prior to release 2.1, AutoTracker handled VLAN assignments for router traffic in IP and IPX network address VLANs in the same manner as normal traffic. In release 2.1 and later, AutoTracker differentiates router traffic from normal traffic and can distinguish traffic that is routed *through* a router from traffic that is generated *by* a router.

AutoTracker now determines VLAN assignments for router interfaces (that is, the MAC addresses of router interface ports) in IP and IPX network address VLANs based on router update messages generated by the router itself. This minimizes VLAN leakage and avoids the problem situation described on the facing page.

The Problem with Router Traffic

AutoTracker functions on the assumption that data in a frame can be associated with the frame's source MAC address. For example, if a frame has an IPX network number of 300, AutoTracker assumes that it has received the frame directly and that the source device is a member of IPX network 300. This is not true in the case of routed frames. Routers route frames from one network to another by changing the frame's MAC header but keeping the layer 3 content intact. This can lead to the problem situation described on the facing page.

In the network on the facing page, Device A gets correctly assigned to VLAN 2 and Device B gets correctly assigned to VLAN 3 without problem. The two router interfaces will be assigned to the correct VLANs *if AutoTracker learns the router interface MAC addresses from their RIP updates*. However, this may not happen. The problem situation on the facing page shows what can occur if AutoTracker learns the router interface MAC addresses from traffic routed through the router rather than from traffic generated by the router (such as a RIP update).

How AutoTracker Handles Router Traffic

To avoid the problem situation on the facing page, AutoTracker now determines if any IP or IPX device it has learned is a router. If it is, AutoTracker marks the device as a router, unlearns all previous VLAN assignments for that device, and reassigns the device based on a router-generated update packet (such as a RIP packet).

AutoTracker determines if a learned device is a router by searching further within the frame. For example, if AutoTracker receives an IP frame, it searches beyond the source IP address and also checks if the IP frame is a RIP, OSPF, BGP, DVMRP, or IGRP update. If it is, as explained, AutoTracker marks the device as a router, unlearns its previous VLAN assignments, and reassigns it using the router-generated update packet.

AutoTracker recognizes the following types of router-generated frames:

- IP protocol: RIP frames, OSPF frames, BGP4 frames, DVMRP frames, and IGRP frames
- IPX protocol: IPX RIP frames and SAP frames

AutoTracker maintains a record of the devices it has learned are routers. Each time a router-generated frame is received from a device marked as a router, AutoTracker updates that device's membership in IP or IPX network address VLANs. If a frame received from a device marked as a router is not IP or IPX, VLAN membership is updated normally.

Please Take Note

This special handling of router traffic occurs in IP and IPX network address VLANs only. Note that it does not alter normal VLAN assignment processes such as checking for VLAN policy matches other than IP or IPX network address.

How Routed Frames can Confuse VLAN Assignment

- 2 The router receives the frame on the interface for Network 2 and routes the frame to the interface for Network 3. To do this, the router strips the MAC header from the frame and inserts the MAC address of its interface for Network 3. The frame now specifies its source as Network 2, MAC address Y.

Frame
from Network 2, MAC address Y

- 1 Device A initiates a request to route a frame to Device B. The switch forwards the frame to the router interface for Network 2.

Frame
from Network 2, MAC address A

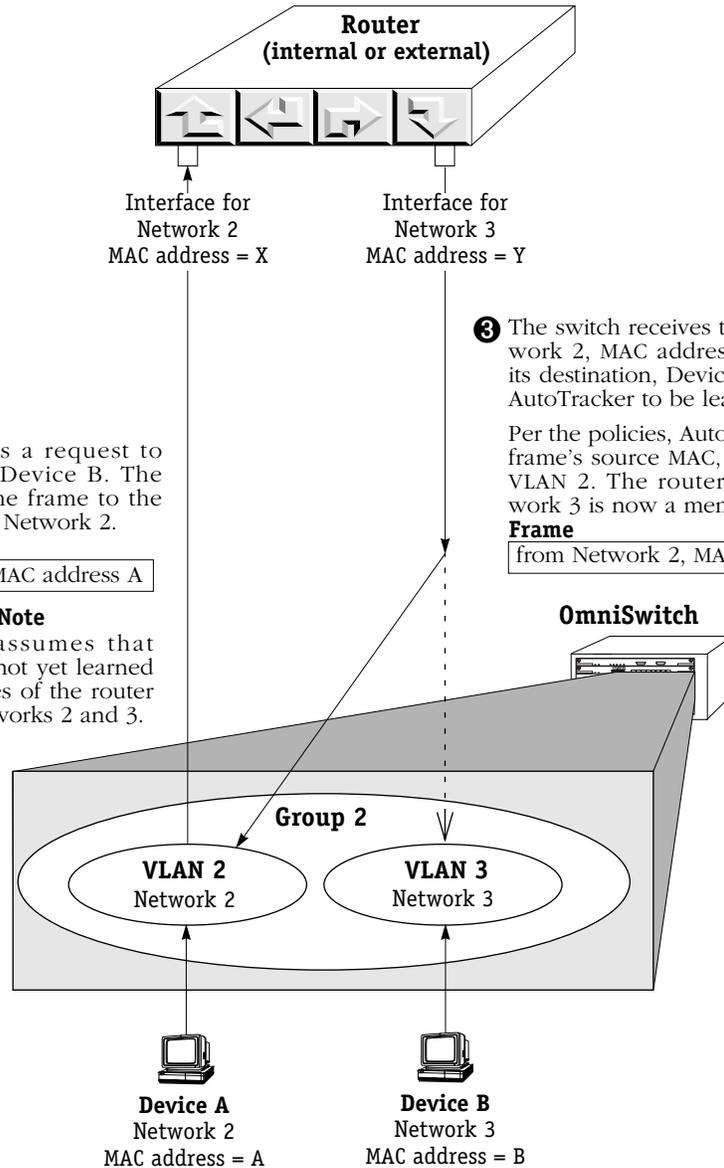
Please Note

This example assumes that AutoTracker has not yet learned the MAC addresses of the router interfaces for Networks 2 and 3.

- 3 The switch receives the frame from Network 2, MAC address Y, forwards it to its destination, Device B, and gives it to AutoTracker to be learned.

Per the policies, AutoTracker assigns the frame's source MAC, MAC address Y, to VLAN 2. The router interface for network 3 is now a member of network 2!

Frame
from Network 2, MAC address Y



- 4 Let's say that the next transmission is a RIP update from the router interface for network 3. The source of the RIP update is Network 3, MAC address Y. AutoTracker thus assigns MAC address Y to VLAN 3. MAC address Y is now assigned to both VLAN 2 and VLAN 3.

The same situation can occur with MAC address X on the router interface for network 2. Both router interfaces will be members of both VLANs and will transmit RIP updates to both.

If this is an IPX network and IPX servers are members of these VLANs, they will respond with router configuration errors. If this is an IP network and devices A and B are IP workstations listening to RIP, they will respond with invalid network address errors.

How Devices are Assigned to AutoTracker VLANs (*continued*)

Port Policy Functionality

In release 2.1 and later, AutoTracker's VLAN port policy can be set to operate in either of two distinct modes:

- In the original mode, wherein membership in all VLANs active on a port is inherited by all devices connected to that port. Original port policy functionality is explained on page 27-10.
- In a new mode, wherein membership in all VLANs active on a port **is not** inherited by all devices connected to that port. This is the current, default functionality with which the switch ships. Current port policy functionality is explained on page 27-11.

Port policy functionality is set on a switch-wide basis, via a flag in the switch's **mpm.cmd** or **mpx.cmd** file called **reg_port_rule**. The switch ships with port policy functionality set to operate in the new mode. You can revert the switch to original port policy functionality by editing the file and setting the **reg_port_rule** flag to 1. You must then restart the switch. (The file is accessed, and can be edited, via the switch User Interface. You can view the current setting of **reg_port_rule** with the **view mpm.cmd** command. See Chapter 11, "Managing Files," for information on editing the **mpm.cmd** or **mpx.cmd** file.)

Why the New Functionality?

Port policies can cause problems in a multi-switch environment. AutoTracker assumes that each switch in a multi-switch environment can independently arrive at identical VLAN assignments for all devices in the network. This is not true when port policies are in effect because of their very nature: port policies are switch-specific and not network wide. The figure on page 27-10, which explains original port policy functionality, provides an example of how port policies can result in inconsistent VLAN membership between two switches – notice the inconsistent VLAN membership in OmniSwitch 1 and in OmniSwitch 2.

The use of port policies in a multi-switch environment can result in connectivity problems if the source switch and the destination switch are separated by other switches. The switches along the path of the frame will not have identical VLAN memberships. At any particular switch along the path, frames could be lost because of inconsistencies in the VLAN membership of the frames' source and destination devices.

In addition, AutoTracker maintains devices in the same VLAN without regard to the devices' location – provided the devices match the same AutoTracker policies throughout the network. Multiple switches will assign a device to the same VLANs provided that device matches the same policies on each switch. This is not possible when port policies are in effect because, as stated, by their very nature port policies are switch-specific and not network-wide.

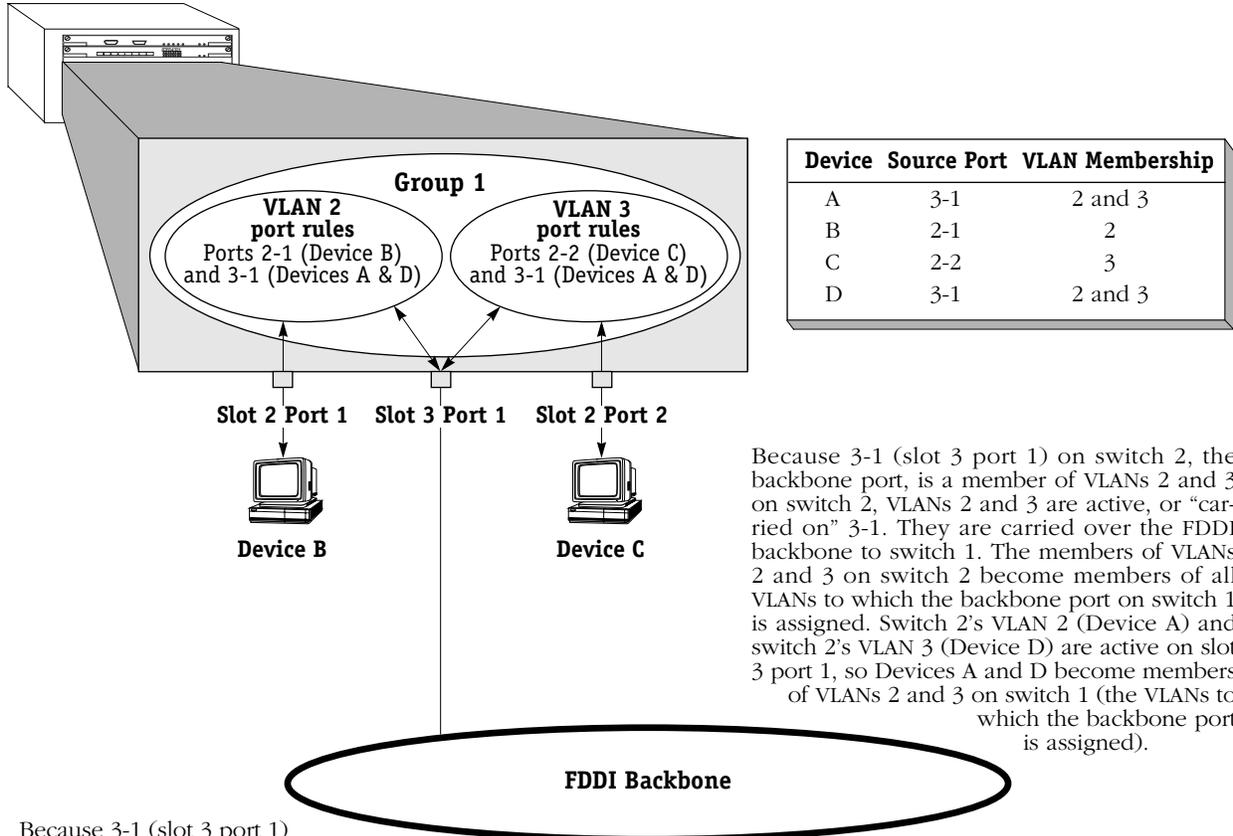
For these reasons, the OmniSwitch now ships with new port policy functionality (although, as explained, you can revert the switch to original port policy functionality if you wish). The new functionality still enables users to assign ports to VLANs and still enables those ports to carry traffic for those VLANs. However, with the new functionality, port policies are not used to learn VLAN assignments for traffic received on ports (as explained on page 27-11). In order for a device to be assigned to a VLAN, it must match an existing logical policy of the VLAN. This is explained on page 27-13.

The Following Examples

The following pages provide examples of original and current port policy functionality. The limitations of port policies become apparent if one tries to use port policies to create two VLANs in these sample networks, one for Devices A and B and one for Devices C and D.

Original Port Policy Functionality
(reg_port_rule = 1)

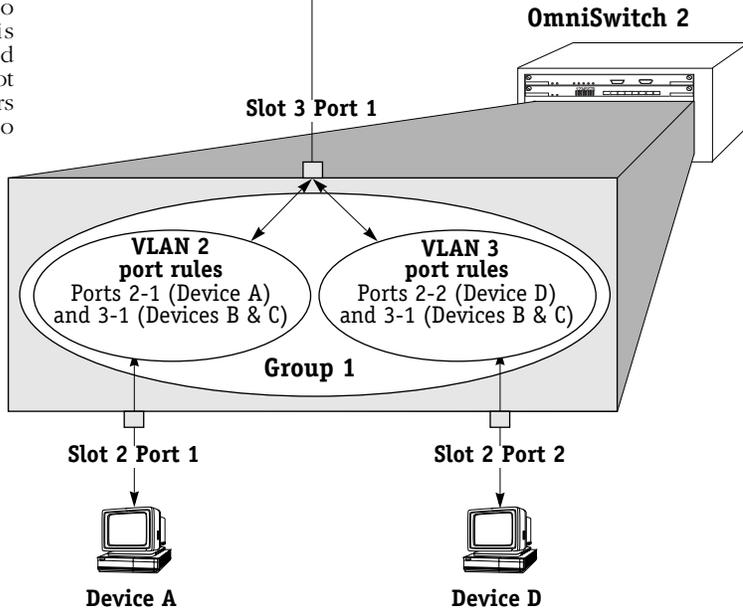
OmniSwitch 1



Because 3-1 (slot 3 port 1) on switch 2, the backbone port, is a member of VLANs 2 and 3 on switch 2, VLANs 2 and 3 are active, or “carried on” 3-1. They are carried over the FDDI backbone to switch 1. The members of VLANs 2 and 3 on switch 2 become members of all VLANs to which the backbone port on switch 1 is assigned. Switch 2’s VLAN 2 (Device A) and switch 2’s VLAN 3 (Device D) are active on slot 3 port 1, so Devices A and D become members of VLANs 2 and 3 on switch 1 (the VLANs to which the backbone port is assigned).

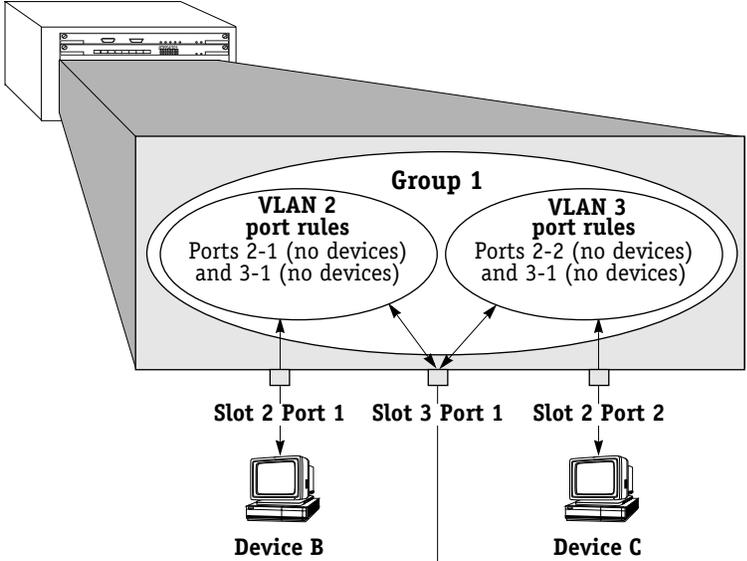
Because 3-1 (slot 3 port 1) on switch 1, the backbone port, is a member of VLANs 2 and 3 on switch 1, VLANs 2 and 3 are active, or “carried on” 3-1. They are carried over the FDDI backbone to switch 2. The members of VLANs 2 and 3 on switch 1 become members of all VLANs to which the backbone port on switch 2 is assigned. Switch 1’s VLAN 2 (Device B) and switch 1’s VLAN 3 (Device C) are active on slot 3 port 1, so Devices B and C become members of VLANs 2 and 3 on switch 2 (the VLANs to which the backbone port is assigned).

Device	Source Port	VLAN Membership
A	2-1	2
B	3-1	2 and 3
C	3-1	2 and 3
D	2-2	3



Current Port Policy Functionality
(reg_port_rule = 0)

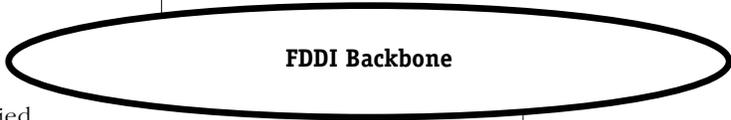
OmniSwitch 1



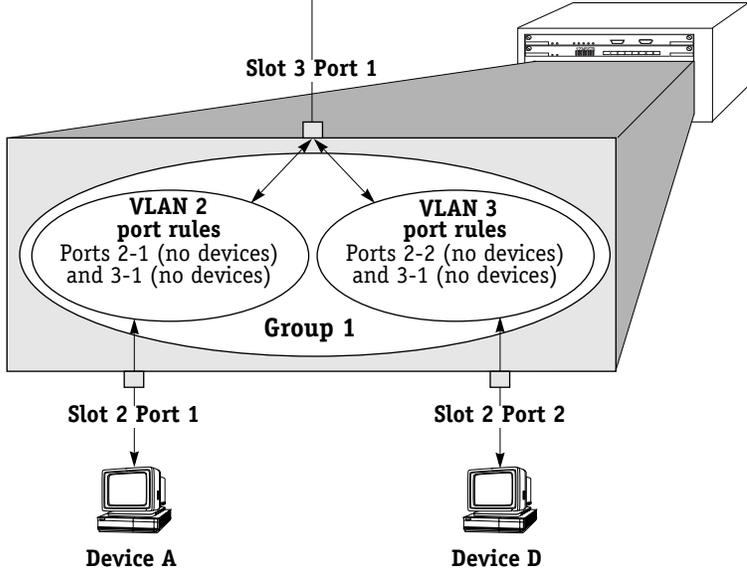
Device	Source Port	VLAN Membership
A	3-1	default VLAN #1
B	2-1	default VLAN #1
C	2-2	default VLAN #1
D	3-1	default VLAN #1

With current port policy functionality, VLANs are not active, or “carried on” ports. Port 3-1 (slot 3 port 1) on switch 2, the backbone port, is still a member of VLANs 2 and 3 on switch 2, but VLANs 2 and 3 **are not** carried over the FDDI backbone to switch 1. The members of VLANs 2 and 3 on switch 2 **do not** become members of all VLANs to which the backbone port on switch 1 is assigned. Rather, they become members of default VLAN #1 on switch 1 if they do not match any of switch 1’s existing VLAN policies and if **defvl** is on for the switch. If **defvl** is off, the traffic is dropped.

With current port policy functionality, VLANs are not active, or “carried on” ports. Port 3-1 (slot 3 port 1) on switch 1, the backbone port, is still a member of VLANs 2 and 3 on switch 1, but VLANs 2 and 3 **are not** carried over the FDDI backbone to switch 2. The members of VLANs 2 and 3 on switch 1 **do not** become members of all VLANs to which the backbone port on switch 2 is assigned. Rather, they become members of default VLAN #1 on switch 2 if they do not match any of switch 2’s existing VLAN policies and if **defvl** is on for the switch. If **defvl** is off, the traffic is dropped.



OmniSwitch 2



Device	Source Port	VLAN Membership
A	2-1	default VLAN #1
B	3-1	default VLAN #1
C	3-1	default VLAN #1
D	2-2	default VLAN #1

The Usefulness of Port Policies

As has been explained – and as illustrated on page 27-10 – original port policy functionality is not well-suited to the creation of consistent VLAN membership in a multi-switch environment. Current port policy functionality – as illustrated on page 27-11 – neither contributes to nor participates in VLAN assignments. Port policies, either original or current, are in fact not useful in the creation of consistent VLAN membership across multiple switches. Logical policies are of far greater use, as illustrated on page 27-13. So, why use port policies at all?

Port Policies are Useful in these Situations:

- **Silent stations.** If a device does not transmit traffic (such as a printer), the port to which the device is connected never gets assigned to VLANs. It is then impossible for other stations to communicate with that device. Creating a port policy that assigns the silent device's port to one or more VLANs will enable traffic to flow out that port to the silent device.
- **Inactive VLANs.** AutoTracker does not activate a VLAN – or its internal router – until a port is assigned to that VLAN. AutoTracker assigns ports to VLANs with port policies immediately. However, AutoTracker only assigns ports to VLANs with logical policies when a frame is received from a source device that matches the VLAN's policies. This means that, in some network situations, you may need to assign a port policy to a VLAN to force it active. *Application Example 5* in Chapter 29 provides an example of this.
- **Backbone connections.** A port policy that assigns the backbone port to a VLAN will enable traffic from that VLAN to flow out onto the backbone.

◆ Important Note ◆

If you are using port policies to extend VLANs across a backbone, you are strongly advised to use current (default) port policy functionality. If you use original port policy functionality, you are, in effect, placing all devices learned from the backbone port into the same VLAN. If the port policy is configured for all VLANs (so that all VLANs can communicate over the backbone), all devices learned from the backbone port are assigned to all VLANs. This is not desirable – it would subject locally-connected devices to all the backbone traffic.

So How Do I Get Devices Assigned to VLANs Over a Backbone?

The way to get devices assigned to VLANs over a backbone is to define logical VLAN policies that so assign them. An example is shown on the facing page utilizing IP and IPX protocol policies. The network on the facing page uses port policies (and current port policy functionality) to assign the backbone port to VLANs on each switch so that traffic can flow out onto the backbone from these VLANs.

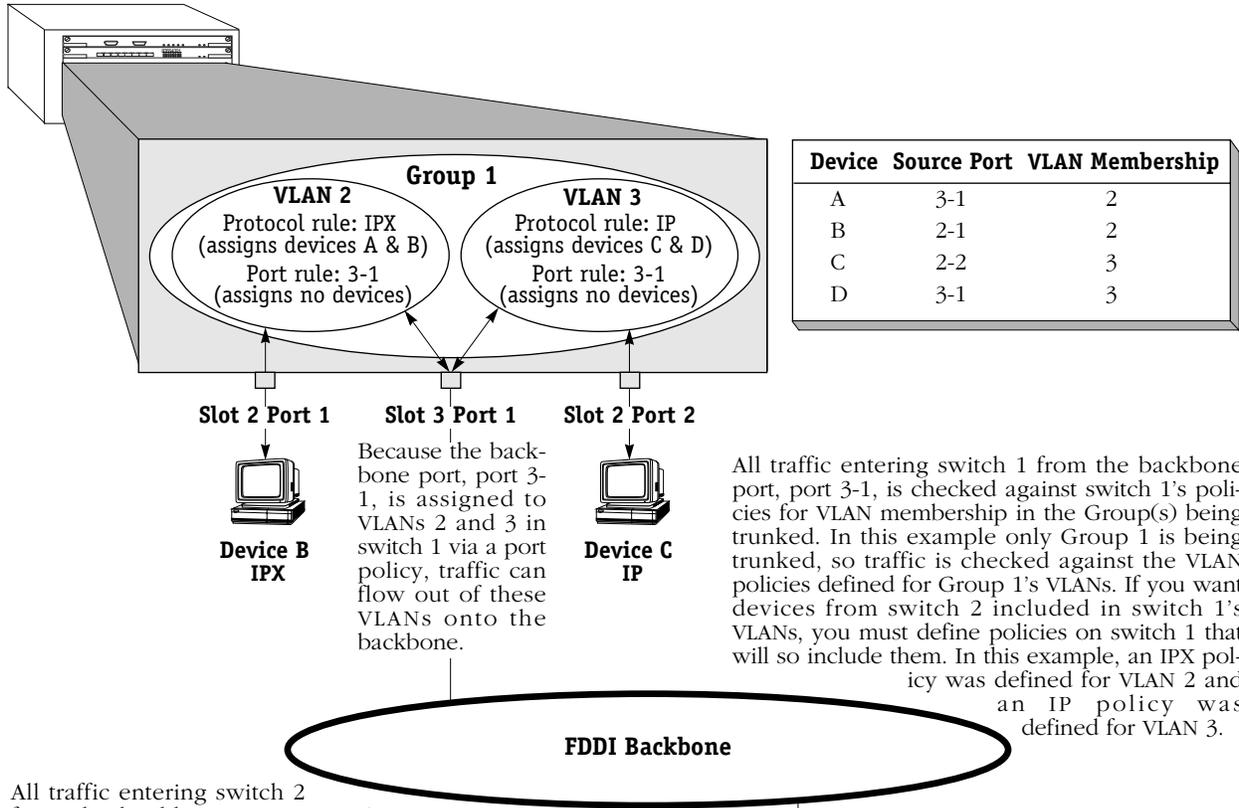
The problem of remote VLAN assignments is solved by the IP and IPX protocol policies. When a frame is received from a backbone port, the frame is examined to determine if it matches any VLAN membership rules. Let's say Device D on switch 2 transmits an IP frame. The frame travels the FDDI backbone and enters switch 1 on port 3-1. AutoTracker learns the frame and assigns it to VLAN 3, since VLAN 3 has an IP protocol policy and the frame is IP.

Notice that with this approach:

- VLAN membership is consistent between the two switches.
- In a multi-switch environment, no frames are lost in switches along the traffic path because of the inconsistent VLAN membership of a frame's source and destination devices.
- Devices can be moved from switch to switch and they will be assigned to the same VLAN – without reconfiguring AutoTracker or the device.
- As was the original intent, it is possible to create two VLANs in this sample network, one for Devices A and B and one for Devices C and D. As is apparent, this was impossible using port policies.

An Example of VLAN Assignment Using Logical Policies and Current Port Policy Functionality (reg_port_rule = 0)

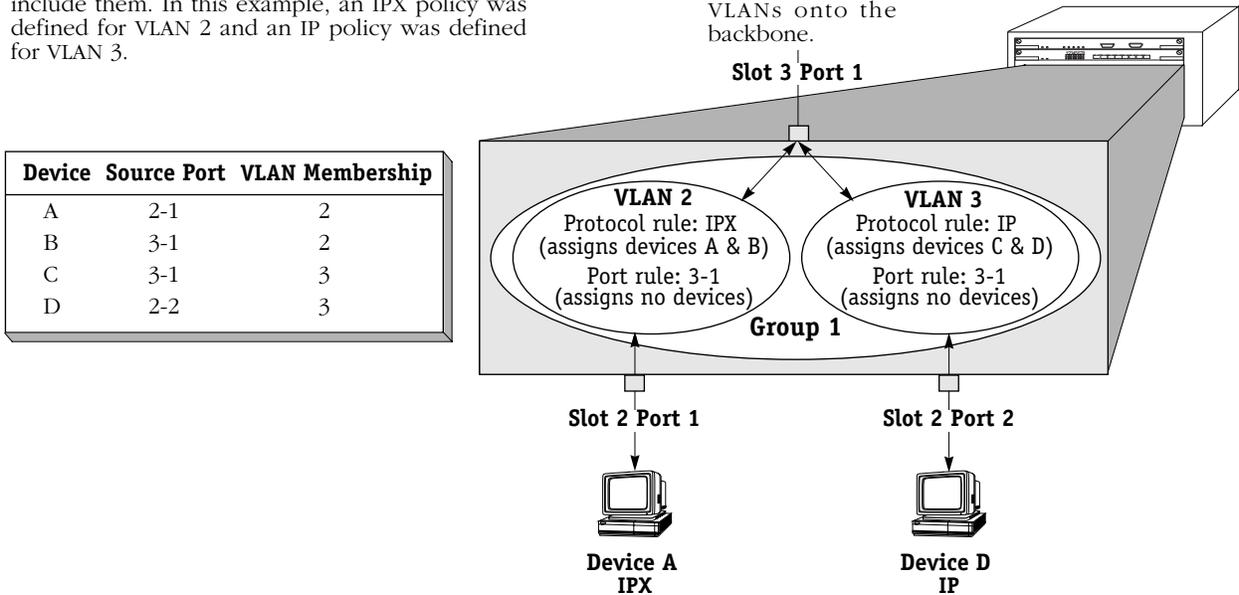
OmniSwitch 1



All traffic entering switch 2 from the backbone port, port 3-1, is checked against switch 2's policies for VLAN membership in the Group(s) being trunked. In this example only Group 1 is being trunked, so traffic is checked against the VLAN policies defined for Group 1's VLANs. If you want devices from switch 1 included in switch 2's VLANs, you must define policies on switch 2 that will so include them. In this example, an IPX policy was defined for VLAN 2 and an IP policy was defined for VLAN 3.

Because the backbone port, port 3-1, is assigned to VLANs 2 and 3 in switch 2 via a port policy, traffic can flow out of these VLANs onto the backbone.

OmniSwitch 2



Frame Flooding in AutoTracker VLANs

Flooding occurs when a frame is received addressed to a device that is unknown to the switch or broadcast or multicast frames are received addressed to multiple users. In a typical bridged environment, the frame would be forwarded out all ports. However, this is not true with VLANs as VLANs segment the network into smaller broadcast domains. In this environment, flooding occurs as follows:

Unicast Traffic

- If the destination address of the frame is unknown but its source address is known and the source device is a member of one or more VLANs, the frame is flooded out all ports of all VLANs in which the source device is a member. Please note the following:
 - If the source device is a member of multiple VLANs, some leakage may occur during the flooding process. Leakage may occur only among VLANs in the same Group—frames do not leak between Groups.
 - If the source device is a member of multiple VLANs and some or all of those VLANs share the same physical port, only one copy of the frame is forwarded out that port.
 - If the source device is a member of multiple VLANs that use trunking, only one copy of the frame is sent to each trunk port.
- If both the source and destination addresses of the frame are unknown, the frame is forwarded to the MPM for processing (to determine the VLAN or VLANs in which the originating device should be a member) **and** the frame is flooded out all ports of all VLANs in which the source port is a member.

Broadcast and Multicast Traffic

Frames are forwarded out all ports that are members of the same VLANs as the source MAC address. If the source MAC address is unknown, it is forwarded out all ports that have VLANs active on the source ports.

Routing Between AutoTracker VLANs

Devices that do not share membership in a common VLAN must use routers to communicate with one another. You can configure a virtual router port that is capable of IP and/or IPX routing for each VLAN. By enabling a router port on a VLAN, you are creating a static route entry within the switch to that VLAN. If this router port is not configured for a VLAN, then that VLAN will not be able to communicate with other VLANs unless an external router is between those VLANs. You may configure up to 16 virtual router ports within a single OmniSwitch. Each VLAN may contain only one router port.

Routing and the Default VLAN. You can enable routing for the default VLAN when you initially create a Group, or when you modify the Group. There are several issues about which you should be aware when enabling routing on the Default VLAN. See *Application Example 4* in Chapter 29, “AutoTracker VLAN Application Examples,” for more information.

Creating AutoTracker VLANs

You create AutoTracker VLANs through the AutoTracker menu options. Creating an AutoTracker VLAN includes the following steps:

- A.** Enter basic information such as the name and number for the VLAN. See *Step A. Entering Basic VLAN Information* on page 27-16 for instructions on this step.
- B.** Define policies that define membership in the VLAN. See *Step B. Defining and Configuring VLAN Policies* on page 27-18 for instructions on this step.
- C.** Configure the type of routing used for communication between VLANs. In order for devices in a VLAN to communicate with devices in other VLANs, a virtual router must be configured or an external router must exist between those VLANs. See *Step C. Configuring the Virtual Router Port (Optional)* on page 27-19 for instructions on this step.

These steps are explained in detail in the sections that follow.

Step A. Entering Basic VLAN Information

1. To begin setting up the AutoTracker VLAN type **cratvl** at any prompt.
2. The following prompt displays:

Enter the VLAN Group id for this VLAN (1):

Enter the number for the Group to which this VLAN will belong. All VLANs belong to a Group. You can create up to 31 VLANs per Group (each Group already contains a default VLAN, VLAN #1).

3. The following prompt displays:

Enter the VLAN Id for this VLAN (2):

Enter the number that will identify this VLAN with the Group specified above. Up to 32 VLANs may belong to the same Group (including the default VLAN). By default the system displays the next available VLAN ID number. Press **<Enter>** to accept this default.

4. The following prompt displays:

Enter the new VLAN's description:

Enter a textual description that will help you identify the VLAN. For example, if you know this VLAN will be composed of only workstations using the IPX protocol, you might call the VLAN, "IPX VLAN." You may use up to 30 characters for this description.

5. The following prompt displays:

Enter the Admin Status for this vlan (Enable (e) / Disable (d):

Enter whether or not you want the Administrative Status for this VLAN to be enabled or disabled. Once enabled, the switch begins using the policies you defined. A disabled VLAN is still defined (name, number, policies intact), but the switch keeps the VLAN disabled. The enable/disable status may be changed at a later time using the **modatvl** command.

Note

A VLAN may not always be operational even when its **Admin** Status is enabled. The VLAN becomes operational as soon as a port is assigned to it. In addition, a VLAN's operation may be disabled by the switch because devices in the VLAN cease transmitting data, among other reasons.

After you enter the Administrative Status, additional prompts display that allow you to select the rules governing membership in this VLAN. Go on to the next section, *Step B. Defining and Configuring VLAN Policies* on page 27-18 to continue setting up this VLAN.

Step B. Defining and Configuring VLAN Policies

You can define AutoTracker policies by port, MAC address, protocol, network address, user definition, or port binding. You can define multiple policies for a AutoTracker VLAN if you wish. A port or device is included in a AutoTracker VLAN if it matches any one rule. For example, you can define rules based on ports, rules based on MAC address, and rules based on protocol in the same AutoTracker VLAN. However, defining multiple rules is not trivial – exercise extreme care when you do so and make sure that you understand the consequences of your definitions. In most situations, it is advisable to use one of AutoTracker’s predefined rules.

Instructions for defining each AutoTracker policy type are included in Chapter 25, “Configuring Group and VLAN Policies.” Follow the directions in that chapter for the policy you wish to set up.

The sections below provide directions for setting up each type of AutoTracker policy. Follow the directions for the policy you wish to set up.

1. When are done specifying AutoTracker policies the following prompt displays:

Configure more rules for this vlan (y/n):

You can set up multiple rules for the same VLAN. Enter a **Y** here if you want to set up more rules in addition to the Network Address rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up on this VLAN. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

VLAN 1:2 created successfully

You are done setting up rules for this VLAN, so you can start configuring the virtual router for this VLAN. See *Step C. Configuring the Virtual Router Port (Optional)* on page 27-19 for information on configuring a virtual router port.

Step C. Configuring the Virtual Router Port (Optional)

You can now optionally configure the virtual router port that this VLAN will use to communicate with other AutoTracker VLANs. A virtual router port for the VLAN is created within the switch. If you do not define a virtual router port for this VLAN, devices within the VLAN will only be able to communicate with devices in other VLANs through an external router.

You will have the choice of configuring IP, IPX, or both IP and IPX routing. Continue with the steps below:

1. After you finish configuring AutoTracker Policies for this VLAN, the following prompt displays:

Enable IP (y):

Press **<Enter>** if you want to enable IP Routing on this virtual router port. If you do not enable IP, then this VLAN will not be able to internally route IP data. If you don't want to set up the IP router port, enter **n**, press **<Enter>** and skip to Step 10.

Note

You may enable routing of both IP and IPX traffic on this router port. If you set up dual-protocol routing, you must fill out information for both IP and IPX parameters.

2. The following prompt displays:

IP Address:

Enter the IP address for this virtual router port in dotted decimal notation or hexadecimal notation (e.g., 198.206.181.10). This IP address is assigned to the virtual router port for this VLAN. After you enter the address, press **<Enter>**.

3. The following prompt displays:

IP Subnet Mask (0xfffff00):

The default IP subnet mask (in parentheses) is automatically derived from the VLAN's IP address class. Press **<Enter>** to select the default subnet mask or enter a new subnet mask in dotted decimal notation or hexadecimal notation and press **<Enter>**.

4. The following prompt displays:

IP Broadcast Address (198.200.10.255):

The default IP broadcast address (in parentheses) is automatically derived from the VLAN's IP address class. Press **<Enter>** to select the default address or enter a new IP broadcast address in dotted decimal notation or hexadecimal notation and press **<Enter>**.

5. The following prompt displays:

Description (30 chars max):

Enter a useful description for this virtual IP router port using alphanumeric characters. The description may be up to 30 characters long. Press **<Enter>**.

6. The following prompt displays:

Disable routing? (n) :

Indicate whether you want to disable routing in the VLAN. You can enable routing later through the **modvl** command.

- The following prompt displays:

Enable NHRP? (n) :

Indicate whether you want to enable NHRP.

- The following prompt displays:

**IP RIP Mode {Deaf (d),
Silent (s),
Active (a),
Inactive (i)} (s):**

Define the RIP mode in which the virtual router port will operate. RIP (Router Information Protocol) is a network-layer protocol that enables this VLAN to learn and advertise routes. The RIP mode can be set to one of the following:

Silent. The default setting shown in parentheses. RIP is active and receives routing information from other VLANs, but does not send out RIP updates. Other VLANs will not receive routing information concerning this VLAN and will not include the VLAN in their routing tables. Simply press **<Enter>** to select Silent mode.

Deaf. RIP is active and sends routing information to other VLANs, but does not receive RIP updates from other VLANs. This VLAN will not receive routing information from other VLANs and will not include other VLANs in its routing table. Enter **d** and press **<Enter>** to select Deaf mode.

Active. RIP is active and both sends and receives RIP updates. This VLAN will receive routing information from other VLANs and will be included in the routing tables of other VLANs. Enter **a** and press **<Enter>** to select Active mode.

Inactive. RIP is inactive and neither sends nor receives RIP updates. This VLAN will neither send nor receive routing information to/from other VLANs. Enter **i** and press **<Enter>** to select Inactive mode.

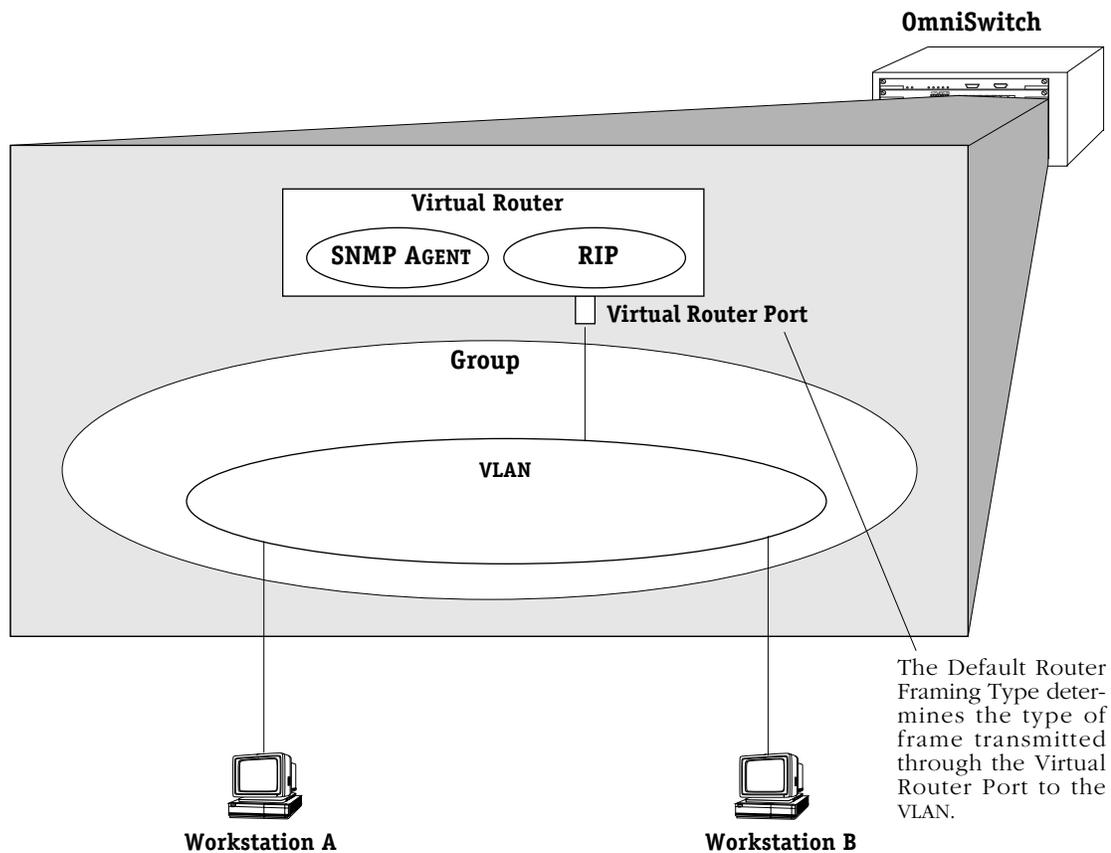
- After you enter the RIP mode, the following prompt displays:

**Default framing type [Ethernet II(e),
fddi (f),
token ring (t),
Ethernet 802.3 SNAP (8),
source route token ring(s)} (e):**

Select the default framing type for the frames that will be generated by this router port and propagated over this VLAN to the outbound ports. Set the framing type to the encapsulation type that is most prevalent in this VLAN. If this VLAN contains devices using encapsulation types other than those defined here, the MPM module must translate those frames, which slows throughput. The figure on the next page illustrates the Default Framing Type and its relation to Virtual Router Port communications.

After you enter the framing type a message displays indicating that this IP router port was created:

Created router port for vlan 1:3



Default Framing Type and the Virtual Router Port

10. You can now configure IPX routing on this port. The following message displays:

Enable IPX? (y) :

Press **<Enter>** if you want to enable IPX Routing on this virtual router port. If you do not enable IPX, then this VLAN will not be able to internally route IPX data. You can set up a virtual router port to route both IP and IPX traffic.

If you don't want to enable IPX routing, enter **n** and press **<Enter>**. You are now done configuring this VLAN. You can monitor activity on this VLAN through other AutoTracker commands. See later section in this chapter for more information on these commands.

11. After selecting to enable IPX, the following prompt displays:

IPX Network:

Enter the IPX network address. IPX addresses consist of eight hex digits and you can enter a minimum of one hex digit in this field. If you enter less than eight hex digits, the system prefixes your entry with zeros to create eight digits.

12. The following prompt displays:

Description (30 chars max):

Enter a useful description for this virtual IPX router port using alphanumeric characters. The description may be up to 30 characters long. Press **<Enter>**.

13. After entering a description, the following prompt displays:

```
IPX RIP and SAP mode {RIP and SAP active (a)
RIP only active (r)
RIP and SAP inactive (i)}                (a):
```

Select how you want the IPX protocols, RIP (router internet protocol) and SAP (service access protocol), to be configured for this VLAN. RIP is a network-layer protocol that enables this VLAN to learn routes. SAP is also a network-layer protocol that allows network services, such as print and files services, to advertise themselves. The choices are:

RIP and SAP active. The default setting. The VLAN to which this IPX router port is attached participates in both RIP and SAP updates. RIP and SAP updates are sent and received through this router port. Simply press **<Enter>** to select RIP and SAP active.

RIP only active. The VLAN to which this IPX router port is attached participates in RIP updates only. RIP updates are sent and received through this router port. Enter an **r** and press **<Enter>** to select RIP only active.

RIP and SAP inactive. The IPX router port is active, but the VLAN to which it is attached does not participate in either RIP nor SAP updates. Enter an **i** and press **<Enter>** to select RIP only active.

14. After selecting the RIP and SAP configuration, the following prompt displays the default router framing type options:

```
Default router framing type for : {
Ethernet Media:
Ethernet II (0),
Ethernet 802.3 LLC (1),
Ethernet 802.3 SNAP (2),
Novell Ethernet 802.3 raw (3),
FDDI Media:
fdi SNAP (4),
source route fdi SNAP (5),
fdi LLC (6),
source route fdi LLC (7),
Token Ring Media:
token ring SNAP (8),
source route token ring SNAP (9),
token ring LLC (a),
source route token ring LLC (b) }      (0) :
```

Select the default framing type for the frames that will be generated by this router port and propagated over the VLAN to the outbound ports. Set the framing type to the encapsulation type that is most prevalent in the VLAN. If the VLAN contains devices using encapsulation types other than those defined here, the MPM module must translate those frames, which slows throughput. See the figure, *Default Framing Type and the Virtual Router Port* on page 27-21 for an illustration of the Default Framing Type and its relation to Virtual Router Port communications.

15. If you chose a Source Routing frame format in the last step (options 5, 7, 9, or b), the an additional prompt displays:

**Default source routing broadcast type : {
ARE broadcasts(a), STE broadcasts(s)} (a) :**

Select how broadcasts will be handled for Source Routing. The choices are:

ARE broadcasts. All Routes Explorer, the default setting. Broadcasts are transmitted over every possible path on inter-connected source-routed rings. This setting maximizes the generality of the broadcast. Simply press **<Enter>** to select All Routes Explorer.

STE broadcasts. Spanning Tree Explorer. Broadcasts are transmitted only over Spanning Tree paths on inter-connected source-routed rings. This setting maximizes the efficiency of the broadcast. Enter an **s** and press **<Enter>** to select Spanning Tree Explorer.

After you enter framing type information a message displays indicating that this IPX router port was created:

Created router port for vlan 1:3

You have now completed the configuration of the virtual router port for this VLAN. You can monitor activity on this VLAN through other AutoTracker commands. See later section in this chapter for more information on these commands.

Modifying an AutoTracker VLAN

After you set up a VLAN you can modify its Admin Status, description, rules, and the Admin Status of each of the rules. You use the **modatvl** command to modify a VLAN as follows:

```
modatvl <Group Number>:<VLAN Number>
```

You must specify the Group and VLAN numbers and they must be separated by a colon. For example, to modify the VLAN 3 in Group 4, you would specify:

```
modatvl 4:3
```

After entering a valid **modatvl** command a screen similar to the sample below displays:

```
VLAN 4: 3 is defined as:
  1. Description = AT VLAN 3
  2. Admin Status = Enabled
  3. Rule Definition
      Rule Num Rule Type Rule Status
        1      Protocol Rule Disabled
Available options:
  1. Set VLAN Admin Status
  2. Set VLAN Description
  3. Add more rules
  4. Delete a rule
  5. Set rule Admin Status
  6. Quit
Option =
```

The first half of the display shows the current configuration of this VLAN. For example, this sample shows a VLAN 3 in Group 4 with a description, "AT VLAN 3." The VLAN is Enabled and a Protocol Rule has been set up, but this rule has not been enabled.

The second half of the displays a list of the VLAN attributes you can modify. You can modify basic information such as the Admin Status and Description. You can also add rules, delete rules, and enable or disable the rule. To modify an attribute, enter the number next to the option you want to modify and press **<Enter>**.

The following sections describe each of the six Available Options for the **modatvl** command.

Changing a VLAN's Admin Status

1. At the **Option=** prompt enter a **1** and press **<Enter>**.
2. The following prompt displays:

```
Set Admin Status to ((e)nable/(d)isable):
```

Type an **E** to enable the VLAN or a **D** to disable it. An enabled VLAN starts using policies to direct data flow. A disabled VLAN is saved, but cannot become active.

The system returns to the **Available Options** menu. You can modify more attributes for this VLAN, or quit modifying the VLAN by typing a **6**.

Changing a VLAN's Description

1. At the **Option=** prompt enter a **2** and press **<Enter>**.
2. The following prompt displays:

Enter a new description:

Type in the revised description for this VLAN. The description can be up to 30 characters long. Press **<Enter>** when you have completed the new description.

The system returns to the **Available Options** menu. You can modify more attributes for this VLAN, or quit modifying the VLAN by typing a **6**.

Adding More Policies for This VLAN

1. At the **Option=** prompt enter a **3** and press **<Enter>**.
2. The following menu displays:

Select rule type:

1. Port Rule
2. MAC Address Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule

Enter rule type (1):

This is the same menu used by the **cratvl** command. This menu has eight options, some of which contain multiple branching options. This menu is documented fully in Chapter 25, "Configuring Group and VLAN Policies." Please consult that chapter for information on this menu.

When you have entered all new rule types, the system returns to the **Available Options** menu. You can modify more attributes for this VLAN, or quit modifying the VLAN by typing a **6**.

Deleting A Policy for This VLAN

1. At the **Option=** prompt enter a **4** and press **<Enter>**.
2. The following menu displays:

Enter rule number to delete:

The rule number is listed with other information on the VLAN just after you entered the **modatvl** command. Find the number corresponding to the rule you want to delete and enter it at this prompt and press **<Enter>**. The rule is deleted and the system returns to the **Available Options** menu. You can modify more attributes for this VLAN, or quit modifying the VLAN by typing a **6**.

Changing the Admin Status for a VLAN Policy

1. At the **Option=** prompt enter a **5** and press **<Enter>**.
2. The following menu displays:

Enter rule number:

The rule number is listed with other information on the VLAN just after you entered the **modatvl** command. Find the number corresponding to the rule you want to change and enter it at this prompt and press **<Enter>**.

3. The following menu displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Type an **E** to enable this rule or a **D** to disable it. If the rule is enabled, the VLAN will start using the rule criteria to segment data traffic.

The system returns to the **Available Options** menu. You can modify more attributes for this VLAN, or quit modifying the VLAN by typing a **6**.

Deleting an AutoTracker VLAN

You can delete an AutoTracker VLAN. When you delete a VLAN, traffic is no longer filtered according to the VLAN's policies. Follow these steps to delete a VLAN.

1. Enter **rmatvl** followed by the Group number, a colon (:), and the VLAN number that you want to delete. For example to delete VLAN 2 in Group 3, you would enter:

rmmcvl 3:2

2. The following prompt displays:

Delete VLAN 3:2 ? (n):

Enter a **Y** and press **<Enter>** to complete the deletion of the VLAN. A message display confirming the deletion.

VLAN 3:2 deleted

Viewing AutoTracker VLANs

You can view the current status of all AutoTracker VLANs in the switch using the **atvl** command. Enter **atvl** and a table similar to the following displays.

VLAN Group :	VLAN Id	VLAN Description	Admin Status	Operational Status
3:	5	VLAN 5	Enabled	Active
3:	11	VLAN 11	Enabled	Inactive
3:	12	VLAN 12	Enabled	Inactive
3:	22	VLAN 22	Enabled	Active
3:	23	VLAN 23	Enabled	Active
3:	24	VLAN 24	Enabled	Inactive
3:	25	VLAN 25	Enabled	Inactive
3:	26	VLAN 26	Enabled	Inactive
3:	27	VLAN 27	Enabled	Inactive
3:	31	VLAN 31	Enabled	Inactive
3:	32	VLAN 32	Enabled	Inactive

VLAN Group. The Group to which this AutoTracker VLAN is assigned. The Group is specified when first creating an AutoTracker VLAN.

VLAN ID. An identification number that you assigned when you created this VLAN.

VLAN Description. A textual description that you entered to describe a VLAN when you created or modified it through **cratvl** or **modatvl**. This description is limited to 30 characters.

Admin Status. The Administrative Status for the VLAN may be enabled or disabled. You enable or disable the Administrative Status for a VLAN when you create or modify it. If the VLAN is enabled, the switch will use the policies you configured to filter traffic to the devices in this VLAN. If you disable the rule, then policies will not be used, but the parameters you set up for the VLAN will be saved.

Oper Status. The VLAN is shown as **Active** or **Inactive**. In order for an enabled VLAN to become “active” it must be able to assign a switch port to the VLAN. If the port rule is used for a VLAN, then the VLAN automatically becomes active. If any other rule is used (MAC address, protocol, etc.), then a frame matching the VLAN rule must first be received by a switch port before the VLAN is active. So, an Active VLAN requires the following:

- Admin Status must be enabled.
- A port must be assigned to the VLAN through either a port-based rule or by a device transmitting data that matches the VLAN policy.

Viewing Policy Configurations

Typing **viatrl** brings up the Policy Configuration Table, which shows the policies defined for the VLAN specified.

VLAN Group :	VLAN Id	Rule Num	Rule Type	Rule Status	Rule Definition
3:	5	1	PORT RULE	Disabled	2/7/Brg/1
3:	11	1	NET ADDR RULE	Enabled	IPX Addr = 11223344 IPX Encapsulation = Ethernet
3:	12	1	NET ADDR RULE	Enabled	DECNET Area = 13579
3:	22	1	PORT RULE	Enabled	2/7/Brg/1
3:	23	1	PORT RULE	Enabled	2/7/Brg/1
3:	24	1	MAC RULE	Enabled	082008:003002 082009:803728
3:	25	1	PROTOCOL RULE	Enabled	Protocol = IP
3:	26	1	NET ADDR RULE	Enabled	IP Addr = 131.1.2.3 IP Mask = 255.255.0.0
3:	27	1	USER RULE	Enabled	Offset = 64 Length = 2 Value = FFFF Mask = FFFF
3:	31	1	PROTOCOL RULE	Enabled	Protocol = IP
3:	32	1	NET ADDR RULE	Enabled	IPX Addr = 00000001 IPX Encapsulation = Ethernet

VLAN Group. The Group to which this AutoTracker VLAN is assigned. The Group number is specified when first creating the VLAN.

VLAN ID. An identification number that you assigned when you created this virtual LAN.

Rule Num. The number of the policy within the VLAN definition. Each rule defined for a VLAN is numbered sequentially in the order of creation. The rule number is needed when you want to modify or delete a rule definition.

Rule Type. The type of VLAN policy. The Rule Type can be a port policy (PORT RULE), MAC Address policy (MAC RULE), network address policy (NET ADDR RULE), Protocol policy (PROTOCOL RULE), or a user-defined policy (USER RULE). You set up VLAN policies when you create or modify the VLAN.

Rule Status. Indicates whether the rule for this row is Enabled or Disabled. If the rule is enabled, then the VLAN is using the rule definition to determine VLAN membership. If Disabled, then the VLAN is not using this rule to determine membership. Note that this Rule Status is different from the Admin Status for the VLAN since it controls only this specific rule within this specific VLAN. You can enable or disable the rule using the **modatvl** command.

Rule Definition. Details of this rule. For a Port Rule, this column lists the virtual interface for the Port included in the VLAN as

<slot>/<port>/<service>/<instance>

For example, the port defined for the first row in the table applies to the first bridge instance on port 7 on the module in slot 2 of the switch. For a MAC address rule, this column lists the MAC address for the device in the VLAN. For a Network Address Rule, the column will list the address (IP or IPX) and the IP Mask (IP) or the Encapsulation type (IPX). For a Protocol policy, the column list the protocol used to determine membership. And in a User-Defined rule, the offset, length, value, and mask are listed.

Viewing Virtual Ports' VLAN Membership

You can view the VLAN membership of each virtual interface in the switch. For physical LAN ports, the virtual interface is the same as a virtual port. However, when multiple services are set up for a physical port, then each service has a virtual port.

Type **vi** and a Virtual Interface Table displays similar to the one that follows. You can also specify just the slot and port number to narrow the range of ports displayed.

Virtual Interface VLAN Membership

Slot/Intf/Service/Instance	Group	Member of VLAN#
1 /1 /Rtr /1	1	1
1 /1 /Rtr /2	3	1
1 /1 /Rtr /3	3	23
1 /1 /Rtr /4	3	24
1 /1 /Rtr /5	3	25
1 /1 /Rtr /6	3	5
2 /1 /Brg /1	1	1
2 /2 /Brg /1	1	1
2 /3 /Brg /1	1	1
2 /4 /Brg /1	1	1
2 /5 /Brg /1	1	1
2 /6 /Brg /1	1	1
2 /7 /Brg /1	1	1 22
2 /8 /Brg /1	1	1
3 /1 /Brg /1	1	1
4 /1 /Brg /1	1	1
4 /2 /Brg /1	1	1
4 /3 /Brg /1	1	1
4 /4 /Brg /1	1	1
4 /5 /Brg /1	1	1
4 /6 /Brg /1	1	1
5 /1 /Brg /1	1	1

Slot/Intf/Service/Instance. Specifies the virtual interface for which AutoTracker VLAN information will be displayed. The **Slot** is the physical slot location to which the virtual interface maps. The **Intf** is the physical port to which the virtual interface maps. The **Service** is the service type for this interface. The service type may be a Router (**Rtr**), Bridge (**Brg**), Classical IP (**CIP**), FDDI Trunk (**Trk**), or an 802.10 Trunk (**T10**). **Instance** is the specific instance of this service type. These different instances are identified numerically. The first instance of a service type belonging to a physical port is identified as 1, the second instance is identified as 2, etc.

Group. The Group to which this virtual interface is assigned. The Group is specified when first creating an AutoTracker VLAN.

Member of VLAN #. The AutoTracker VLANs to which this virtual interface belongs. An interface may belong to more than one VLAN. For example, a port may contain devices using the IP Protocol and could match the Port policy of one AutoTracker VLAN and the Protocol policy of another AutoTracker VLAN. Also, physical ports always remain members of the default VLAN #1.

View VLAN Membership of MAC Devices

The **fwtlv** command displays a table of learned MAC addresses and the VLAN membership of those MAC addresses. Follow these steps to view this table.

1. Enter **fwtlv**.
2. The following prompt displays:

Enter Slot/Interface (return for all ports) :

Enter the slot and port for which you want to view MAC Address/VLAN information. You can also press **<Enter>** to view information on all ports in the switch.

3. The following message and prompt displays:

Total number of MAC addresses learned for Group 1: 4
Maximum number of entries to display [20] :

The top line displays the number of MAC addresses learned on this switch. This number indicates the potential number of entries you can display in the Learned MAC Address Table. The second line allows you to indicate how many of these MAC addresses you want to display. Enter the number of MAC entries you want to display or press **<Enter>** to select the default in brackets [20].

4. The Learned MAC Address/VLAN Membership Table displays as follows:

MAC Address	Slot/Intf/Service/Instance	AT VLAN Membership
0020DA:05F623	4/ /1 /Brg 1	1
0020DA:021533	4/ /1 /Brg 1	1
0020DA:0205B3	4/ /1 /Brg 1	1
0020DA:06BAD3	4/ /1 /Brg 1	1
0020DA:05F610	4/ /1 /Brg 1	1

MAC Address. The MAC address for which virtual interface and VLAN membership information will be displayed.

Slot/Intf/Service/Instance. Specifies the virtual port for which AutoTracker VLAN information will be displayed. The **Slot** is the physical slot location to which the MAC address maps. The **Intf** is the physical port to which the MAC address maps. The **Service** is the service type for this MAC address. The service type may be a Router (**Rtr**), Bridge (**Brg**), Classical IP (**CIP**), FDDI Trunk (**Trk**), or an 802.10 Trunk (**T10**). **Instance** is the specific instance of this service type. These different instances are identified numerically. The first instance of a service type belonging to a physical port is identified as 1, the second instance is identified as 2, etc.

AT VLAN Membership. The AutoTracker VLANs to which this MAC Address belongs. An MAC address may belong to more than one VLAN. For example, let's say a MAC device runs on an IPX network. It could be included in a MAC Address policy for one AutoTracker VLAN and the IPX Protocol Policy of another VLAN.

Creating a VLAN for Banyan Vines Traffic

Banyan Vines uses a fixed encapsulation for each network interface. For this reason, it is straightforward to create a VLAN for Banyan Vines traffic. For Ethernet traffic, Banyan Vines uses Ethernet II encapsulation; Token Ring uses LLC; FDDI uses SNAP. This procedure describes how to create a VLAN for Ethernet, Token, *and* FDDI traffic. Follow these steps to create a Banyan Vines VLAN:

1. Type **cratvl** at any prompt.

2. The following prompt displays:

Enter the VLAN Group id for this VLAN (1):

Enter the number for the Group to which this Banyan Vines VLAN will belong.

3. The following prompt displays:

Enter the VLAN Id for this VLAN (2):

Enter the number that will identify this VLAN within the Group specified above. By default the system displays the next available VLAN ID number. Press **<Enter>** to accept this default.

4. The following prompt displays:

Enter the new VLAN's description:

Enter a textual description that will help you identify the VLAN. For example, you might call the VLAN, "Banyan Vines VLAN." You may use up to 30 characters for this description.

5. The following prompt displays:

Enter the Admin Status for this vlan (Enable (e) / Disable (d)):

Enter whether or not you want the Administrative Status for this VLAN to be enabled or disabled. Once enabled, the switch begins using the policies you defined. A disabled VLAN is still defined (name, number, policies intact), but the switch keeps the VLAN disabled. The enable/disable status may be changed at a later time using the **modatvl** command.

6. The following menu displays:

Select rule type:

1. Port Rule
2. MAC Address Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP PORT Rule

Enter rule type (1):

Press **3** and press **<Enter>**.

7. The following prompt displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Type **e** to enable this rule. When enabled, the VLAN will begin using the rule to determine membership of devices.

8. The following prompt displays:

```
Select Protocol:
1. IP
2. IPX
3. DECNET
4. APPLETALK
5. Protocol specified by ether-type
6. Protocol specified by DSAP and SSAP
7. Protocol specified by SNAP
```

Enter protocol type (1):

Enter a **5** to define a protocol by ether-type and press **<Enter>**.

9. The following prompt displays:

```
Enter the Ether-type value in hex:
```

10. Enter **0bad** as the Ether-type value for Ethernet II encapsulation.

11. The following prompt displays:

```
Configure more rules for this vlan (y/n):
```

Enter a **Y**. You still need to set up rules for LLC and SNAP traffic.

12. The following prompt displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP PORT Rule
```

Enter rule type (1):

Press **3** and press **<Enter>**.

13. The following prompt displays:

```
Set Rule Admin Status to ((e)nable/(d)isable):
```

Type **e** to enable this rule.

14. The following prompt displays:

```
Select Protocol:
1. IP
2. IPX
3. DECNET
4. APPLETALK
5. Protocol specified by ether-type
6. Protocol specified by DSAP and SSAP
7. Protocol specified by SNAP
```

Enter protocol type (1):

Enter a **6** to define a protocol by DSAP and SSAP and press **<Enter>**.

15. The following prompt displays

Enter the DSAP value in hex:

Enter **bc** as the destination service access protocol (DSAP) value and press **<Enter>**.

16. The following prompt displays:

Enter the SSAP value in hex:

Again, enter **bc** as the source service access protocol (SSAP) value and press **<Enter>**.

17. The following prompt displays:

Configure more rules for this vlan (y/n):

Enter a **Y**. You still need to set up a rule for SNAP traffic.

18. The following prompt displays:

Select rule type:

1. Port Rule
2. MAC Address Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP PORT Rule

Enter rule type (1):

Press **3** and press **<Enter>**.

19. The following prompt displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Type **e** to enable this rule.

20. The following prompt displays:

Select Protocol:

1. IP
2. IPX
3. DECNET
4. APPLETALK
5. Protocol specified by ether-type
6. Protocol specified by DSAP and SSAP
7. Protocol specified by SNAP

Enter protocol type (1):

Enter a **7** to define a protocol by SNAP and press **<Enter>**.

21. The following prompt displays:

Enter the SNAP value in hex

Enter 00000080c4 as the desired SNAP value and press **<Enter>**.

22. The following prompt displays:

Configure more rules for this vlan (y/n):

Enter an **N**. You are done setting up rules for this VLAN. A prompt similar to the following displays:

VLAN 1:2 created successfully

23. The following prompt displays:

Enable IP (y):

Enter an **N**.

24. The following prompt displays:

Enable IPX (y):

Enter an **N**. The Banyan Vines traffic VLAN is complete.

28 Multicast VLANs

Multicast VLANs enable you to control the flooding of multicast traffic in your network. For example, you can define a multicast VLAN for all users that want to receive CNN Newscasts or any other video feed or combination of feeds.

You define the multicast traffic to be transmitted by specifying a multicast address. You define the recipients of the multicast traffic by specifying ports and/or specific MAC addresses. The members of a multicast VLAN consist of the ports specified to **receive** the multicast traffic and the ports to which MAC address recipients are connected. Instructions for creating multicast VLANs begin on page 28-4.

Note the difference between multicast VLANs and AutoTracker VLANs. In AutoTracker VLANs, devices are assigned to VLANs by examination of the frames that **originate** from those devices. The members of an AutoTracker VLAN consist of source devices that fit the VLAN's policies and the ports to which those source devices are connected.

There are several differences between the configuration of multicast VLANs and the configuration of AutoTracker VLANs. The following is a summary of points to note when configuring multicast VLANs:

- You can not configure routing for multicast VLANs. Multicast VLANs are independent broadcast domains for multicast traffic originating from a multicast address and transmitted to one or more recipients.
- Multicast VLANs allow three rules: Port, MAC Address, and multicast policy.
- There is not a default multicast VLAN. Therefore, you can define rules for all 32 available multicast VLANs. All ports (even those that eventually become part of a multicast VLAN) start off in the standard AutoTracker default VLAN #1, but they only get assigned to a multicast VLAN if you explicitly assign them to one.
- All multicast VLANs include the multicast policy. This policy specifies the multicast address. You use the other two rules—Port and MAC Address—to define the destination of the multicast traffic.

How Devices are Assigned to Multicast VLANs

If the recipients of the multicast traffic were defined using the port rule, each specified port is then marked as a member of the multicast VLAN.

If the recipients of the multicast traffic were defined using the MAC address rule to specify the MAC addresses of the receiving devices, no action is taken until a frame is received from one of those devices. When such a frame is received, the switch learns the device, adds its MAC address to the filtering database, and marks the port on which the frame was received as a member of the multicast VLAN. Note that the MAC address does not itself become a member of the multicast VLAN, even though it is a recipient of the multicast traffic. Only ports are members of multicast VLANs.

When the switch receive multicast traffic that has an address specified as a multicast address for the multicast VLAN, the traffic is switched to the ports defined as VLAN members.

◆ Please Take Note ◆

The source port of the multicast traffic (i.e., the port through which multicast traffic enters the switch) can be a member of any Group. The source port does *not* need to be a member of the same Group as recipient ports. Note that the source port does not become a member of the multicast VLAN.

Although some leakage may occur before devices are assigned to AutoTracker VLANs, no leakage occurs in conjunction with device assignment to multicast VLANs.

◆ Please Take Note ◆

There is no default multicast VLAN. Unless you explicitly create multicast VLANs, none will exist.

Multicast VLANs and Multicast Claiming

The goal of multicast claiming and multicast VLANs is the same—to free the MPM module from processing multicast traffic. Both methods off-load multicast traffic processing to the switching modules. However, multicast VLANs can be seen as a refinement to multicast claiming.

Multicast claiming claims the MAC addresses of all source devices sending multicast traffic and places those MAC addresses in the CAMs of all switching modules in a switch. Instead of claiming all multicast traffic, multicast VLANs claim only the traffic from the multicast address you specify. In addition, this multicast address is only placed in the CAMs of switching modules with destination ports that are part of the multicast VLAN.

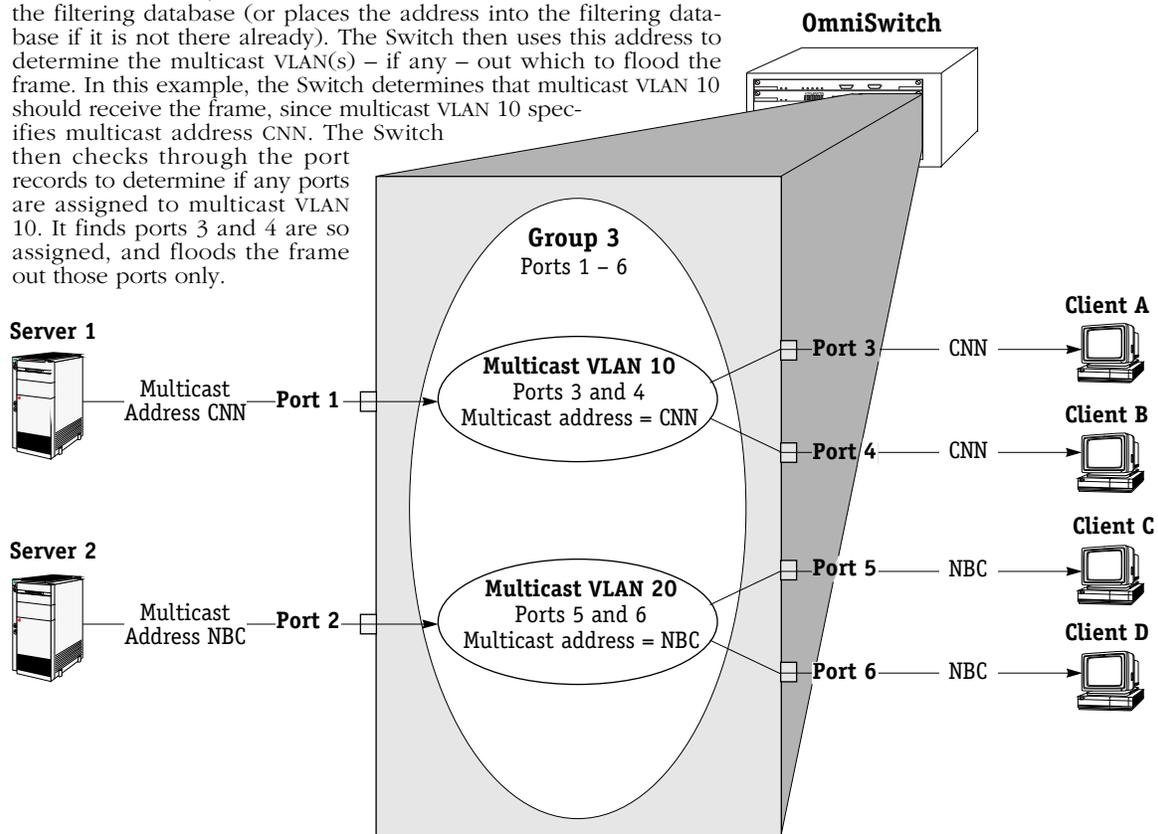
Frame Flooding in Multicast VLANs

Multicast traffic is flooded as follows in an environment that includes multicast VLANs:

- If the destination address is a multicast address, **and**
- if the destination multicast address is in the filtering database, **and**
- if the destination multicast address is a specified multicast address for a multicast VLAN, **then**

flood the traffic on all ports that have at least one multicast VLAN in common with the destination multicast address. This is illustrated below. If any of the conditions described above are untrue, the traffic is flooded as it is for normal AutoTracker VLANs.

When the Switch receives a frame with multicast destination address CNN from Server 1, the Switch locates the CNN multicast address in the filtering database (or places the address into the filtering database if it is not there already). The Switch then uses this address to determine the multicast VLAN(s) – if any – out which to flood the frame. In this example, the Switch determines that multicast VLAN 10 should receive the frame, since multicast VLAN 10 specifies multicast address CNN. The Switch then checks through the port records to determine if any ports are assigned to multicast VLAN 10. It finds ports 3 and 4 are so assigned, and floods the frame out those ports only.



For this Example, the Port Records are:

Port	VLAN Membership	MVLAN Membership
1	1	none
2	1	none
3	1	10
4	1	10
5	1	20
6	1	20

The port records show the VLAN and multicast VLAN (MVLAN) membership of each port. This table is for informational purposes only—it is not available as a UI command.

For this Example, the Filtering Database is:

MAC Address	Port	VLAN Membership	Type
CNN	n/a	10	MVLAN
NBC	n/a	20	MVLAN
Server 1	1	1	BRIDGE
Server 2	2	1	BRIDGE
Client A	3	1	BRIDGE
Client B	4	1	BRIDGE
Client C	5	1	BRIDGE
Client D	6	1	BRIDGE

The filtering database is a record of source MAC addresses, their ports of entry into the switch, and their VLAN membership. Note that the ports of entry for multicast addresses CNN and NBC are irrelevant in the filtering database. This table is for informational purposes—it is not available in the UI.

Creating Multicast VLANs

You create multicast VLANs through the AutoTracker menu options. Creating a multicast VLAN includes the following steps:

- A.** Entering basic information such as the name and number for the multicast VLAN. See *Step A. Entering Basic Information* on page 28-5 for instructions on this step.
- B.** Defining the multicast address. You define one or more multicast addresses that define the multicast stream(s) for the multicast VLAN. See *Step B. Defining the Multicast Address* on page 28-6 for instructions on this step.
- C.** Defining the recipients of multicast traffic. You may define these recipients as virtual ports or as specific MAC addresses. See *Step C. Defining the Recipients of Multicast Traffic* on page 28-7 for instructions on this step.

These steps are explained in detail below.

Step A. Entering Basic Information

1. To begin setting up a multicast VLAN type **crmcvl** at any prompt.
2. The following prompt displays:

Enter the VLAN Group id for this VLAN (1):

Enter the number for the Group to which this multicast VLAN will belong. You can create up to 32 multicast VLANs and up to 31 AutoTracker VLANs in a single Group.

3. The following prompt displays:

Enter the VLAN Id for this VLAN (5):

Enter the number that will identify this multicast VLAN within the Group specified above. Up to 32 multicast VLANs may belong to the same Group. By default the system displays the next available VLAN ID number.

◆ **Note** ◆

Unlike AutoTracker VLANs, you can configure rules for the multicast VLAN #1. There is not a default multicast VLAN, so multicast VLAN #1 is treated the same as the other 31 possible multicast VLANs.

Press **<Enter>** to accept this default.

4. The following prompt displays:

Enter the new VLAN's description:

Enter a textual description that will help you identify the multicast VLAN. For example, if you know this multicast VLAN will be composed of only workstations receiving CNN news feeds, you might call the multicast VLAN "CNN MVLAN." You may use up to 30 characters for this description.

5. The following prompt displays:

Enter the Admin Status for this vlan (Enable (e) / Disable (d)):

Enter whether or not you want the Administrative Status for this multicast VLAN to be enabled or disabled. Once enabled, the switch begins using the policies you defined. A disabled multicast VLAN is still defined (name, number, policies intact), but the switch keeps the multicast VLAN disabled. The enable/disable status may be changed at a later time using the **modmcvl** command.

◆ **Note** ◆

A multicast VLAN may not always be operational even when its Admin Status is enabled. A multicast VLAN's operation may be disabled by its switches because devices in the multicast VLAN cease transmitting data, among other reasons.

After you enter the administrative status, additional prompts display that allow you define the multicast address. See the next section, *Step B. Defining the Multicast Address* on page 28-6 for further instructions.

Step B. Defining the Multicast Address

The multicast address is an address that identifies a multicast traffic stream, such as CNN News.

◆ Please Take Note ◆

The source port of the multicast traffic (i.e., the port through which multicast traffic enters the switch) can be a member of any Group. The source port does *not* need to be a member of the same Group as recipient ports. Note that the source port does not become a member of the multicast VLAN.

1. After you enter the administrative status for this multicast VLAN, the following prompt displays:

Configure the Multicast Address Rule
Set Rule Admin Status to [(e)nable/(d)isable] (d):

Indicate whether you want to enable or disable this multicast Address Rule. If you enable this rule, AutoTracker will use the address to flood multicast traffic. Enter an **E** (enable) or a **D** (disable) and press **<Enter>**.

If you disable the rule, then this address will not be used to flood multicast traffic, but the parameters you set up will be saved. This Admin Status is different from the Admin Status for the multicast VLAN as it controls only this specific rule within this specific multicast VLAN. You can enable or disable the rule at a later time using the **modmctl** command.

2. The following prompt displays:

Enter the Multicast addresses (AABBCC:DDEEFF) in Canonical format
(Enter save to end):

Enter one or more multicast addresses, separated by spaces. The address must be a multicast address. If you enter too many characters, the system truncates the address. The switch will flood all traffic from the address(es) you specify here to the ports and/or MAC addresses you define as recipients in Step C.

All multicast MAC addresses must consist of 12 hex digits. In all valid multicast addresses, the least significant bit of the most significant byte is set to 1. Addresses with this bit unset will be rejected.

Most Significant Byte

x x x x x x x 1



least significant bit
must be set to 1

Structure of Multicast Address

When you have entered the final MAC address press **<Enter>**, and type **save** at the prompt.

Next, a menu displays prompting you to select the rules governing membership in this multicast VLAN. Go on to the next section, *Step C. Defining the Recipients of Multicast Traffic* on page 28-7 to continue setting up this multicast VLAN.

Step C. Defining the Recipients of Multicast Traffic

You can define the recipients of multicast traffic by virtual port or MAC address. You define these recipients as policies for this multicast VLAN. The available policies for recipients are Port and MAC Address. You can use both rules within a single multicast VLAN. For example, you might want to flood multicast traffic to all devices attached to one switch port, but only a few devices attached to other switch ports. In this case, you could use a Port rule for the devices on the port where all devices receive the multicast traffic, and then the MAC address rule to flood multicast traffic only to specific devices attached to the other ports on the switch.

Follow the directions in one of the following sections for the rule type you want to define.

Defining Recipients By Port

After you define the multicast address, the following menu displays:

```

Select rule type:
1. Port Rule
2. MAC Address Rule
3. Multicast Address Rule

```

```
Enter rule type (1):
```

1. Press **<Return>**.
2. The following prompt displays:

```
Set Rule Admin Status to ((e)nable/(d)isable):
```

Indicate whether or not you want to enable this rule. Type **e** to enable or **d** to disable. If you enable the rule, the multicast VLAN will use it to determine membership of devices. If you disable the rule, then this rule will not be used in assigning devices to this multicast VLAN, but the parameters you set up for the multicast VLAN will be saved. This Admin Status is different from the Admin Status for the multicast VLAN as it controls only this specific rule within this specific multicast VLAN. You can enable or disable the rule at a later time using the **modmctl** command.

3. The following prompt displays:

```
Enter the list of port in Slot/Int/Service/Instance format:
```

Enter the ports that you want to receive multicast traffic for this multicast VLAN. You may enter multiple ports at a time. You can include a total of 255 ports per switch in a port-based multicast VLAN. Use the **<slot>/<port>** format. For example, to include port 7 from the module in slot 2, you would enter **2/7**. (The service and instance numbers are not necessary for specifying physical ports. They are only necessary when specifying logical or virtual ports, which normally only differ from physical ports in more complex configurations, such as ATM LAN Emulation.)

4. The following prompt displays:

```
Configure more rules for this vlan (y/n):
```

You can set up multiple rules for the same multicast VLAN. Enter a **Y** here if you want to set up more rules in addition to the port rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up on this multicast VLAN. If you enter **N**, you will receive a message, similar to the one below, indicating that the multicast VLAN was set up.

```
VLAN 3:23 created successfully
```

5. If you are done setting up rules for this multicast VLAN, then your multicast VLAN is set up. You can monitor activity on these multicast VLANs through other AutoTracker commands. See later sections in this chapter for information on these commands.

Defining Recipients By MAC Address

After you define the multicast address, the following menu displays:

Select rule type:

- 1. Port Rule**
- 2. MAC Address Rule**
- 3. Multicast Address Rule**

Enter rule type (1):

1. Press **2** and **<Return>**.
2. The following prompt displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Indicate whether or not you want to enable this rule. Type **e** to enable or **d** to disable. If you enable the rule, the multicast VLAN will use it to determine membership of devices. If you disable the rule, then this rule will not be used in assigning devices to this multicast VLAN, but the parameters you set up for the multicast VLAN will be saved. This Admin Status is different from the Admin Status for the multicast VLAN as it controls only this specific rule within this specific multicast VLAN. You can enable or disable the rule at a later time using the **modmctl** command.

3. The following prompt displays:

Enter the list of MAC addresses (Enter save to end):

Enter the MAC addresses that you want to receive multicast traffic for this multicast VLAN. Separate addresses by a space. When you have entered the final MAC address, leave a space and type **save**.

4. The following prompt will display:

Configure more rules for this vlan (y/n):

You can set up multiple rules for the same multicast VLAN. Enter a **Y** here if you want to set up more rules in addition to the port rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up on this multicast VLAN. If you enter **N**, you will receive a message, similar to the one below, indicating that the multicast VLAN was set up.

VLAN 3:24 created successfully

5. If you are done setting up rules for this multicast VLAN, then your multicast VLAN is set up. You can monitor activity on these multicast VLANs through other AutoTracker commands. See later sections in this chapter for information on these commands.

Modifying Multicast VLANs

After you set up a multicast VLAN you can modify its Admin Status, description, rules, and the Admin Status of each of the rules. You use the **modmctl** command to modify a multicast VLAN as follows:

modmctl <Group Number>:<VLAN Number>

You must specify the Group and multicast VLAN number and they must be separated by a colon. For example, to modify multicast VLAN 2 in Group 2, you would specify:

modmctl 2:2

After entering a valid **modmctl** command, a screen similar to the following sample displays:

```

VLAN  2: 2 is defined as:
  1.   Description    = MVLAN 2
  2.   Admin Status  = Enabled
  3.   Rule Definition
      Rule Num  Rule Type    Rule Status
        1      Port Rule    Enabled
        2      Multicast Rule Enabled
Available options:
  1.   Set VLAN Admin Status
  2.   Set VLAN Description
  3.   Add more rules
  4.   Delete a rule
  5.   Set rule Admin Status
  6.   Quit
Option =
    
```

The first half of the display shows the current configuration of this multicast VLAN. For example, this sample shows multicast VLAN 2 in Group 2 with a description, “MVLAN 2.” The multicast VLAN is Enabled and a Port Rule has been set up and it is enabled.

The second half of the display shows a list of the multicast VLAN attributes you can modify. You can modify basic information such as the Admin Status and Description. You can also add rules, delete rules, and enable or disable a rule. To modify an attribute, enter the number next to the option you want to modify and press **<Enter>**.

The following sections describe each of the six Available Options for the **modmctl** command.

Changing a VLAN’s Admin Status

1. At the **Option=** prompt enter a **1** and press **<Enter>**.
2. The following prompt displays:

Set Admin Status to ((e)nable/(d)isable):

Type an **e** to enable the multicast VLAN or a **d** to disable it. An enabled VLAN starts using policies to direct data flow. A disabled multicast VLAN is saved, but can not become active.

The system returns to the **Available Options** menu. You can modify more attributes for this multicast VLAN, or quit modifying the multicast VLAN by typing a **6**.

Changing a VLAN's Description

1. At the **Option=** prompt enter a **2** and press **<Enter>**.
2. The following prompt displays:

Enter a new description:

Type in the revised description for this multicast VLAN. The description can be up to 30 characters long. Press **<Enter>** when you have completed the new description.

The system returns to the **Available Options** menu. You can modify more attributes for this multicast VLAN, or quit modifying the multicast VLAN by typing an **6**.

Adding More Policies for This VLAN

1. At the **Option=** prompt enter a **3** and press **<Enter>**.
2. The following menu displays:

Select rule type:

1. **Port Rule**
2. **MAC Address Rule**
3. **Multicast Address Rule**

Enter rule type (1):

This is the same menu used by the **crmcvl** command. This menu has three options, some of which contain multiple branching options. This menu is documented fully in the section, *Step C. Defining the Recipients of Multicast Traffic* on page 28-7. Please consult this section for information on this menu.

When have entered all new rule types, the system returns to the **Available Options** menu. You can modify more attributes for this multicast VLAN, or quit modifying the multicast VLAN by typing an **6**.

Deleting A Policy for This VLAN

1. At the **Option=** prompt enter a **4** and press **<Enter>**.
2. The following menu displays:

Enter rule number to delete:

The rule number is listed with other information on the multicast VLAN just after you entered the **modmctl** command. Find the number corresponding to the rule you want to delete and enter it at this prompt and press **<Enter>**. The rule is deleted and the system returns to the **Available Options** menu. You can modify more attributes for this multicast VLAN, or quit modifying the multicast VLAN by typing a **6**.

Changing the Admin Status for a VLAN Policy

1. At the **Option=** prompt enter a **5** and press **<Enter>**.
2. The following menu displays:

Enter rule number:

The rule number is listed with other information on the multicast VLAN just after you entered the **modmctl** command. Find the number corresponding to the rule you want to change and enter it at this prompt and press **<Enter>**.

3. The following menu displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Type an **e** to enable this rule or a **d** to disable it. If the rule is enabled, the multicast VLAN will start using the rule criteria to segment data traffic.

The system returns to the **Available Options** menu. You can modify more attributes for this multicast VLAN, or quit modifying the multicast VLAN by typing a **6**.

Deleting a Multicast VLAN

You can delete a multicast VLAN. When you delete a multicast VLAN, multicast traffic is no longer flooded to the recipients you defined. Follow these steps to delete a multicast VLAN.

1. Type **rmmctl** followed by the Group number, a colon (:), and the multicast VLAN number that you want to delete. For example to delete multicast VLAN 2 in Group 3, you would type:

rmmctl 3:2

2. The following prompt displays:

Delete VLAN 3:2 ? (n):

Enter a **y** and press **<Enter>** to complete the deletion of the multicast VLAN. A message display confirming the deletion.

VLAN 3:2 deleted

Modifying a Multicast Address Policy

After you create a multicast VLAN, you can modify the multicast address policy by adding more addresses through the **modmctl** command. However, you can not add an existing multicast address. Follow the steps outlined in *Modifying Multicast VLANs* on page 28-9 and the steps for *Adding More Policies for This VLAN* on page 28-10. Continue with the procedure below.

The following menu displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
3. Multicast Address Rule
```

```
Enter rule type (1):
```

1. Press **3** and **<Return>**.
2. The following prompt displays:

```
Set Rule Admin Status to ((e)nable/(d)isable):
```

Indicate whether or not you want to enable this rule. Type **e** to enable or **d** to disable. If you disable the rule, then the multicast addresses you enter will not be used to flood traffic, but the parameters you set up for the multicast VLAN will be saved. This Admin Status is different from the Admin Status for the multicast VLAN as it controls only this specific rule. You can enable or disable the rule at a later time using the **modmctl** command.

3. The following prompt displays:

```
Enter the list of MAC addresses (Enter save to end):
```

Enter one or more multicast addresses. Separate addresses by a space. When you have entered the final multicast address, leave a space and type **save**.

4. The following prompt will display:

```
Configure more rules for this vlan (y/n):
```

You can set up multiple rules for the same multicast VLAN. Enter a **Y** here if you want to set up more rules in addition to the multicast address rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up on this multicast VLAN. If you enter **N**, you will receive a message, similar to the one below, indicating that the multicast VLAN was set up.

```
VLAN 3:24 created successfully
```

Viewing Multicast VLANs

You can view the current status of all multicast VLANs in the switch using the **mcvl** command. Type **mcvl** and a table similar to the following displays:

VLAN Group :	VLAN Id	VLAN Description	Admin Status	Operational Status
3:	5	MVLAN 5	Enabled	Active
3:	11	MVLAN 11	Enabled	Inactive
3:	12	MVLAN 12	Enabled	Inactive
3:	22	MVLAN 22	Enabled	Active
3:	23	MVLAN 23	Enabled	Active
3:	24	MVLAN 24	Enabled	Inactive
3:	25	MVLAN 25	Enabled	Inactive
3:	26	MVLAN 26	Enabled	Inactive
3:	27	MVLAN 27	Enabled	Inactive
3:	31	MVLAN 31	Enabled	Inactive
3:	32	MVLAN 32	Enabled	Inactive

VLAN Group. The Group to which this multicast VLAN is assigned. The Group is specified when first creating a multicast VLAN.

VLAN ID. An identification number that you assigned when you created this multicast VLAN.

VLAN Description. A textual description that you entered to describe a multicast VLAN when you created or modified it through **crmcvl** or **modmcvl**. This description is limited to 30 characters.

Admin Status. A multicast VLAN can be enabled or disabled. You enable or disable a multicast VLAN when you create or modify it. If the multicast VLAN is enabled, AutoTracker floods multicast traffic to the recipients you specified when setting up the multicast VLAN. If the multicast VLAN is disabled, the multicast traffic is not flooded as you specified; however, the parameters you set up for the multicast VLAN are saved.

Oper Status. The multicast VLAN is shown as active or inactive. In order for an enabled multicast VLAN to become “active” it must be able to assign a switch port to the multicast VLAN. If the port rule is used for a multicast VLAN, then the multicast VLAN automatically becomes active. If you defined multicast traffic recipients by MAC address only, then a frame destined for a defined MAC address must first be received by a switch port before the multicast VLAN is active. An active multicast VLAN requires the following:

- Admin Status must be enabled.
- A port must be assigned to the multicast VLAN through either a port-based rule or by a device transmitting data that matches the multicast VLAN policy.

Viewing Multicast VLAN Policies

You can view the current multicast VLAN policies and their status using the **vimcrl** command. Type **vimcrl** and a Policy Configuration Table displays similar to the following:

VLAN Group :	VLAN Id	Rule Num	Rule Type	Rule Status	Rule Definition
3:	5	1	PORT RULE	Disabled	2/7/Brg/1
3:	5	2	MCAST	Disabled	072467:0034ab
3:	22	1	PORT RULE	Enabled	2/7/Brg/1
3:	22	2	MCAST	Enabled	080027:0135de1
3:	23	1	PORT RULE	Enabled	2/7/Brg/1
3:	23	2	MCAST	Enabled	050034:000017
3:	24	1	MAC RULE	Enabled	082008:003002 082009:803728
3:	24	2	MCAST	Enabled	053967:0126af5

VLAN Group. The Group to which this multicast VLAN is assigned. The Group is specified when first creating a multicast VLAN.

VLAN ID. An identification number that you assigned when you created this multicast VLAN.

Rule Num. The number for this rule within the multicast VLAN definition. Each rule defined for a multicast VLAN is numbered sequentially in the order of creation. The rule number is needed when you want to modify or delete a rule definition.

Rule Type. The type of multicast VLAN rule. For multicast VLANs, the rule type can be PORT RULE, MAC RULE, or MULICAST RULE. Each multicast VLAN by definition will contain a multicast rule. The multicast rule defines the multicast address. In addition, the multicast VLAN contains either a Port-based rule, MAC address rule, or both a Port and MAC address rule. The Port and MAC address rules define the recipients of multicast traffic.

Rule Status. Indicates whether the rule for this row is Enabled or Disabled. If the rule is enabled, then the switch is using the rule definition to determine multicast traffic flooding. If Disabled, then the switch is not using this rule to regulate multicast traffic flow. Note that this Rule Status is different from the Admin Status for the multicast VLAN since it controls only this specific rule within this specific multicast VLAN. You can enable or disable the rule using the **modmctl** command.

Rule Definition. Details of this rule. For a Port Rule, this column lists the virtual interface for the Port that is a recipient of the multicast traffic as

```
<slot>/<port>/<service>/<instance>
```

For example, the port defined for the first row in the table applies to the first bridge instance on port 7 on the module in slot 2 of the switch. For a MAC address rule, this column lists the MAC address for the recipient of the multicast traffic. For a multicast Rule, this column lists the multicast address.

Viewing the Virtual Interface of Multicast VLANs

You can view the multicast VLAN membership of each virtual interface in the switch. In most cases the virtual interface is the same as a virtual port. However, when multiple services are set up for a virtual port, then each service may be split into one or more instances.

Type **vimcvi** and a Virtual Interface Table displays similar to the one that follows. You can also specify just the slot and port number to narrow the range of ports displayed.

Virtual Interface VLAN Membership

Slot/Intf/Service/Instance				Group	Member of VLAN#
1	/1	/Rtr	/1	1	1
1	/1	/Rtr	/2	3	23
1	/1	/Rtr	/3	3	24
2	/1	/Brg	/1	1	23
2	/7	/Brg	/1	1	22
4	/1	/Brg	/1	1	24
5	/1	/Brg	/1	1	22

Slot/Intf/Service/Instance. Specifies the virtual interface for which multicast VLAN information will be displayed. The **Slot** is the physical slot location to which the virtual interface maps. The **Intf** is the physical port to which the virtual interface maps. The **Service** is the service type for this interface. The service type may be a Router (**Rtr**), Bridge (**Brg**), Classical IP (**CIP**), FDDI Trunk (**Trk**), or an 802.10 Trunk (**T10**). **Instance** is the specific instance of this service type. These different instances are identified numerically. The first instance of a service type belonging to a physical port is identified as 1, the second instance is identified as 2, etc.

Group. The Group to which this virtual interface is assigned. The Group is specified when first creating a multicast VLAN.

Member of VLAN #. The multicast VLANs to which this virtual interface belongs. An interface may belong to more than one multicast VLAN. For example, if you set up a multicast VLAN for CNN News and another for NBC News, you may want certain ports to receive both multicast traffic streams.

29 AutoTracker VLAN Application Examples

This chapter provides specific examples of AutoTracker VLANs in various network configurations. These examples illustrate basic concepts about AutoTracker and highlight issues that can arise when AutoTracker is used in different network situations.

- *Application Example 1* illustrates a network organized according to logical policies and explains the benefits of a logical network organization.
- *Application Example 2* explains unique characteristics of IPX networks that must be considered when using AutoTracker IPX network address VLANs.
- *Application Example 3* highlights an issue concerning translated frames and AutoTracker IPX network address VLANs.
- *Application Example 4* explains how routing works generally in IPX networks and explains how to avoid an exception condition in which AutoTracker can affect the behavior of an IPX-routed network.
- *Application Example 5* explains why a port-based policy may be required for a VLAN – in addition to any other policies defined for that VLAN – to establish communications in some network situations, such as traversing a backbone.

Application Example 1

VLANs Based on Logical Policies

Example 1 shows a network organized logically. The network is organized according to IP networks, but this organization is achieved through the application of logical policies rather than physical segmentation. The use of logical policies provides the flexibility of moving IP users from segment to segment and preserving their original VLAN membership – without reconfiguring AutoTracker or the workstations.

Group and VLAN Membership

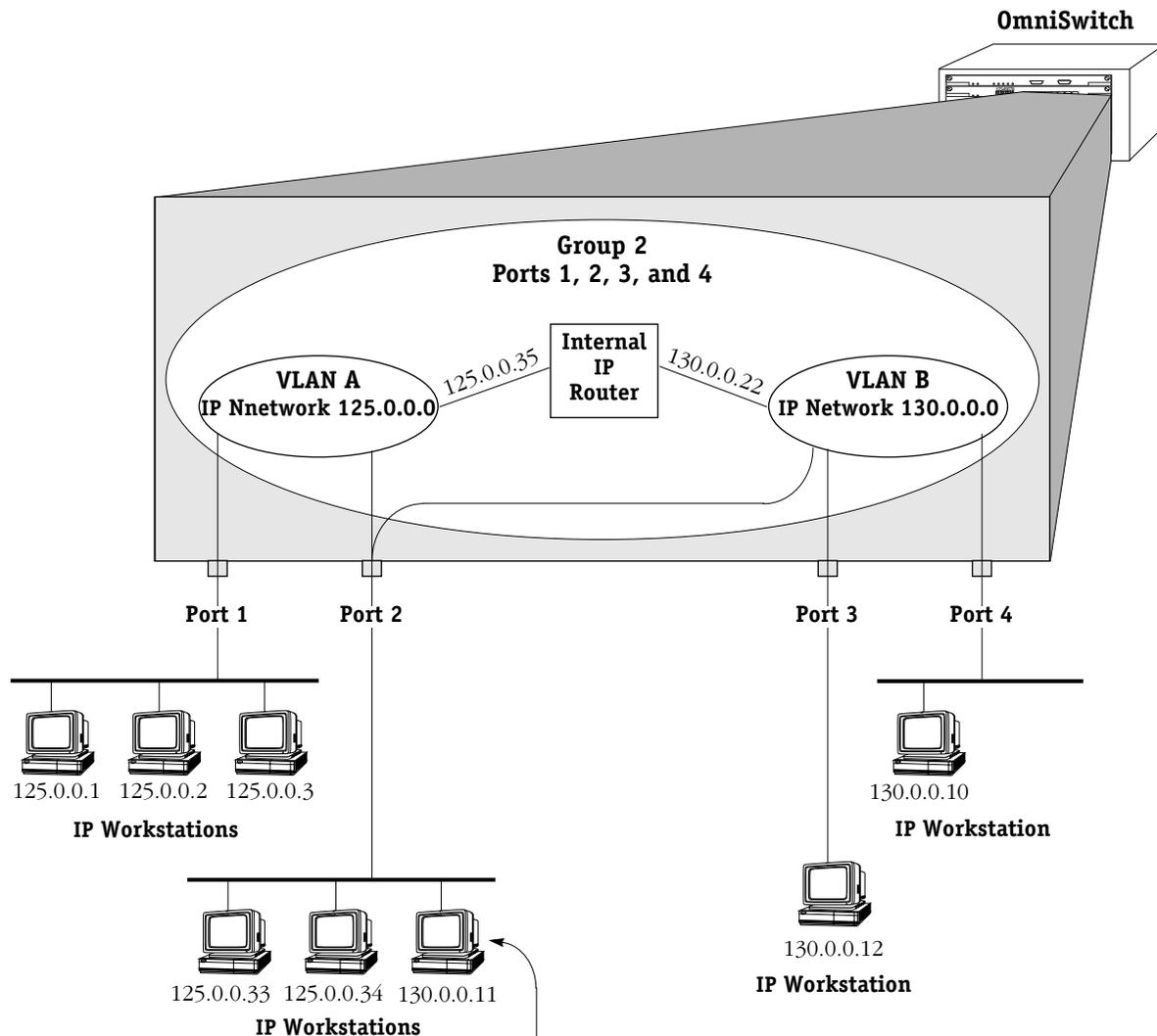
The network shown in Example 1 contains one Group – Group 2 – that consists of ports 1, 2, 3, and 4. Note that a Group defines a physical area – a set of ports – within the network. When VLANs with logical policies are created within a Group, the logical policies are applied to traffic received from all ports within the Group – but not to traffic from ports outside the Group – to determine if any source device should be a VLAN member.

As shown on the facing page, two VLANs were created within Group 2, each with a logically-based Network Address policy. The Network Address policy for VLAN A defines IP network 125.0.0.0 and the Network Address policy for VLAN B defines IP network 130.0.0.0. All traffic received on ports 1, 2, 3, and 4 will be checked for possible membership in these two VLANs.

Routing was enabled on both VLAN A and VLAN B so that traffic can move between the two VLANs, as is shown in this example by the presence of the internal IP router.

Benefits

This network configuration shown in this example provides flexibility. As explained on the following page, this logical network organization enables the Network Manager to move IP users between segments while preserving their original VLAN membership – without reconfiguring AutoTracker or the workstations.



Workstation 130.0.0.11 has been moved from the segment connected to port 4 to the segment connected to port 2. When workstation 130.0.0.11 transmits its first frame from its new location, the switch automatically places it into its original VLAN, VLAN B, because VLAN B has a network address rule that places all devices with network address 130.0.0.0 into VLAN B.

Both VLAN A and VLAN B are now active on port 2. In addition, VLAN B is now active on multiple ports – ports 2, 3, and 4. However, this does not cause confusion.

As an example, if workstation 125.0.0.1 (in VLAN A) wants to talk to workstation 130.0.0.11 (in VLAN B), workstation 125.0.0.1 ARPs for workstation 130.0.0.11's MAC address. The address returned is that of workstation 125.0.0.1's default gateway, which is VLAN A's internal IP router, 125.0.0.35. Workstation 125.0.0.1 transmits its frame to this address and the internal IP router routes the frame to VLAN B.

When VLAN B's internal IP router receives the frame addressed to workstation 130.0.0.11, it ARPs for workstation 130.0.0.11's MAC address if it does not already know it. The switch's filtering database identifies the port through which this MAC address can be reached. The frame sent by workstation 125.0.0.1 to workstation 130.0.0.11 is correctly transmitted to port 2.

Application Example 2

VLANs in IPX Networks

Example 2 illustrates the use of AutoTracker VLANs in IPX networks – specifically, VLANs based on IPX network address rules. IPX networks have unique characteristics that must be considered when configuring VLANs based on network address rules.

Encapsulation Type in IPX Networks

The encapsulation type a MAC station uses is very important in IPX networks, because a close relationship exists between encapsulation type and IPX network number. In IPX networks, a network number and an encapsulation type are configured for each segment. When two IPX servers share the same LAN segment, they must have the same network number and the same encapsulation type in order to communicate. In addition, only clients and servers that use the same encapsulation type can communicate. (The OmniSwitch removes this restriction somewhat through MAC-layer translations, which will not be discussed at this time.)

In summary, network number and encapsulation type define a broadcast domain in an IPX network that is analogous to a LAN – or a VLAN. (Remember that VLANs have the same characteristics as LANs, with the exception that VLANs can span multiple segments as LANs cannot.)

An encapsulation type is configured within each IPX client prior to bootup on the network. An IPX client acquires its network number dynamically from an IPX server (or from an intervening router) using a “Get_Nearest_Server” mechanism. Upon bootup, each client sends a query seeking the nearest server that uses the same encapsulation type as the client. Only those servers using the same encapsulation type respond to the query. (An intervening router can also respond to the query: routers traditionally interconnect LAN segments and can use different encapsulation types for different networks.) This means that IPX clients do not know their network numbers at bootup, but rather acquire their network numbers after they have communicated with IPX servers or with an intervening router.

VLAN Assignment in IPX Networks

The close relationship between encapsulation type and network number in IPX networks is the main reason AutoTracker’s IPX network address policy requires you to specify both a network number and an encapsulation type. The OmniSwitch assigns devices to IPX network address VLANs as follows:

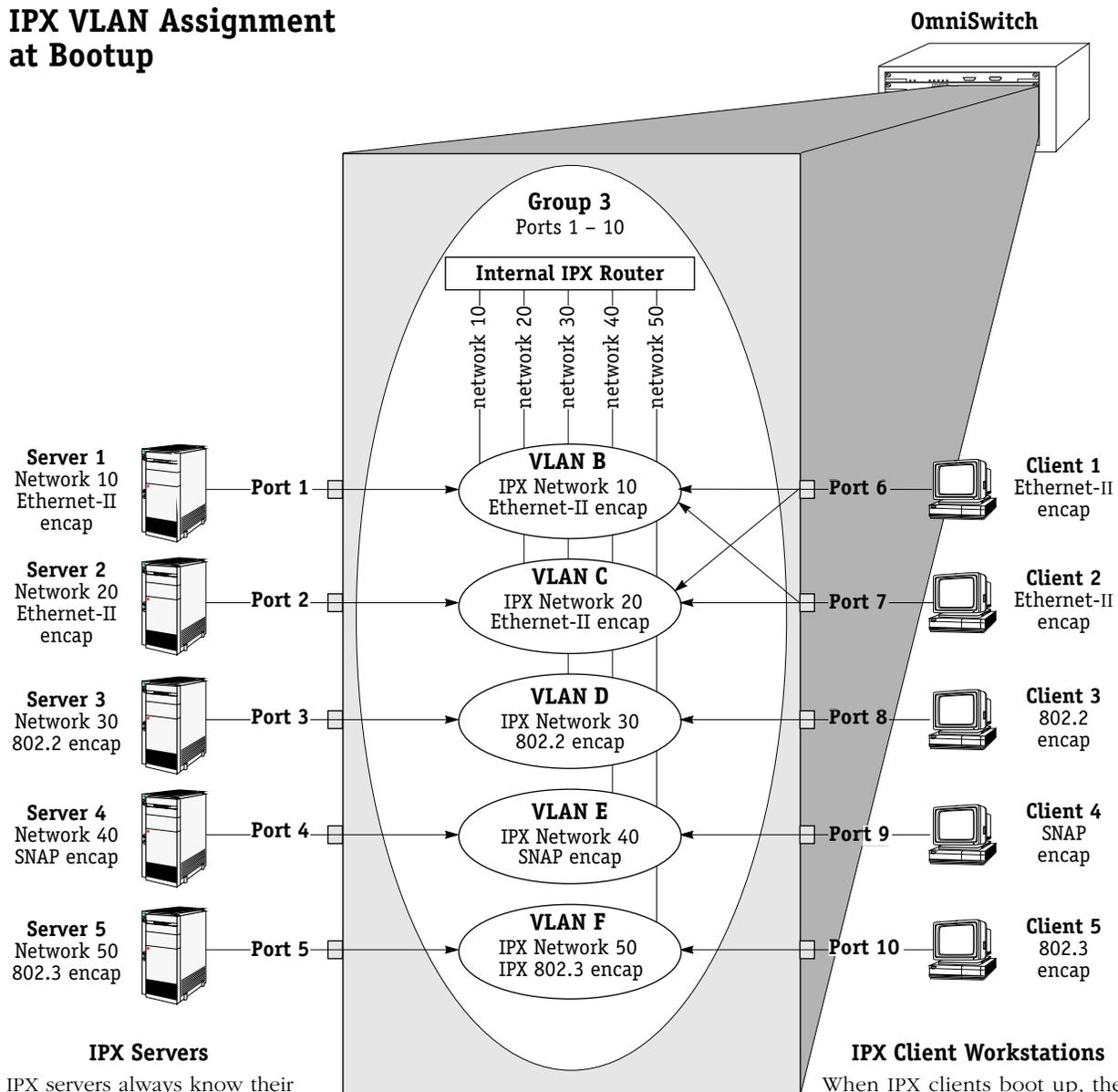
- **IPX servers.** Frames from an IPX server always contain information on the server’s network number, so the OmniSwitch can always assign IPX servers to the correct VLAN based on the server’s network number.
- **IPX clients.** As explained previously, IPX clients do not know their network number at bootup and so cannot, initially, be assigned to VLANs based on their network number. For this reason the OmniSwitch initially assigns clients to IPX network address VLANs based on their encapsulation type. An example of this is shown on the facing page. Once an IPX client communicates with a server or an intervening router, learns its network number and begins transmitting frames with that number, it is removed from all previously-assigned IPX network address VLANs (but not from VLANs of other policy types) and placed into the correct IPX network address VLAN according to network number.

So How Do I Avoid Conflicts?

As an example, IPX defines four different types of Ethernet encapsulation: Ethernet-II, 802.2, SNAP, and IPX 802.3 (also referred to as “raw”). So, what do you do to avoid conflicts when you have more than four servers and they use different encapsulation types? The solution is to put each server into a different VLAN, as shown in the example on the facing page.

continued ...

IPX VLAN Assignment at Bootup



IPX servers always know their network number, so IPX servers are assigned to VLANs according to network number.

When IPX clients boot up, their encapsulation types are known but their network numbers are not. Therefore, IPX clients are initially assigned to VLANs according to encapsulation type. This is the reason Clients 1 and 2 (which use Ethernet-II encapsulation) are assigned to VLANs B and C (which both specify Ethernet-II encapsulation).

Once an IPX client communicates with a server or an intervening router, learns its network number and begins transmitting frames with that number, it is removed from all previously-assigned IPX VLANs and placed into a single IPX VLAN according to network number. Client 1 and Client 2 will be reassigned to either VLAN B or VLAN C when their respective network numbers are known.

IPX Client	VLAN Membership
Client 1	both B & C initially, then either B or C when network number is known
Client 2	both B & C initially, then either B or C when network number is known
Client 3	D
Client 4	E
Client 5	F
Please note that all ports in Group 3 are also members of ports 3's default VLAN #1.	

Application Example 2

In this example one Group was created – Group 3 – that includes all ports to which IPX servers and clients are connected. Within this Group five VLANs were created, one for each server:



When the OmniSwitch receives frames from the five servers, each server is assigned to the appropriate VLAN and no conflict occurs. IPX routing is enabled for each VLAN – with appropriate framing specified – so that traffic can route between the VLANs.

When a client workstation boots up and queries for a server, the OmniSwitch assigns the client to the appropriate VLAN(s) based on encapsulation type. If the client uses 802.2 encapsulation, SNAP encapsulation, or IPX 802.3 encapsulation, VLAN assignment is simple: the client is assigned to VLAN D (802.2 encapsulation), VLAN E (SNAP encapsulation), or VLAN F (IPX 802.3 encapsulation), respectively.

However, when a client workstation using Ethernet-II encapsulation boots up and queries for a server, the OmniSwitch initially assigns the client to both VLAN B and VLAN C, since both of these VLANs specify Ethernet-II encapsulation. However, the OmniSwitch recognizes that the client's frame is a "Get_Nearest_Server" query and remembers that the client is in search of its network number. While the client remains in this transitional state, it remains assigned to all VLANs that specify Ethernet-II encapsulation. Once the client has received response from a server or servers or from an intervening router, the client selects its network number and begins transmitting frames with the network number embedded. The OmniSwitch detects these frames, removes the client from all previously-assigned IPX network address VLANs (but not from VLANs of other policy types) and assigns it to the proper IPX network address VLAN according to network number.

Please Take Note

IPX clients often are not particular about the server to which they attach. However, clients can select a preferred server if the **/PS** (preferred server name) option is included in their start-up script.

Why is this Solution Recommended?

As as been explained, isolating each IPX server in its own IPX network address VLAN is the recommended way to avoid conflicts. No problems occur if a client receives broadcast and multicast traffic from multiple servers, especially for the brief period that the client remains in a transitional state in search of a server.

Problems do occur if two servers with different network numbers and the same encapsulation type are members of the same VLAN, because each server will detect the other's frames, notice conflicting network numbers for the same VLAN, and respond with a router configuration error. For this reason it is not advisable to create four VLANs based on IPX network address policies within the same Group, each configured for one of the four encapsulation types. It is important to isolate the servers, but it is not important to isolate the clients – at least immediately.

While it is not important to isolate IPX clients immediately at bootup, it is desirable to isolate them as soon as possible. Isolating clients – rather than letting them remain in multiple VLANs that specify the same encapsulation type – increases efficiency and reduces broadcast and multicast traffic in the network. If a client remains in multiple VLANs that specify the same encapsulation type, the client receives all broadcast and multicast traffic from each server using that encapsulation type, even though the client only communicates with the server that shares its network number. In addition, when a VLAN is extended across a WAN backbone, it is wasteful and inefficient to transmit unnecessary frames across the WAN. For these reasons, as soon as a client learns its network number and begins transmitting frames with that number, the OmniSwitch removes the client from all previously-assigned IPX network address VLANs and assigns it to a single IPX VLAN according to network number.

Application Example 3

IPX Network Address VLANs and Translated Frames

Application Example 3 shows two IPX networks connected over a bridged FDDI ring spanning two OmniSwitches. VLAN B exists in both switches and specifies an IPX network address policy of network number 100 and Ethernet-II encapsulation.

The Problem

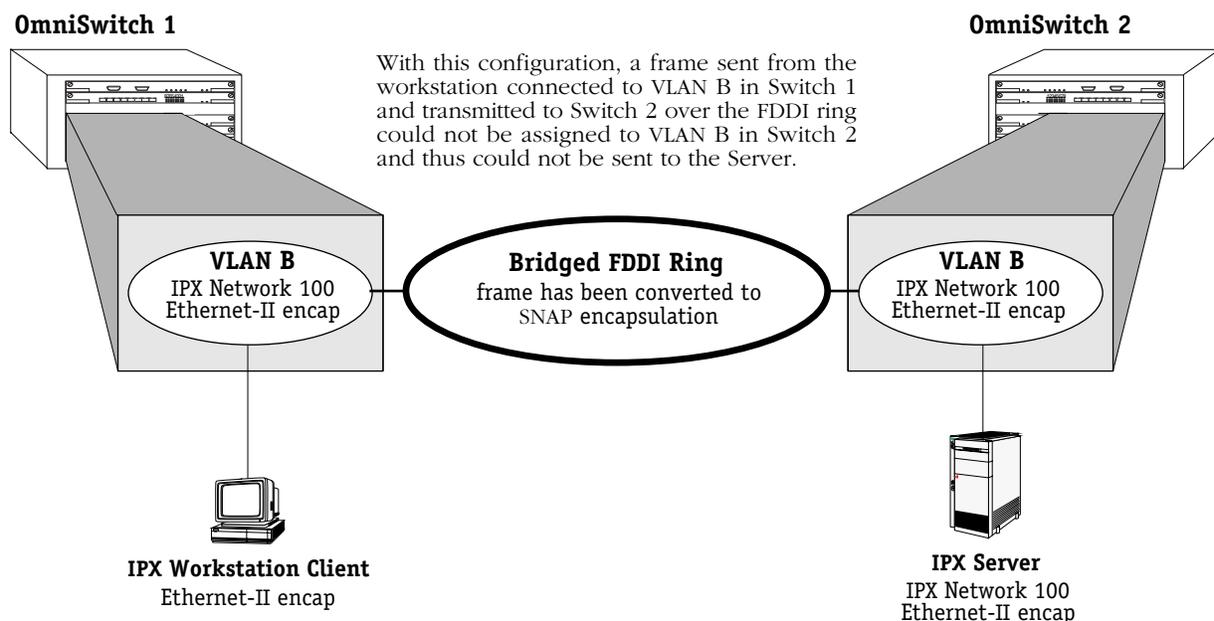
In the figure below, when the IPX client connected to Switch 1 boots up and sends a frame seeking a server, Switch 1 assigns the frame to VLAN B (since VLAN B specifies Ethernet-II encapsulation) and then converts the frame to SNAP encapsulation so that the frame can traverse the FDDI ring. When the frame arrives at Switch 2, the network number is not available (since, as previously explained, IPX clients do not know their network number at bootup) and the frame's encapsulation is no longer Ethernet-II – it is now SNAP. Because the IPX network address policy selects VLAN members according to network number and encapsulation, Switch 2 cannot assign the frame to VLAN B and send it to the IPX server.

The Solution

The solution for this problem is to specify a second encapsulation type for VLAN B in addition to Ethernet-II – for example, SNAP encapsulation. If VLAN B specifies Ethernet-II or SNAP encapsulation, the frame will match the network address policy for VLAN B when it arrives at Switch 2 and can thus be assigned to VLAN B and sent to the server. Note that the second encapsulation type must be specified for VLAN B in both Switches, to accommodate data transmission in either direction.

Please Take Note

This situation can occur whenever translations occur, such as with bridged FDDI rings or Token Rings. If you are using FDDI trunking you do not need to specify a second encapsulation policy for IPX network address VLANs, because trunked frames are not translated.



Application Example 4

Routing in IPX Networks

How Routing Works Generally

AutoTracker “activates” a VLAN – and its internal router interface – when the first port is assigned to the VLAN. If a VLAN has a port policy, AutoTracker assigns the specified port(s) and activates the VLAN immediately. If a VLAN has a logical policy, AutoTracker assigns the first port to the VLAN when a frame is received from a source device that matches the VLAN’s policy. When such a frame is received, the source device – and the port to which that device is connected – are assigned to the VLAN and the VLAN is activated.

Until a port is assigned to a VLAN, that VLAN is maintained in an inactive state and its internal router port is inactive – even if routing was enabled by the user. Use of a VLAN’s routing service is “on-demand” and AutoTracker does not enable routing until a port is present that might require it. When AutoTracker assigns the first port to a particular VLAN, it activates that VLAN and its routing service (as long as routing was enabled by the user).

Once AutoTracker has established devices’ VLAN assignments and activated the appropriate VLAN routing services, it does not participate in the routing process. Routing works correctly as long as the policies of the IPX protocol were followed – with the exception below.

The Exception

There is one scenario in which AutoTracker affects the behavior of an IPX-routed network. This situation occurs when an IPX server is a member of any VLAN with IPX network address policies **and** IPX routing is enabled on the Group’s default VLAN #1. An exception condition arises in this situation because all ports in a Group are always members of that Group’s default VLAN #1 in addition to any other VLANs of which they are members. As a result, default VLAN #1 is always active.

The figure on the facing page illustrates this problem situation. In this figure, three VLANs within Group 2 – one of which is default VLAN #1 – have IPX routing enabled, as indicated by the presence of the internal IPX router. VLANs 2 and 3 both have IPX network address policies. When IPX Server A is connected to the OmniSwitch on port 1, the Server is assigned to VLAN 2 (per the network address policy) and port 1 becomes a member of VLAN 2. When IPX Server B is connected to the OmniSwitch on port 2, the Server is assigned to VLAN 3 (per the network address policy) and port 2 becomes a member of VLAN 3. However, ports 1 and 2 are also members of the Group’s default VLAN #1, so port 1 is now a member of VLAN 1 and VLAN 2 and port 2 is now a member of VLAN 1 and VLAN 3.

When IPX Server A sends broadcasts, they are restricted to VLAN 2 because of the network address policies. When IPX Server B sends broadcasts, they are restricted to VLAN 3, also because of the network address policies. However, when the internal IPX router sends out broadcasts on VLAN 1 the broadcasts are flooded out all ports in the Group, because all ports in the Group are, by default, members of VLAN 1. IPX Server A responds to this with a router configuration error because it is receiving broadcasts on VLAN 1 when it should only receive them on VLAN 2. IPX Server B also responds with a router configuration error because it is receiving broadcasts on VLAN 1 when it should only receive them on VLAN 3.

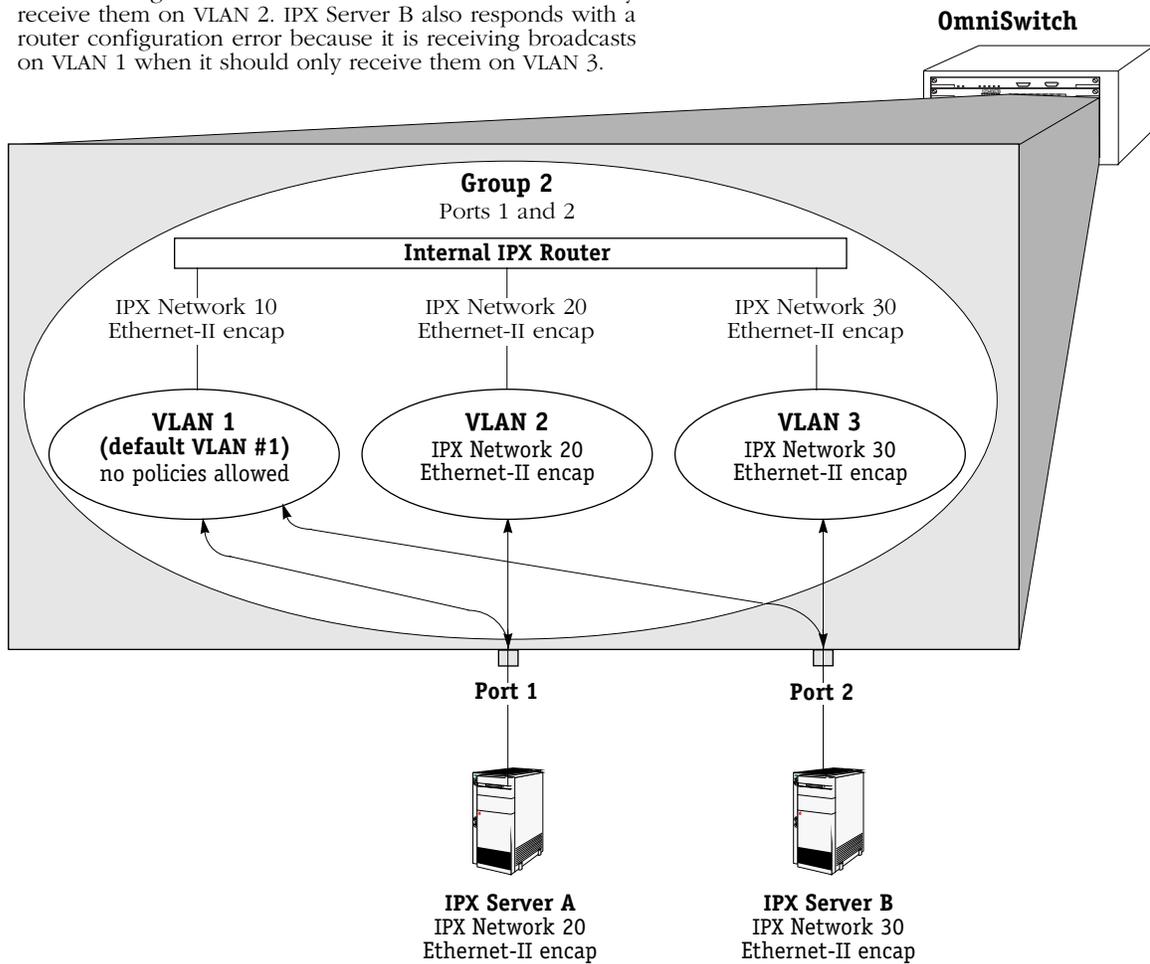
The Solution

The solution for this problem is to disable IPX routing on default VLAN #1. Because of this, when your network includes IPX servers that are members of IPX network address VLANs and IPX routing is enabled, you should configure your network such that disabling IPX routing on default VLAN #1 is not a problem.

Important Note

If you enable routing for a Group, you are actually enabling routing for that Group's default VLAN #1. For this reason, do not enable routing for any Group in which an IPX server is a member of an IPX network address VLAN.

When the internal IPX router sends out broadcasts on VLAN 1, they are flooded out all ports in the Group because, by default, all ports in the Group are members of VLAN 1. IPX Server A responds with a router configuration error because it is receiving broadcasts on VLAN 1 when it should only receive them on VLAN 2. IPX Server B also responds with a router configuration error because it is receiving broadcasts on VLAN 1 when it should only receive them on VLAN 3.



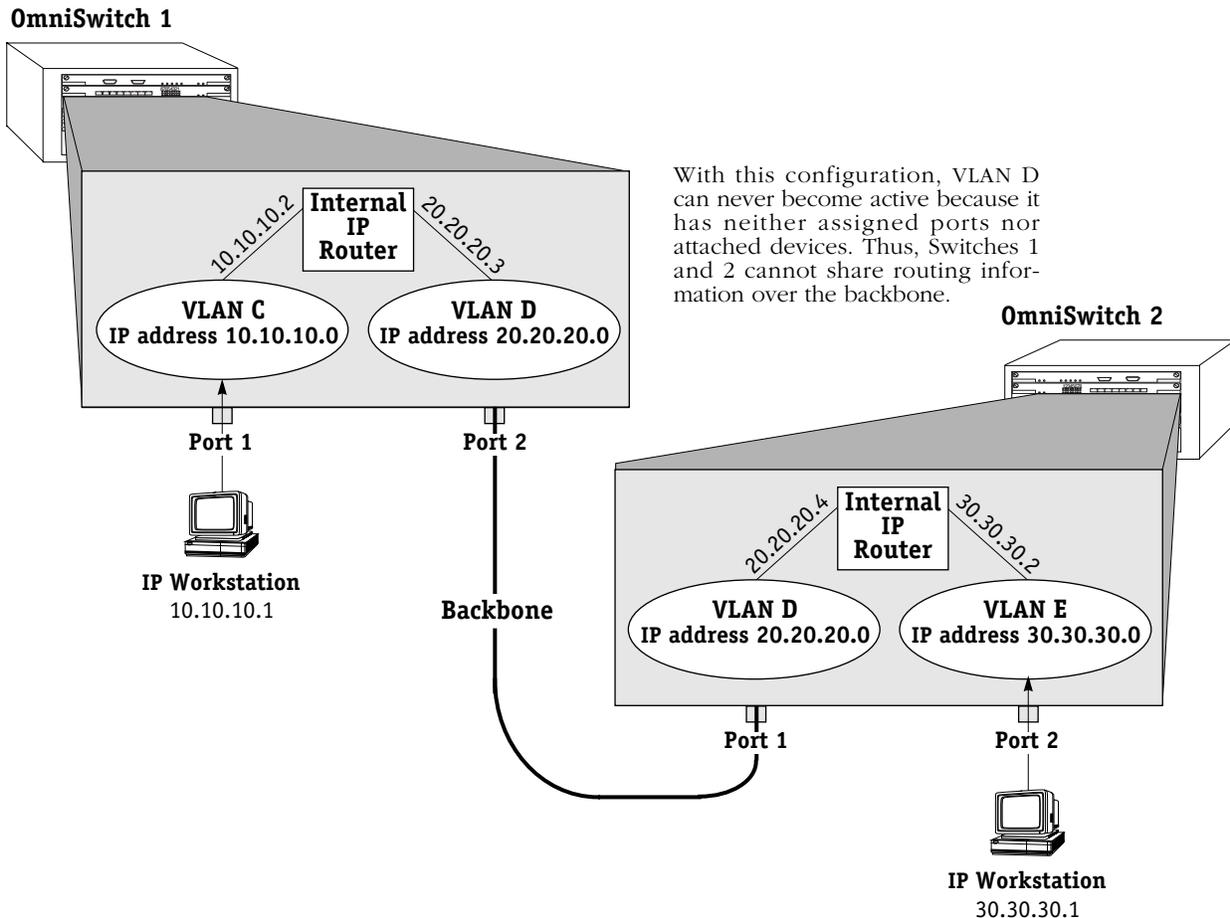
Application Example 5

Traversing a Backbone

Application Example 5 illustrates why port-based policies may be required to establish communications in some network situations, such as traversing a backbone. This necessity arises because, as explained in *How Routing Works Generally* on page 29-8, AutoTracker does not activate a VLAN – or its internal router interface – until a port is assigned to that VLAN. AutoTracker assigns ports to VLANs with port policies immediately. However, AutoTracker only assigns ports to VLANs with logical policies when a frame is received from a source device that matches the VLAN’s policies. This means that, in some network situations, you may need to assign a port policy to a VLAN to force it active.

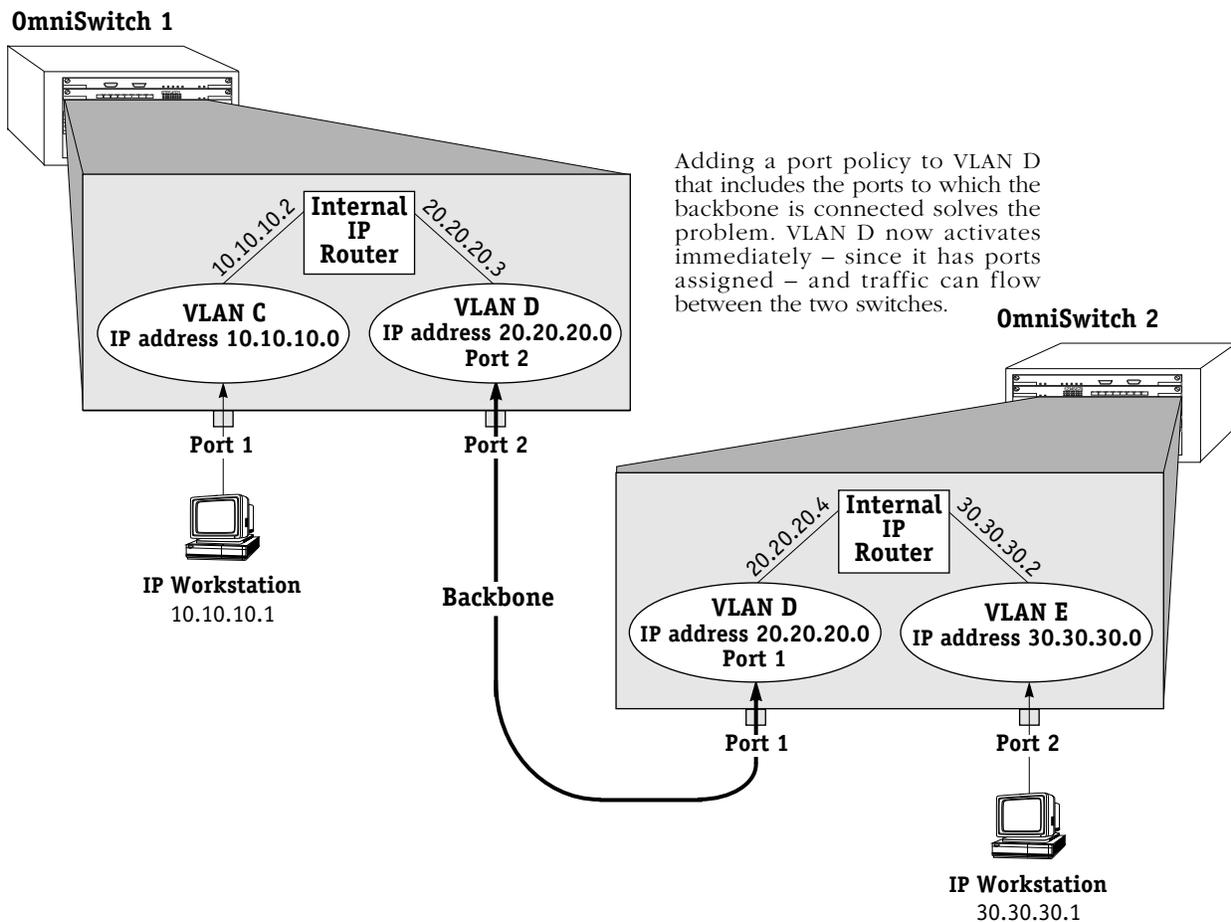
The figure below illustrates the problem that can occur. The network below contains two OmniSwitches in which three IP network address VLANs exist: VLAN C (IP address 10.10.10.0), VLAN D (IP address 20.20.20.0), and VLAN E (IP address 30.30.30.0). VLAN D spans both OmniSwitches, but has no assigned devices. Routing is enabled for all three VLANs. A backbone connects port 2 on OmniSwitch 1 to port 1 on OmniSwitch 2.

When IP workstation 10.10.10.1 transmits a frame VLAN C and its internal router activate. When IP workstation 30.30.30.1 transmits a frame VLAN E and its internal router activate. All subsequent traffic on VLAN C is transmitted to IP workstation 10.10.10.1 and all subsequent traffic on VLAN E is transmitted to IP workstation 30.30.30.1. VLAN D cannot activate because there are no devices that match its network address policy and it has no ports assigned. Because VLAN D is not active, Switches 1 and 2 cannot exchange routing information. Switch 1 will not be aware of network 30 and Switch 2 will not be aware of network 10.



The Solution

The recommended solution is to add a port policy to VLAN D, as is shown in the figure below. A port policy can be defined in addition to any other policies defined for a VLAN. If VLAN D has a port policy that includes port 2 on Switch 1 and port 1 on Switch 2 – the ports to which the backbone is connected – VLAN D and its internal router will activate immediately in both Switch 1 and Switch 2. Traffic (i.e., routing information) can then flow between Switch 1 and Switch 2 over the backbone. Switch 1 will be aware of network 30 and Switch 2 will be aware of network 10.



Please Take Note

Refer to Chapter 25, “Configuring Group and VLAN Policies,” for information on original and current port policy functionality.

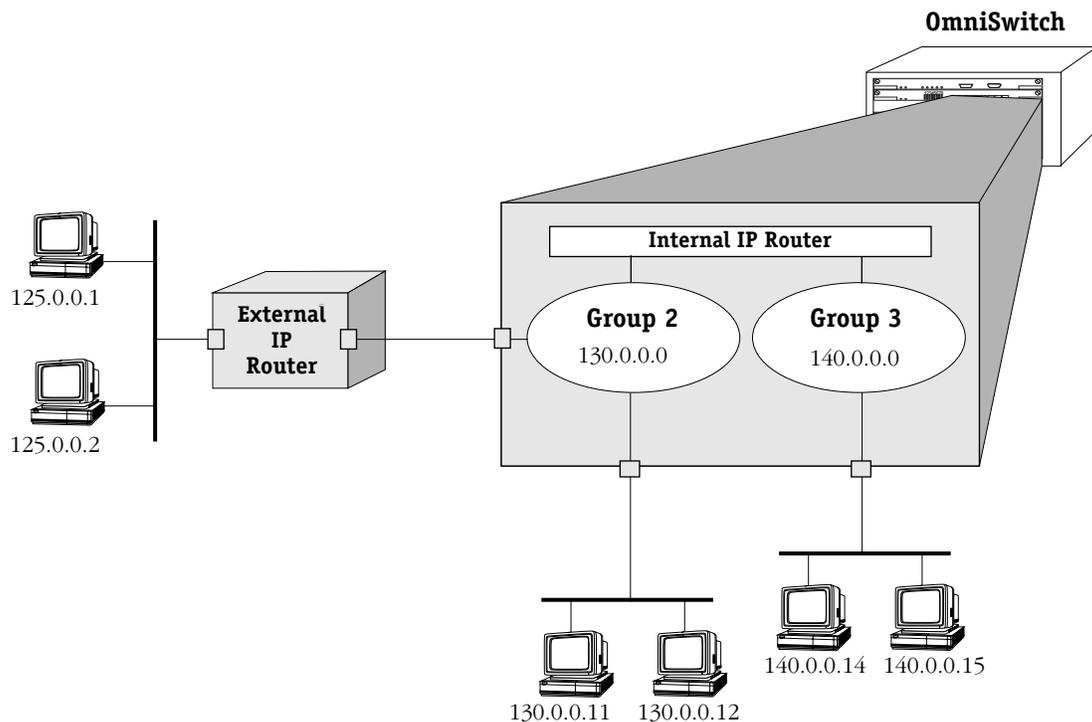
30 IP Routing

Introduction

This chapter gives an overview of IP routing and includes information about configuring static routes and viewing/configuring TCP/IP protocols such as Telnet and the Routing Information Protocol (RIP). IP routing requires at least one virtual router port to be configured on the switch. For information about configuring virtual router ports, see Chapter 24, “Managing Groups and Ports.”

When IP routing is enabled on the switch, the switch exchanges routing information with external IP routers in the network, and stations connected to groups and VLANs with virtual router ports can communicate. Groups or VLANs that do not have router ports with routing enabled are essentially firewalled from each other.

In the example shown here, stations connected to each group can communicate if a virtual router port is created for each group and each router port on the switch has IP routing enabled. Stations in group 2 and group 3 communicate with stations attached to the external IP router if a default route to that router is configured on the switch or the switch learns about the external router through RIP or some other routing protocol.



IP Routing Overview

In switching, traffic may be transmitted from one media type to another within the same broadcast domain (or group/VLAN). Switching happens at layer 2, the physical layer; routing happens at layer 3, the network layer. In routing, traffic may be transmitted across groups/VLANs, and broadcast or multicast traffic is prevented from being transmitted across those domains (unless some other mechanism is set up on the switch, such as UDP forwarding or IP multicast routing).

In IP routing, the switch builds routing tables to keep track of optimal destinations for traffic it receives that is destined for remote networks. The switch also sends and receives routing messages, or advertisements, to/from other routers in the network. When the switch receives a packet to be routed, it strips off the MAC header and examines the IP header of the packet. It looks up the source/destination address in the routing table, and then adds the appropriate MAC address to the packet.

Calculating routing tables and stripping/adding MAC headers to packets is performed by switch software unless a Hardware Routing Engine (HRE) or HRE-X is installed. The HRE or HRE-X significantly improves routing performance. See Chapter 1, “Omni Switch/Router Chassis and Power Supplies,” and Chapter 6, “The MPM,” for information about the HRE-X and HRE respectively. On the Omni S/R, IP routing has a fastpath mechanism that requires the **fpx.img** file to be installed on the switch. On an OmniSwitch with an MPM-III installed, the **fpx3.img** file is required. When fastpath is loaded, some additional statistics display on the IP Statistics and Errors screen available through the **ips** command (see *Viewing IP Statistics and Errors* on page 30-12).

IP is associated with several layer 3 and layer 4 protocols. Some of these protocols are built into the base code loaded into the switch. Others are included as part of Advanced Routing software. Some protocols are specifically used for routing; others are used by any host or end station that has an IP address. A brief overview of supported IP protocols is included here.

Routing Protocols

When IP routing is enabled, the switch uses routing protocols to build routing tables that keep track of stations in the network and to decide the best path for forwarding data. These routing protocols include:

- Routing Information Protocol (RIP)—An interior gateway protocol that defines how routers exchange information in an autonomous system. RIP makes routing decisions using a “least-cost path” method. RIP services are performed by a program operating in the switch called RouteD. RIP and RIP II services are also available from a program called GateD, which is part of Alcatel’s optional Advanced Routing software. RIP, whether performed by RouteD or GateD, allows the switch to learn routing information from other, neighboring RIP routers.
- Open Shortest Path First (OSPF)—An interior gateway protocol that provides a routing function similar to RIP but which uses different techniques to determine the best route for a datagram. OSPF services are provided by GateD, part of Alcatel’s optional Advanced Routing software.
- Border Gateway Protocol (BGP)—An exterior gateway protocol that provides for routing between autonomous systems. BGP is not part of the base code but is included in the Advanced Routing software.

Transport Protocols

IP is both connectionless (it routes each datagram separately) and unreliable (it does not guarantee delivery of datagrams). This means that a datagram may be damaged in transit, or thrown away by a busy router, or simply never make it to its destination. The resolution of these transit problems is to use a layer 4 transport protocol:

- Transmission Control Protocol (TCP)—A major data transport mechanism that provides reliable, connection-oriented, full-duplex data streams. While the role of TCP is to add reliability to IP, TCP relies upon IP to do the actual delivering of datagrams.
- User Datagram Protocol (UDP)—A secondary transport-layer protocol that uses IP for delivery. However, UDP is not connection-oriented so it does not provide reliable end-to-end delivery of datagrams. But some applications can safely use UDP to send datagrams that don't require the extra overhead added by TCP.

Application-Layer Protocols

- Bootstrap Protocol (BOOTP)/Dynamic Host Configuration Protocol (DHCP)—May be used by an end station to obtain an IP address. The switch provides a UDP relay that allows BOOTP requests/replies to cross different networks. See Chapter 31, “UDP Forwarding.”
- Simple Network Management Protocol (SNMP)—Used to manage nodes on a network. SNMP is discussed in Chapter 17, “Configuring SNMP.”
- Telnet—Used for remote connection to a device. The **telnet** command is described in this chapter.
- File Transfer Protocol (FTP)—Enables transferring files between hosts.

Additional IP Protocols

- Internet Control Message Protocol (ICMP)—Specifies the generation of error messages, test packets, and informational messages related to IP. ICMP supports the **ping** command used to determine if hosts are online.
- Address Resolution Protocol (ARP)—Used to find the IP address that corresponds to a given physical (MAC) address.
- Internet Group Management Protocol (IGMP)—Tracks multicast group membership. See the Multicast Services section of the *Advanced Routing User Manual*.
- Resource ReSerVation Protocol (RSVP)—Signals Quality of Service (QoS) requests in an IP network. For more information, see the *Switched Network Services User Manual*.

Setting Up IP Routing on the Switch

IP routing is enabled on a per-port basis by creating a virtual IP router port for a group/VLAN. The switch does not do any routing unless the virtual router port has IP routing enabled (routing is enabled by default). The steps for setting up IP routing on the switch are given here:

Step 1. Configuring a Virtual Router Port

A virtual router port may be created when you set up or modify a group/VLAN through the **crpg** command or **modvl** command described in Chapter 24, “Managing Groups and Virtual Ports.” To create a virtual router port, enable IP routing and specify an IP address for the router port.

When routing is enabled on the port, the switch creates routing tables and address translation tables so it knows how to forward traffic. The switch keeps track of router ports and any other routers in the network. The switch uses the Address Resolution Protocol (ARP) to match IP addresses with MAC addresses. It uses routing protocols, such as the Routing Information Protocol (RIP), to determine the best path for forwarding traffic. (Other routing protocols are available in the Advanced Routing software package.) It also periodically sends/receives routing messages to/from other routers to keep its routing tables updated.

◆ Important Note ◆

When Spanning Tree and IP routing are both enabled, packets are not forwarded unless the Spanning Tree Status for the port to which packets are to be forwarded has progressed from Listening to Learning to Forwarding. For example, if IP is enabled on VLAN 42 that has ports 1/1-3 attached to it and you want to forward to a host from port 1/2. Use the **vi 1/2** command to determine if the Spanning Tree Protocol has entered the Forwarding state for that port.

Step 2. Configuring Optional IP Routing Parameters

Optional configuration for IP routing includes the following:

- Static routes. These are routes that are manually added to the routing table and may be used rather than dynamic routes (which are learned through routing protocols like RIP).
- RIP filters. Controls the operation of RIP by minimizing the number of entries that will be added to the routing table.

Static routes and RIP filters are described in this chapter. This chapter also describes how to view various IP statistics as well as the routing table. It includes information about how to ping another IP host in the network, how to telnet to a remote system, and how to trace an IP route.

Step 3. Configuring Other IP Routing Features

There are several optional features that may be used with IP routing. Some features are included as part of the base code and are described in this user manual. Other features are available as optional switch software and are described in separate user manuals. The features are listed here:

- UDP forwarding—Forwards UDP broadcasts/multicasts across groups/VLANs. See Chapter 31, “UDP Forwarding.”
- GateD—Provides gateway protocols, including RIP, OSPF, and BGP/CIDR. See the *Advanced Routing User Manual*.
- Virtual Router Redundancy Protocol (VRRP)—Used to back up static IP routes. See the *Advanced Routing User Manual*.
- IP Firewall—Enables the switch to act as a gateway to provide security for all data entering and exiting the switch to and from its attached physical ports, as well as internally between groups and VLANs that are defined in the switch. See the *Switched Network Services User Manual*.
- Multicast services—Includes IP multicast switching (IPMS) and IP multicast routing (MrouteD). See the *Advanced Routing User Manual*.
- IP Control—Manages IP addresses through Lightweight Directory Access Protocol (LDAP), DHCP, and Domain Name Service (DNS). See the *Switched Network Services User Manual*.

The Networking Menu

The Networking menu contains commands that control, and are related to, the routing protocols that are run on the switch.

To switch to, and to display, the **Networking** menu, enter the following commands:

```
networking
?
```

If you have enabled the verbose mode, you do not need to enter the question mark (?).

A screen similar to the following displays:

Command	Networking Menu
snmps	View SNMP statistics
snmpc	Configure SNMP
Names	Configure the DNS resolver
probes	Display all RMON probes
events	Display all logged RMON events
IP	Enter IP networking command sub-menu.
IPX	Enter IPX networking command sub-menu
Gated	Enter Gated menu/control Gated
IPMR	Enter the IPMR routing sub-menu
IPMS	Enter the IPMS networking command sub-menu
VRRP	Enter the VRRP menu
QoS	Enter the QoS menu
Policy	Administer the SNS policy sub-menu
LDAP	Configure the SNS LDAP server sub-menu
Monitor	Enter port monitor utility command sub-menu
chngmac	Configure router port's MAC address on selected Group
RD	Routing Domain Management Menu

Main File Summary VLAN Networking
Interface Security System Services Help

The commands in this menu are described throughout this manual as follows:

- The **snmps** and **snmpc** commands are described in Chapter 17, “Configuring SNMP.”
- The **Names**, **probes**, **events**, and **chngmac** commands are described in Chapter 18, “RMON and DNS Resolver.”
- The IP submenu is discussed in this chapter. The IPX submenu is described in Chapter 32, “IPX Routing.”
- The Gated, IPMR, IPMS, VRRP, and RD submenus are available if Advanced Routing software is loaded on the switch. See the *Advanced Routing User Manual* for more information.
- The QoS, Policy, and LDAP submenus are available if Switched Network Services software is loaded on the switch. See the *Switched Network Services User Manual* for more information.
- The Monitor submenu is described in Chapter 24, “Managing Groups and Ports.”

The IP Submenu

The **ip** command in the Networking menu is used to display the IP submenu. To display the IP submenu, enter the following commands:

```
ip
```

```
?
```

If you have enabled the verbose mode, you don't need to enter the question mark (?).

A screen similar to the following displays:

Command	IP Menu
xlat	View the address translation table
ips	View IP stats & errors
ipr	View IP routes
aisr	Add an IP static route
risr	Remove an IP static route
icmps	View ICMP stats & errors
ping	Ping a system
udps	View UDP stats and errors
udpl	View the UDP listener table
rips	View RIP stats and errors
tcps	View TCP-related statistics
tcpc	View the TCP Connection table
telnet	Remote login to another system using TELNET
traceroute	Trace an IP route
relay	Use 'relayc' or 'relays'
fwconfig	Configure the IP Firewall
ripflush	Flush all routes obtained by RIP
ipfilter	Add/delete an IP RIP filter
ipf	Display IP RIP filters
ipmac	View the IP to MAC Address Association table
ipclass	Turn on/off IP Class Address Checking
ipdirbrcast	Turn on/off IP directed broadcast

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

This chapter describes all of the above commands with the exception of **fwconfig**, **relayc**, **relays**, and **ipclass** commands. The **fwconfig** command is described in the *Switched Network Services User Manual*. The relay commands, **relayc** and **relays**, are described in Chapter 31, "UDP Forwarding." The **ipclass** command is described in the *Advanced Routing User Manual*.

Viewing the Address Translation (ARP) Table

The **xlat** command is used to access the ARP (Address Resolution Protocol) Table. This table contains a listing of IP addresses and their corresponding translations to MAC addresses (or slot/port for WAN interfaces). Submenu commands are used to add entries to the table, to delete them, show all the entries currently in the table, to flush “temporary” entries, to display specific entries by either MAC or IP address, and to quit out of the **xlat** submenu.

To begin working with the ARP Table, enter the following command:

xlat

A screen similar to the following displays:

ARP Table Functions

Enter command (Add/Delete/Show/Flush/Macfind/Ipfind/Quit) (Show) :

The default command is **show** which is used to display all entries in the table. The **quit** command is used to exit out of this submenu and return to the main system prompt.

Displaying All Entries in the ARP Table

At the above prompt, press **<Enter>** to select **Show**, the default command.

A screen similar to the following displays:

Address Translation Table

IP Address	at	Physical Address
90.0.0.1	at	3/1, dlci=32
198.206.184.34	at	00:05:02:c0:7f:11
198.206.184.254	at	00:20:da:6a:98:40

Enter command (Add/Delete/Show/Flush/Macfind/Ipfind/Quit) (Show) :

The fields on this screen have the following meanings:

IP Address

The IP address, in dotted-decimal format, of a specific host or other device.

Physical Address

The MAC address, in hexadecimal format, of the specific host or other device that corresponds to the IP address in the left-hand column.

Adding Entries to the ARP Table

The **add** subcommand is used to manually add an IP address entry to the ARP Table. To be able to manage your switch over an IP network connection, you will need at least one IP address configured for the switch.

Follow the steps below to add an address to the ARP Table.

1. Enter **add**.

The following prompt displays:

Host name or IP addr to add:

Enter the name of the host or its IP address.

2. The following prompt displays:

Physical address (format aa:bb:cc:dd:ee:ff):

Enter the host's physical address in hexadecimal format.

3. The following prompt displays:

Publish (i.e., proxy for) this entry? (y/n) (n):

Enter **y** to publish (i.e., proxy for) this ARP entry. This feature allows the switch to answer all ARP requests directed at the hosts on a subnetwork. As the "proxy" for these hosts, the switch responds with its own MAC address whenever ARP requests come in for any of the hosts on the subnetwork. Enter **n** if you do not want this ARP entry to act as a proxy.

4. The following prompt displays:

Is this entry permanent (ie. flush will not remove it) (y/n)? (n) :

Enter **y** if this entry is to be permanent (that is, you do not want it to be removed by the **Flush** subcommand). Enter **n** if the entry is to be temporary (that is, you want to allow it to be removed by the **Flush** subcommand). All of the entries in the table, whether they are permanent or temporary, survive across switch reboots. Therefore, you must use the **Delete** subcommand when you want to remove permanent entries from the table.

5. The following prompt displays:

Use trailer encapsulation on this host (y/n)? (n) :

Enter **y** if you want to use trailer encapsulation on this host. Enter **n** if you do not want to use trailer encapsulation on this host.

6. The system then confirms the addition to the table (an example is shown below).

ARP table entry for host 198.206.184.35 successfully added

7. The **xlat** submenu redisplay:

Enter command (Add/Delete/Show/Flush/Macfind/Ipfind/Quit) (Show) :

Deleting Entries from the ARP Table

The **Delete** subcommand is used to delete a “permanent” IP address from the ARP Table. Follow the steps below to delete an address from the ARP Table.

1. Enter **delete**.

The following prompt displays:

Host name or IP addr to delete:

Enter the host name or address that you wish to delete.

2. The system will then confirm the deletion from the table (an example is shown below).

ARP table entry for host 198.206.184.35 successfully deleted

3. The **xlat** submenu redisplay:

Enter command (Add/Delete/Show/Flush/Macfind/Ipfind/Quit) (Show) :

Flushing Temporary Entries from the ARP Table

The **Flush** subcommand is used to delete “temporary” IP addresses from the ARP Table. Follow the steps below to flush all temporary addresses from the ARP Table.

1. Enter **flush**.

The following prompt displays:

Flushing all non-permanent ARP table entries...done

2. The **xlat** submenu redisplay:

Enter command (Add/Delete/Show/Flush/Macfind/Ipfind/Quit) (Show) :

Finding a Specific IP Address in the ARP Table

The **Macfind** subcommand is used to locate a specific IP address in the ARP Table *based on a known MAC address*. (The **Ipfind** subcommand, discussed next, is used to find a specific MAC address based on a known IP address).

Follow the steps below to display a specific IP address in the ARP Table.

1. Enter **macfind**.

The following prompt displays:

MAC address to find (format aa:bb:cc:dd:ee:ff):

2. Enter the known MAC address (for example, 00:05:02:c0:7f:11).

A prompt similar to the following displays which shows the IP address that is related to the MAC address you entered:

Corresponding IP address: 198.206.184.34

3. The **xlat** submenu will then be redisplayed:

Enter command (Add/Delete/Show/Flush/Macfind/Ipfind/Quit) (Show) :

Finding a Specific MAC Address in the ARP Table

The **ipfind** subcommand is used to locate a specific MAC address in the ARP Table *based on a known IP address or host name*. (The **Macfind** subcommand, discussed above, is used to find a specific IP address based on a known MAC address).

Follow the steps below to display a specific MAC address in the ARP Table.

1. Enter **ipfind**.

The following prompt displays:

Hostname or IP address to find:

2. Enter the known IP address or host name (for example, 198.206.184.34).

A prompt similar to the following displays which shows the MAC address that is related to the IP address entered:

Corresponding MAC address: 00:05:02:c0:7f:11

3. The **xlat** submenu redisplay:

Enter command (Add/Delete/Show/Flush/Macfind/Ipfind/Quit) (Show) :

Viewing IP Statistics and Errors

The **ips** command is used to monitor IP datagram traffic and errors. The **ips** command displays *cumulative* IP statistics and errors. The statistics show the cumulative totals since the last time the switch was powered on or since the last reset of the switch was executed.

To display information about IP statistics and errors, enter the following command:

```
ips
```

The screen display depends on the type of switch you are using. For an OmniSwitch with an MPM-1G, a screen similar to the following displays:

```

IP Statistics and Errors

Default Time to Live                32
Reassembly Timeout (seconds)        1

Total Datagrams Recvd/Forwarded     77972 / 58177
HRE Datagrams Forwarded              0
PDUs Requested for Transmit          4294931545
PDUs Needing Reassembly              0
PDUs Successfully Reassembled        0
PDUs Needing Fragmentation           0
Fragments created                    0

IP Errors (Discards due to the following problems)
Header errors                        0
Address errors                       45994
Unknown/Unsupported Protocol         0
Local discards inbound/outbound      0 / 0
Unknown Route                       45994
Reassembly Failures                  0
Fragmentation Failures               0

```

The Omni Switch/Router (OmniS/R) and an OmniSwitch with MPM-III includes fastpath code that enhances the speed of IP routing. The **fpx.img** file must be loaded on the OmniS/R or the **fpx3.img** file must be loaded on the OmniSwitch for this feature to be enabled. Fastpath statistics are included on the IP Statistics and Errors screen:

```

IP Statistics and Errors

Default Time to Live                32
Reassembly Timeout (seconds)        1

Total Datagrams Recvd/Forwarded     513342 / 513283
Fastpath Datagrams Received          513281
Fastpath Datagrams Forwarded         513280
Fastpath Inbound Discards            1
Fastpath Utilization                 100%
PDUs Requested for Transmit          4294931545
PDUs Needing Reassembly              0
PDUs Successfully Reassembled        0
PDUs Needing Fragmentation           0
Fragments created                    0

IP Errors (Discards due to the following problems)
Header errors                        0
Address errors                       45994
Unknown/Unsupported Protocol         0
Local discards inbound/outbound      0 / 0
Unknown Route                       45994
Reassembly Failures                  0
Fragmentation Failures               0

```

The fields on this screen have the following meanings:

Default Time to Live

The default time, in seconds, assigned to each outgoing IP datagram before it is discarded as expired.

Reassembly Timeout (seconds)

The time, in seconds, to wait for all fragments to arrive before discarding datagrams.

Total Datagrams Recvd/Forwarded

The total number of input IP datagrams received, including those received in error.

HRE Datagrams Forwarded

The total number of IP datagrams forwarded by the HRE (Hardware Routing Engine).

Fastpath Datagrams Received

(Displays for Omni S/R or OmniSwitch with MPM-III.) The number of IP datagrams received by the fastpath code.

Fastpath Datagrams Forwarded

(Displays for Omni S/R or OmniSwitch with MPM-III.) The number of IP datagrams forwarded to their destination without using the MPM.

Fastpath Inbound Discards

(Displays for Omni S/R or OmniSwitch with MPM-III.) The number of bad packets received and discarded. Typically this value should be zero.

Fastpath Utilization

(Displays for Omni S/R or OmniSwitch with MPM-III.) The percentage of total datagrams received that are forwarded by the fastpath code.

PDU's Requested for Transmit

The total number of IP datagrams which transmit local IP user-protocols (including ICMP) supplied to IP in requests for transmission, not including forwarded datagrams.

PDU's Needing Reassembly

The number of IP datagram fragments that needed to be reassembled by this switch.

PDU's Successfully Reassembled

The number of IP datagrams successfully reassembled by this switch.

PDU's Needing Fragmentation

The number of IP datagrams requiring fragmentation by this switch.

Fragments created

The number of IP datagram fragments that have been generated as a result of fragmentation by this switch.

Header errors

The number of input IP datagrams discarded due to errors in their IP header, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discarded in processing their IP options, etc.

Address errors

The number of input IP datagrams discarded because the IP header destination field contained an invalid address.

Unknown/Unsupported Protocol

The number of local addresses, unsupported protocols, datagrams received successfully but discarded because of an unknown or unsupported protocol.

Local discards inbound/outbound

The number of packets discarded, both inbound and outbound, though they had no errors to prevent their being transmitted (lack of buffer space, etc.).

Unknown Route

The number of packets received and discarded by IP because IP was unable to route them.

Reassembly Failures

The number of failures detected by the IP reassembly algorithm for all reasons (timed out, error, etc.) This value is not necessarily a count of the discarded fragments.

Fragmentation Failures

The number of IP datagrams discarded because they needed to be fragmented but could not be. This situation could happen when a large packet has the "Don't Fragment" flag set.

Viewing the IP Forwarding Table

The **ipr** command is used to display the IP Forwarding Table. The entries in the table show the routes entered by a routing protocol, if the switch is running any of the supported protocols, and the static routes that you may have entered manually. You can also add to, or remove static routes from, the IP Forwarding Table (see *Adding an IP Static Route* on page 30-17 and *Removing an IP Static Route* on page 30-19).

To display the IP Forwarding Table, enter the following command:

```
ipr
```

A screen similar to the following displays:

10 routes in forwarding table

IP FORWARDING TABLE

Network	Mask	Gateway	Metric	Group VLAN Id:	Protocol
0.0.0.0	255.0.0.0	198.206.184.254	1	1:1	STATIC
10.0.0.0	255.0.0.0	10.0.0.1	1	6:1	STATIC
11.0.0.0	255.0.0.0	11.0.0.1	1	5:1	STATIC
90.0.0.0	255.0.0.0	90.0.0.3	1	4:1	DIRECT
127.0.0.0	255.0.0.0	127.0.0.1	0	1:2	LOOPBACK
127.0.0.1	255.255.255.255	127.0.0.1	0	2:3	LOOPBACK
196.196.7.0	255.255.255.0	196.196.7.42	1	3:1	RIP
198.206.187.0	255.255.255.0	198.206.183.0	1	1:4	STATIC
198.206.184.0	255.255.255.0	198.206.184.42	1	1:1	RIP
203.229.229.0	255.255.255.0	203.229.229.250	1	2:1	RIP

If routing domains are configured on the switch, the **ipr** command will display the forwarding table for the default routing domain only. Routing domains are part of Advanced Routing software and are not part of the base code. For more information about routing domains, see Chapter 14, "Routing Domains," in the *Advanced Routing User Manual*.

To display the forwarding table for a routing domain other than the default domain, enter the **ipr** command with the relevant routing domain ID. For example:

```
ipr 2
```

The screen display is similar to the following:

4 routes in forwarding table

IP FORWARDING TABLE for Routing Domain 2

Network	Mask	Gateway	Metric	Group VLAN Id:	Protocol
0.0.0.0	255.0.0.0	198.206.184.254	1	1:1	STATIC
10.0.0.0	255.0.0.0	10.0.0.1	1	6:1	STATIC
11.0.0.0	255.0.0.0	11.0.0.1	1	5:1	STATIC
90.0.0.0	255.0.0.0	90.0.0.3	1	4:1	DIRECT

Viewing the IP Forwarding Table

The fields on the IP Forwarding Table have the following meanings:

Network

The destination network IP address.

Mask

The IP subnet mask.

Gateway

The network address of the gateway (the router from which this address was learned).

Metric

The metric associated with this network. Generally, this is a RIP “hop” count, or the number of hops the network is away from this router.

Group VLAN Id

The group and VLAN number from which this IP address was learned.

Protocol

The way in which this route was learned, for example, through RIP.

Adding an IP Static Route

The **aisr** command is used to add IP static routes to the switch's IP Forwarding Table. You might want to add a static route to send traffic to a router other than the one determined by the routing protocols.

In order to add a static route, you will need to know the host/net IP address and the gateway IP address which will be used to route traffic to the external IP address. If routing domains are configured on the switch and you want to add the route to a particular domain other than the default, you will need to know the relevant routing domain ID (RDID). For more information about routing domains, see Chapter 14, "Routing Domains," in the *Advanced Routing User Manual*.

Follow the steps below to add an IP static route.

1. Enter **aisr**. The prompt that displays depends on whether routing domains are configured on the switch.

If routing domains *are* configured on this switch, the following prompt displays:

**Routing Domains (RD) are configured on this switch.
List the RD(s) you want this route applied to? (default: none) :**

If you do not want to apply the new route to a particular routing domain, press **Enter**. To apply the route you are adding to an existing routing domain, enter the desired routing domain ID (RDID) and go to step 3.

If routing domains *are not* configured on this switch or if you are applying this route to the default domain, the following prompt displays:

Do you want to see the current route table? (y or n) (y) :

2. Enter a **y** at this prompt (or press **Enter**) to display the current forwarding table.

A screen similar to the following displays:

IP FORWARDING TABLE

Network	Mask	Gateway	Metric	Group VLAN Id:	Protocol
0.0.0.0	255.0.0.0	198.206.184.254	1	1:1	STATIC
10.0.0.0	255.0.0.0	10.0.0.1	1	6:1	STATIC
11.0.0.0	255.0.0.0	11.0.0.1	1	5:1	STATIC
90.0.0.0	255.0.0.0	90.0.0.3	1	4:1	DIRECT
127.0.0.0	255.0.0.0	127.0.0.1	0	1:2	LOOPBACK
127.0.0.1	255.255.255.255	127.0.0.1	0	2:3	LOOPBACK
196.196.7.0	255.255.255.0	196.196.7.42	1	3:1	RIP
198.206.187.0	255.255.255.0	198.206.183.0	1	1:4	STATIC
198.206.184.0	255.255.255.0	198.206.184.42	1	1:1	RIP
203.229.229.0	255.255.255.0	203.229.229.250	1	2:1	RIP

Destination IP address of host or network :

3. At the prompt for the destination IP address, enter the address of the host or network to which you are setting up a route. For a "default" route, use an entry of 0.0.0.0 as the IP address (or just enter the word **default**).
4. If you entered an IP address, a prompt similar to the following displays:

Host or network mask (255.255.255.000) :

Enter the mask (or just press **<Enter>** to accept the default mask).

5. The following prompt displays:

IP address of next hop :

Enter the IP address of the next hop (the gateway) router to the destination IP address. The gateway address must be on the same network as one of the VLANs (that is, it must be a directly connected network).

A message will confirm the creation of the static route:

Route successfully added

Removing an IP Static Route

The **risr** command is used to remove IP static routes from the switch's IP Forwarding Table.

Follow the steps below to remove an IP static route.

1. Enter **risr**. The prompt that displays depends on whether routing domains are configured on the switch. For more information about routing domains, see Chapter 14, "Routing Domains," in the *Advanced Routing User Manual*.

If routing domains *are* configured on this switch, the following prompt displays:

**Routing Domains (RD) are configured on this switch.
List the RD(s) you want this route applied to? (default: none) :**

If you are removing a route from an existing domain, press **Enter**. To remove a route from an existing routing domain, enter the desired routing domain ID (RDID) and go to step 3.

If routing domains are not configured on this switch, or if you are applying this route to the default domain, the following prompt displays:

Do you want to see the current route table? (y or n) (y) :

2. Enter a **y** at this prompt (or just press **<Enter>**) to display the current forwarding table.

A screen similar to the following displays:

IP FORWARDING TABLE

Network	Mask	Gateway	Metric	Group VLAN Id:	Protocol
0.0.0.0	255.0.0.0	198.206.184.254	1	1:1	STATIC
10.0.0.0	255.0.0.0	10.0.0.1	1	6:1	STATIC
11.0.0.0	255.0.0.0	11.0.0.1	1	5:1	STATIC
90.0.0.0	255.0.0.0	90.0.0.3	1	4:1	STATIC
127.0.0.0	255.0.0.0	127.0.0.1	0	1:2	LOOPBACK
127.0.0.1	255.255.255.255	127.0.0.1	0	2:3	LOOPBACK
196.196.7.0	255.255.255.0	196.196.7.42	1	3:1	RIP
198.206.187.0	255.255.255.0	198.206.183.0	1	1:4	STATIC
198.206.184.0	255.255.255.0	198.206.184.42	1	1:1	RIP
203.229.229.0	255.255.255.0	203.229.229.250	1	2:1	RIP

Destination IP address of host or network :

3. At the prompt for the destination IP address, enter the IP address of the host or network that you want to remove.

4. A prompt similar to the following displays:

Host or network mask (255.255.255.000) :

Enter the mask (or just press **<Enter>** to accept the default mask).

5. The following prompt displays:

IP address of next hop :

Enter the IP address of the next hop (the gateway) router to the destination IP address.

A message will confirm the deletion of the static route:

Route successfully deleted

Viewing ICMP Statistics and Errors

The `icmps` command is used to monitor ICMP activity.

To display information about ICMP statistics and errors, enter the following command:

```
icmps
```

A screen similar to the following displays:

ICMP Statistics		
	In	Out
Total ICMP Messages	1	1
Redirect Messages	0	0
Echo Messages	1	0
Echo Reply Messages	0	1
Time Stamp Messages	0	0
Time Stamp Reply Messages	0	0
Address Mask Messages	0	0
Address Mask Reply Messages	0	0

ICMP Errors		
	In	Out
Errors	0	0
Destination Unreachable Msgs	0	0
Time Exceeded Msgs	0	0
Parameter Problems	0	0
Source Quenches	0	0

The following field descriptions pertain to both the “in” and “out” statistics:

Total ICMP Messages

The total number of ICMP messages which this switch received or attempted to send out.

Redirect Messages

The number of ICMP Redirect messages sent/received by this switch.

Echo Messages

The number of ICMP Echo messages sent/received by this switch to see if a destination is active and reachable.

Echo Reply Messages

The number of ICMP Echo Reply messages received by this switch.

Time Stamp Messages

The number of Time Stamp Request messages sent/received by this switch requesting/receiving a reply with timestamp.

Time Stamp Reply Messages

The number of Time Stamp Reply messages sent/received by this switch.

Address Mask Messages

The number of Address Mask Reply messages that were sent/received by this switch in an attempt to determine the subnet mask for a network.

Address Mask Reply Messages

The number of Address Mask Reply messages that were sent/received by this switch.

Errors

The number of ICMP messages this switch sent/received but was unable to process because something was wrong (for example, a checksum failure).

Destination Unreachable Msgs

The number of ICMP “destination unreachable” messages that were sent/received. These occur when the gateway is unable to route a datagram to its destination.

Time Exceeded Msgs

The number of “time exceeded” messages that were sent/received. These occur when a packet is dropped because the Time-to-Live counter reaches zero. When a large number of these messages are encountered this is a symptom that packets are looping, that congestion is severe, or that the Time-to-Live counter is set too low. These messages also occur when all the fragments trying to be reassembled don't arrive before the reassembly timer expires.

Parameter Problems

The number of messages sent/received which indicate that an illegal value has been detected in a header field. These messages can indicate a problem in the sending host's IP software or possibly in the gateway's software.

Source Quenches

The number of messages sent/received which tell a host that is sending too many packets. A host should attempt to reduce its transmissions upon receiving these messages.

Using the PING Command

The **ping** command is used to test the reachability of IP network destinations. A fast ping command (**fping**) is also available for repeating the last ping request sent from the switch. The commands send an ICMP echo request to a destination and then wait for a reply.

Follow the steps below to issue an IP ping request.

1. Enter **ping**.

A screen similar to the following displays:

Host () :

Enter the IP address of the host that you want to “ping.”

2. The following prompt displays:

Count (0 for infinite) (0) :

Enter the number of frames to be transmitted (0 equals “infinite”). To abort an “infinite” transmission once it is in progress, just press **Enter** again.

3. The following prompt displays:

Size (64) :

Enter the desired size of the data portion of the packet. You can specify a packet size or a range of packet sizes up to 8148. If you give a range, the switch will increment the packet size by 1 each time up to the top of the range. It will then wrap and continue from the bottom size of the range again until the total number of frames specified in the count has been sent. You can also set the increment by which the packet size is increased each time by entering a comma and an increment number after the size. For example, an entry of

1-100,5

will send out the number of frames specified in the “Count” prompt, starting with a frame size of 1 and incrementing up to a frame size of 100 in steps of 5. Note that if the “Count” is too small, the 100-byte frame size may never be reached. If the count is large enough, the packet size will wrap and go back to 1.

4. The following prompt displays:

Timeout (1) :

Enter the number of seconds the program is to wait for a response before timing out.

5. After answering the previous prompt, a screen similar to the following displays:

```

Ping starting, hit <RETURN> to stop
PING 198.206.184.18: 64 data bytes

[0      ] ..... .T...
[50     ] ...T. ....
[100    ] .....
[150    ] .....
[200    ] .....
[250    ] .....

```

This screen shows the progress of the ping operation as it is taking place. The numbers in the square brackets indicate how many packets have been transmitted for that row. The periods to the right of the brackets represent packets as they are exchanged between the switch and the device owning the IP address entered for the ping.

A period (.) indicates a packet that was sent out by the switch and came back to the switch. Occasionally, you may see a **T** character in place of a period. A **T** indicates a packet that was sent out and never came back to the switch (or a “lost” packet).

When you press **Enter**, the ping operation stops and a screen similar to the following displays.

```

---198.206.184.18 PING Statistics---
283 packets transmitted, 281 packets received, 0% packet loss
Round-trip (ms) min/avg/max = 6/28/638

```

This display shows a recap of the **ping** request just completed and its results. The screen shown in this example indicates a successful ping operation.

```

-- PING 198.206.184.18 PING Statistics --

```

This display indicates the IP address of the device the switch tried to ping. This is the same IP address entered in step 1 of the ping request.

```

283 packet transmitted, 281 packets received, 0% packet loss

```

The first value indicates the total number of packets transmitted from the switch to the IP address. The second value indicates the total number of packets received by the switch, back from the IP address. The third value indicates the percent of packets lost of those originally transmitted.

```

Round-trip (ms) min/avg/max

```

These values indicate the amount of time it took for the ping to be sent, received by the other device, replied to by the other device and received back by the switch. Because the amount of time needed to complete a round-trip will vary, three values are given to indicate the minimum, maximum and the average time taken to complete a round-trip. These values are shown in milliseconds.

To repeat the last ping request, enter the following command at the system prompt:

```

fping

```

The last ping issued on the switch is immediately sent again. If no ping was previously issued, a prompt for the host address displays and defaults are used for Count, Size, and Timeout.

Viewing UDP Statistics and Errors

The **udps** command is used to display a listing of UDP statistics and errors. The **udps** command displays cumulative statistics since the last time the switch was powered on or since the last reset of the switch was executed.

To display information about UDP statistics and errors, enter the following command:

```
udps
```

A screen similar to the following displays:

```
Total UDP datagrams received           : 831  
Total UDP datagrams transmitted      : 22  
Total Datagrams received w/unknown applications : 0  
Total UDP datagrams w/other Errors    : 0
```

The fields on this screen have the following meanings:

Total UDP datagrams received

The total number of UDP datagrams delivered to UDP applications.

Total UDP datagrams transmitted

The total number of UDP datagrams sent from this switch.

Total UDP datagrams received w/unknown applications

The total number of datagrams for which there was no application at the destination.

Total UDP datagrams w/other Errors

The total number of UDP datagrams that could not be delivered for reasons other than lack of application at the destination.

Viewing the UDP Listener Table

The **udpl** command is used to display the UDP Listener Table. This table contains information about the switch's UDP end-points on which a local application is currently accepting datagrams. The UDP Listener Table shows the local IP addresses for each UDP listener and the local port number for this listener. An IP address of zero (0.0.0.0) indicates that it is listening on all interfaces.

To view the UDP Listener Table, enter the following command:

```
udpl
```

A screen similar to the following appears:

UDP Listener Table			Recv-Q	Send-Q
Local Address/Port				
0.0.0.0	/	162	0	0
0.0.0.0	/	161	0	0
0.0.0.0	/	520	0	0
0.0.0.0	/	1024	0	0

Local Address/Port

The local IP address, and the local port number, for this UDP connection. In the case of a connection in the listen state, which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.

Recv-Q and Send-Q

For the SNMP Traps (port 162) this is the number transmitted (there is no receive).

For the SNMP Requests (port 161) this is the number of Request PDUs sent and the number of Response PDUs received.

For RIP (port 520) this is the number of packets received and transmitted.

Viewing RIP Statistics and Errors

The **rips** command is used to display RIP statistics and errors. This command displays cumulative statistics since the last time the switch was powered on, or since the last reset of the switch was executed.

To display information about RIP statistics and errors, enter the following command:

```
rips
```

A screen similar to the following displays:

```

                                RIP Statistics
Rtr (Group ID:VLAN ID 1:1) IP Address 198.206.182.115 RIP Mode silent
In          4769          Out          0
Transmit Error    0          Non-zero field    0
Bad Version      0          Bad Metric        0
Bad Family       0          Bad Size          0
Bad Address      0          Bad Command       0
```

The fields on this screen have the following meanings:

In/Out

The total number of RIP packets received and transmitted on a per-virtual-LAN basis.

Transmit Error

The total number of RIP packets that were unable to be sent.

Bad Version

The total number of RIP messages delivered to the switch that were not version 1.

Bad Family

The number of packets received on this VLAN whose family ID was not of the Internet family.

Bad Address

The number of received packets whose IP address was not a Class A, B, or C.

Non-zero Field

The number of received packets whose mandated “must-be-zero” fields were not zero.

Bad Metric

The number of received packets with a routing entry’s metric that was out of range.

Bad Size

The number of received packets that were not compatible with the expected size.

Bad Command

The number of received packets whose command field was not a “request” or “response.”

Viewing TCP Statistics

The **tcps** command is used to monitor TCP traffic activity and check TCP configuration parameters. To reconfigure TCP parameters, see *Viewing the TCP Connection Table* on page 30-29.

To display information about TCP activity, enter the following command:

```
tcps
```

A screen similar to the following displays:

```

TCP Statistics

Round Trip Algorithm Used      : RSRE (MIL-STD-1778)
Retransmission Min/Max Timeout : 300/3000
Max Connections Allowed       : Unlimited
Active Opens                   : 76
Passive Opens                  : 43
Attempt Fails                  : 0
Established Resets            : 5
Currently Established         : 3
Total Segments Received       : 1117
Total Segments Sent           : 832
Total Segments Retransmitted  : 0
Total Segments Received w/err : 0
Total Segments Sent w/RST flag : 0

```

The fields on this screen have the following meanings:

Round Trip Algorithm Used

The algorithm used to determine the Timeout value used for retransmitting unacknowledged octets. The value is: RSRE (MIL-STD-1778).

Retransmission Min/Max Timeout

The minimum/maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.

Max Connections Allowed

The maximum number of connections allowed. Currently, the number is unlimited.

Active Opens

The number of times TCP connections have made a direct transition to the “synSent” state from the “closed” state (refer to RFC 973).

Passive Opens

The number of times TCP connections have made a direct transition to the “synReceived” state from the “listen” state (refer to RFC 973).

Attempt Fails

The number of times TCP connections have made a direct transition to the “closed” state from either the “synSent” state or the “synReceived” state, plus the number of times TCP connections have made a direct transition to the “listen” state from the “synReceived” state.

Established Resets

The number of times TCP connections have made a direct transition to the “closed” state from either the “established” state or the “closeWait” state.

Currently Established

The number of TCP connections for which the current state is either “established” or “closeWait”.

Total Segments Received

The total number of segments received, including those received in error. This count includes segments received on currently established connections.

Total Segments Sent

The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

Total Segments Retransmitted

The number of TCP segments transmitted containing one or more previously transmitted octets.

Total Segments Received w/err

The total number of TCP segments that are in error; for example, bad TCP checksums.

Total Segments Sent w/RST flag

The number of TCP segments containing the RST flag.

Viewing the TCP Connection Table

The **tcpc** command is used to check the current TCP connections available in the TCP Connection Table.

To display the TCP Connection Table, enter the following command:

```
tcpc
```

A screen similar to the following displays:

TCP Connection/Listener Table						
Local Address/Port	Remote Address/Port	Recv-Q	Send-Q	Conn State		
127.0.0.1 / 1090	27.0.0.1 / 1091	0	0	ESTABLISHED		
127.0.0.1 / 1091	127.0.0.1 / 1090	0	322	ESTABLISHED		
198.206.184.42 / 23	198.206.184.34 / 2057	0	0	ESTABLISHED		
0.0.0.0 / 23	0.0.0.0 / 0	0	0	LISTEN		
0.0.0.0 / 21	0.0.0.0 / 0	0	0	LISTEN		

The fields on this screen have the following meanings:

Local Address/Port

The local IP address for this TCP connection and the local port for this TCP connection. In the case of a connection in the listen state which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.

Remote Address/Port

The remote IP address/the remote port number for this TCP connection.

Recv-Q

The number of segments received on this port.

Send-Q

The number of segments sent on this port.

Conn State

Describes the state of the TCP connection, as defined in RFC 973. Possible values are: closed, listen, synSent, synReceived, established, finWait1, finWait2, closeWait, lastAck, closing, time-Wait, and deleteTCB.

Using the TELNET Command

The **telnet** command is used to connect to another system. All of the standard TELNET commands are supported by the software in the switch.

To initiate a TELNET session, enter the following command:

```
telnet
```

A screen similar to the following displays:

```
telnet>
```

To display a listing of the TELNET commands, enter the following command:

```
?
```

A screen similar to the following displays:

```
Commands may be abbreviated. Commands are:
```

close	close current connection
display	display operating parameters
mode	try to enter line or character mode ('mode ?' for more)
open	connect to a site
quit	exit telnet
send	transmit special characters ('send ?' for more)
set	set operating parameters ('set ?' for more)
unset	unset operating parameters ('unset ?' for more)
status	print status information
toggle	toggle operating parameters ('toggle ?' for more)
environ	change environment variables ('environ ?' for more)
?	print help information

Enter the desired commands to establish and conduct your TELNET session.

Cancelling a Telnet request

If you initiate a Telnet session to an IP address that is not responding, after several seconds the switch will respond with the following message:

```
telnet: Unable to connect to remote host: S_error_ETIMEDOUT
```

If you don't want to wait for the switch to timeout on its own, you can cancel your request for a Telnet session by typing either **Ctrl-J** or **Ctrl-C**.

Tracing an IP Route

The **tracert** command is used to find the IP route from the local switch to a specified IP address destination. This command displays the individual hops to the destinations as well as some timing information. When using the **tracert** command, you must enter the name of the destination as part of the command line.

As an example, we might want to trace the route to “corporate.com.” To do so, we would enter this command:

```
tracert corporate.com
```

A screen similar to the following displays:

```
tracert to corporate.com (198.206.185.7),30 hops max,40 byte packets  
1 branch-wan-gw.CORPORATE.COM (198.206.181.252) 16 ms 0 ms 16 ms  
2 10.254.1.253 (10.254.1.253) 98 ms 81 ms 98 ms  
3 198.206.185.7 (198.206.185.7) 121 ms 81 ms 98 ms
```

Each number displayed corresponds to an individual hop. The time needed to reach that hop is shown (in milliseconds) after the hop’s IP address. The time may be followed by one of the following codes:

- !** The TTL of the received ICMP message is less than or equal to 1.
- !H** The host was unreachable.
- !N** The network was unreachable.
- !P** The protocol was unreachable.

If the time is replaced by an asterisk (*), no response was received from the host during the default 3-second timeout period.

Flushing the RIP Routing Tables

The **ripflush** command is used to flush all entries in the RIP Routing Table. All existing routes, with the *exception* of static and direct routes, are removed from the table by entry of the **ripflush** command.

To flush the RIP Routing Table, enter the following command:

ripflush

No message is displayed; the system prompt simply reappears.

Configuring IP RIP Filters

The **ipfilter** command is used to add or delete an IP RIP Output or Input filter. The IP RIP Filtering feature gives you a means of controlling the operation of the IP RIP protocol. By using IP RIP filters, you can minimize the number of entries that are put into the IP Forwarding Table as well as improve overall network performance by eliminating unnecessary traffic.

Two types of IP RIP filters are available:

- **RIP Input** filters control which IP networks are allowed into the switch's IP Forwarding Table whenever IP RIP updates are received.
- **RIP Output** filters control the list of IP networks that are included in the RIP Updates sent out by the switch on any interface. Thus, RIP Output filters effectively control which networks the router advertises in the RIP updates it generates.

Here are some example uses of IP RIP filters:

- RIP Input and Output filters can be used to isolate entire network segments (and/or routers) in order to make the network "appear" differently to the network's various segments.
- RIP Input and Output filters can be used to reduce the overall amount of WAN traffic that is needed to advertise routes that should not be used by a particular network segment.

◆ Important Note ◆

The IP RIP Filtering feature works *only* with the switch's standard RIP routing protocol. If you elect to use Alcatel's Advanced Routing feature (GateD) to provide RIP routing functionality in your switch, you will not be able to activate IP RIP Filtering.

Adding a "Global" IP RIP Filter

Follow the steps below to add a "global" IP RIP Output or Input filter.

1. Enter **ipfilter**.

A screen similar to the following displays:

Selecting global IP filter:

Add or delete entry {add(a), delete(d)} (a) :

Enter **a** (or just press **Enter**) to select to add a filter.

2. The following prompt displays:

**Filter type{RIP Output(ro),
RIP Input(ri)} (ro) :**

Enter **ro** (or just press **Enter**) to add a RIP Output filter. Enter **ri** to add a RIP Input filter.

3. The following prompt displays:

Filter action {block(b), allow(a)} (a) :

Enter **a** (or just press **Enter**) to set the filter action to "allow."

Enter **b** to set the filter action to "block."

- The following prompt displays:

IP address (default: all networks) :

Enter the IP address of the network that is to be allowed or blocked by the filter (or just press **Enter** to use the default of all networks). If you choose the default you will *not* be prompted for the network mask (as is shown in the next step).

- The following prompt displays:

IP network mask (default: 255.255.255.0) :

Enter the IP network mask of the network that is to be allowed or blocked by the filter (or just press **Enter** to use the default mask of 255.255.255.0). Note that the default mask will vary depending on the class of the IP address you entered above.

- A message displays indicating that the filter was successfully added:

ipfilter successfully added

Adding an IP RIP Filter For a Specific Group or VLAN

Follow the steps below to add an IP RIP Output or Input filter for a specific Group or VLAN.

- Enter the Group and VLAN numbers after the command like this: **ipfilter 1:1**.

A screen similar to the following displays:

Selecting IP filter for interface 1:1 :

Add or delete entry {add(a), delete(d)} (a) :

Filter action {block(b), allow(a)} (a) :

IP address (default: all networks) :

IP network mask (default: 255.255.255.0) :

ipfilter successfully added

Enter **a** (or just press **Enter**) to select to add a filter.

- The following prompt displays:

**Filter type{RIP Output(ro),
RIP Input(ri)} (ro) :**

Enter **ro** (or just press **Enter**) to add a RIP Output filter. Enter **ri** to add a RIP Input filter.

- The following prompt displays:

Filter action {block(b), allow(a)} (a) :

Enter **a** (or press **Enter**) to set the filter action to “allow.” Enter **b** to set the filter action to “block.”

- The following prompt displays:

IP address (default: all networks) :

Enter the IP address of the network that is to be allowed or blocked by the filter (or press **Enter** to use the default of all networks). If you choose the default you will *not* be prompted for the network mask (as is shown in the next step).

5. The following prompt displays:

IP network mask (default: 255.255.255.0) :

Enter the IP network mask of the network that is to be allowed or blocked by the filter (or just press **Enter** to use the default mask of 255.255.255.0). Note that the default mask will vary depending on the class of the IP address you entered above.

6. If the Group:VLAN is a WAN routing service, the following prompt displays:

**Do you wish to apply this filter to a specific WAN endpoint? (n): y
Frame Relay VC or PPP Peer {vc(v), peer(p)} (v):**

Enter **y** to apply this filter to a specific WAN endpoint.

7. The following prompt displays:

Frame Relay VC or PPP Peer {vc(v), peer(p)} (v):

Enter **v** (or just press **Enter**) to apply this filter to a Frame Relay VC.

Enter **p** if you want to apply this filter to a PPP Peer.

8. If you choose to apply the filter to a Frame Relay VC, this prompt will appear:

Slot/port:

Enter the slot and port numbers to which you want to apply this filter.

9. You will then be prompted for the virtual circuit (VC) to which to apply this filter:

VC:

Enter the VC to which you want to apply this filter.

10. If you choose to apply a filter to a PPP Peer, this one prompt will appear:

Peer ID:

Enter the Peer ID to which you want to apply this filter.

A message will appear indicating that the filter was successfully added.

IP RIP Filter Precedence

Whenever you use multiple “allow” filters you must first define a filter to block all RIPs. Then, any other “allow” filters of the same type must be *at least* as specific in all areas in order for the filters to work. Note that filtering precedence is related only to “allow” filters. Multiple “block” filters can be defined with varying specificity in each of the areas of the filter. The filtering done by the configurable parameters (Address/Mask) in the “allow” filter must be at least as specific as the filtering defined in the “block” filter.

Deleting IP RIP Filters

Follow the steps below to delete an existing IP RIP Output or Input filter.

1. Enter **ipfilter**.

A screen similar to the following displays:

Selecting global IP filter:

Add or delete entry {add(a), delete(d)} (a) :

Enter **d** to select to delete a filter.

2. A screen similar to the following displays:

Displaying all filters:

#	Type	Network	Mask	Md	GP:VL (s/p/vc) (Peer ID)
1	RIP OUT	99.0.0.0	255.0.0.0	A	global
2	RIP IN	99.0.0.0	255.0.0.0	B	2:1

Entry number to delete? (default: none) :

This screen contains a list of the existing IP RIP filters. The fields on this screen are described in the next section (see *Displaying IP RIP Filters* on page 30-37).

3. Enter the index number of the filter that you want to delete. If you decide at this point that you want to abort out of the deletion process, simply press **Enter** to accept the default of “none”.
4. A message will confirm the deletion of the filter:

ipfilter successfully deleted

Displaying IP RIP Filters

The **ipf** command is used to display a list of all existing IP RIP Output and Input filters. See *Configuring IP RIP Filters* on page 30-33 for complete information on creating these filters.

Displaying a List of All IP RIP Filters

To display the listing of all existing IP RIP filters, enter the following command:

```
ipf
```

A screen similar to the following displays:

Displaying all filters:

#	Type	Network	Mask	Md	GP:VL (s/p/vc) (Peer ID)
1	RIP OUT	99.0.0.0	255.0.0.0	A	global
2	RIP IN	99.0.0.0	255.0.0.0	B	2:1
3	RIP OUT	All Networks		B	5:1 (3/1/32)
4	RIP IN	All Networks		B	6:1 (P1)

This screen contains a list of the existing IP RIP filters. The fields on this screen have the following meanings:

#

Indicates the index number assigned to identify this filter.

Type

Indicates the type of filter, either RIP Input (**RIP IN**) or RIP Output (**RIP OUT**).

Network

Indicates the IP address that is to be filtered (entered in dotted-decimal format). An entry of "All Networks" means that all addresses are to be filtered.

Mask

The IP network mask of the network to be filtered (entered in dotted-decimal format). This field is blank if the network entered is "All Networks."

Md

Indicates the filter's mode of operation, either to "allow" traffic (**A**) or to "block" traffic (**B**).

GP:VL (s/p/vc) or (Peer ID)

The first number (**GP**) is the Group associated with this entry. The second number (**VL**) is the VLAN associated with this entry. When a filter applies to all interfaces, this field will say "global." If an entry refers to a Frame Relay interface, column headings for slot, port, and virtual circuit (**s/p/vc**) may be displayed when the filter is applied to a particular virtual circuit rather than to the entire VLAN. If an entry refers to a PPP interface, the Peer ID (**Peer ID**) may be displayed when the filter is applied to a particular PPP Peer.

Displaying a List of "Global" IP RIP Filters

To display a listing of just the global IP RIP filters, enter the following command:

```
ipf global
```

A screen similar to the following displays:

Displaying global filters:

#	Type	Network	Mask	Md	GP:VL (s/p/vc) (Peer ID)
1	RIP OUT	99.99.99.99	255.0.0.0	A	global

Displaying a List of Specific IP RIP Filters

To display a listing of IP RIP filters for a specific interface, you can specify other parameters along with the **ipf** command. The format for the command in this case is:

```
ipf <type> <GP:VL>
```

The type is one of these codes:

ri for RIP INput

ro for RIP OUTput

For example, to display a list of the filters defined for Group 2, VLAN 1, you would enter:

```
ipf 2:1
```

A screen similar to the following would be displayed:

Displaying filters for interface 2:1:

#	Type	Network	Mask	Md	GP:VL (s/p/vc) (Peer ID)
1	RIP IN	99.0.0.0	255.0.0.0	B	2:1

As another example, to display a list of all global RIP Output filters, you would enter:

```
ipf ro global
```

A screen similar to the following would be displayed:

#	Type	Network	Mask	Md	GP:VL (s/p/vc) (Peer ID)
1	RIP OUT	99.0.0.0	255.0.0.0	A	global

Viewing the IP-to-MAC Address Table

The **ipmac** command is used to display the IP-to-Mac Address Association Table. This table contains a listing of IP addresses and their associated MAC (Media Access Control) addresses together with the slot/port from which the information was learned. The information in this table is learned from ARP (Address Resolution Protocol) messages received on “leaf” ports. A “leaf” port is one on which Spanning Tree has been disabled or on which no Spanning Tree BPDUs have yet been received.

The **ipmac** command can be very helpful in resolving certain problems. For example, in large networks where hosts are frequently moved around, users can experience connectivity problems. In this situation, the **ipmac** command can be used to help locate a particular IP workstation. Another use is to help resolve duplicate IP addresses on a network. The program checks all ARP messages, whether they are received on a “leaf” port or not, against those in its table to see if a duplicate IP address exists. If a duplicate is detected, an SNMP trap message is generated and the duplicate can easily be seen in the table produced by the **ipmac** command.

The **ipmac** command can be entered alone in which case it will display all entries currently in the table, or you may enter a specific IP address along with the command to show only the information related to that IP address. An optional parameter (-f) can be entered to flush the table. Each of these uses of the **ipmac** command is illustrated below.

Displaying All Entries in the IP-to-MAC Table

To display the list of all the entries in the IP-to-MAC table, enter the following command:

```
ipmac
```

A screen similar to the following displays:

IP to MAC ADDRESS ASSOCIATION TABLE

IP Address	MAC Address	Slot / Intf
192. 168. 10. 1	0020DA:6DE610	4 / 5
172. 16. 0. 5	0020DA:76D3D0	3 / 2
172. 16. 0. 7	00E029:00D41E	3 / 2
172. 16. 0. 41	0000C0:24FFEC	3 / 2
172. 16. 0. 47	00A0C9:0AA907	3 / 2
172. 16. 0. 28	0020DA:7AE9D3	3 / 2
172. 16. 0. 45	080020:8AE301	3 / 2
172. 16. 0. 60	0020DA:73C3A0	3 / 2
172. 16. 30. 00	0020AF:04BA57	3 / 2
172. 16. 41. 03	0000C0:AD8EE9	3 / 2
172. 16. 50. 12	080020:7B79E1	3 / 2
172. 16. 255.254	0020DA:6F97E5	3 / 2
*****	0020DA:032273	5 / 1
192. 168. 10. 1	0020DA:7AEA60	3 / 2
198. 206. 182.222	0020DA:7F48A0	3 / 2

The fields on this screen have the following meanings:

IP Address

The IP address learned from ARP messages received on “leaf” ports. A series of asterisks (*****) in this field indicates that the preceding entry is a duplicate to this entry. In the example screen shown above, the address 172.16.255.254 is assigned to two MAC addresses.

MAC Address

The MAC address corresponding to the listed IP address.

Slot/Intf

The slot number and interface number from which the IP and MAC addresses were learned.

Displaying Information for a Specific IP Address

To display the entry in the IP-to-MAC table for a specific IP address, enter the desired IP address after the command. For example, to locate the entry for IP address 192.168.10.1, enter the following command:

```
ipmac 192.168.10.1
```

A screen similar to the following displays:

IP to MAC ADDRESS ASSOCIATION TABLE

IP Address	MAC Address	Slot / Intf
192.168. 10. 1	0020DA:6DE610	4 / 5

Flushing Entries from the Table

To flush all the entries in the IP-to-MAC table, enter the following command:

```
ipmac -f
```

The system prompt redisplay.

Enabling/Disabling Directed Broadcasts

An IP directed broadcast is an IP datagram that has all zeroes or all 1's in the host portion of the destination IP address. The packet is sent to the broadcast address of a subnet to which the sender is not directly attached. The datagram is routed through the network as a unicast packet. When it arrives at the subnet, it is converted into a broadcast packet.

Directed broadcasts are used in denial-of-service *smurf* attacks. In a smurf attack, a continuous stream of ping requests are sent from a falsified source address to a directed broadcast address, resulting in a large stream of replies, which can overload the host of the source address.

By default, the switch drops directed broadcasts. Typically, directed broadcasts should not be enabled.

To enable directed broadcasts to be routed through the switch:

1. At the system prompt, enter the **ipdirbcast** command.
2. Enter **y** to enable direct broadcasts.

Path MTU Discovery

All Gigabit Ethernet modules and all Mammoth-based Ethernet modules on the OmniSwitch and Omni Switch/Router in Release 4.0 and later support path Maximum Transmission Unit (MTU) discovery. In path MTU discovery, the Ethernet frame (datagram) size is set to the largest size that does not require fragmentation anywhere along the path from a source host to its destination. This frame size, known as a Path MTU (PMTU), is thus equal to the minimum of the MTUs of each hop in the path.

◆ Note ◆

MTU discovery is *not* supported on token ring, FDDI, WAN, or non-Mammoth Ethernet modules. However, token ring and FDDI can be used as intermediate links (e.g., trunking or bridging) between remote switches.

Path MTU discovery is active all of the time and is part of the switch's operating system; you do not need configure it.

The source host initially assumes that the PMTU of a path is the MTU of the first hop. It sends all datagrams with the "Don't Fragment" (DF) bit set. If a switch/router along the path receives a datagram that is too large to forward without fragmentation, the following steps will be executed:

1. The switch/router that cannot forward these datagrams (i.e., the constricting hop) will discard them.
2. The constricting hop will send ICMP destination unreachable messages to the source host with a code that indicates fragmentation is needed and the "Don't Fragment" (DF) bit in the Internet Protocol (IP) header has been set. This message (known as a "Datagram Too Big" message) contains the PMTU of the constricting hop.
3. After receiving a "Datagram Too Big" message, the source host reduces the size of the MTU so it matches the PMTU of the constricting hop.
4. The MTU discovery process ends when datagrams can be sent without fragmentation. However, the source host will *not* reduce the size of a datagram below 68 octets.

31 UDP Forwarding

UDP is a connectionless transport protocol that is used for applications that do not require the establishment of a session and end-to-end error checking, such as email and file transfer. This chapter describes the UDP relay function in the switch, which allows UDP broadcast packets to be forwarded across groups and VLANs that have IP routing enabled. The UDP relay allows you to use nonroutable protocols in a routing environment. (For information about IP routing, see Chapter 30, “IP Routing.”)

◆ Note ◆

BOOTP/DHCP relay has previously been available on the switch. It is now part of an expanded feature that includes relays for NetBIOS and generic services.

The relay may be configured for the following services:

- Bootstrap Protocol (BOOTP)/Dynamic Host Configuration Protocol (DHCP)
- NetBIOS Name Server (NBNS)
- NetBIOS Datagram Distribution Server (NBDD)
- Generic applications, such as Trivial File Transfer Protocol (TFTP)

The UDP services, their corresponding well-known port numbers, and configurable options on the switch are listed here.

Service	UDP Port No.	Configurable Options
BOOTP/DHCP	67/68	Next-hop address (up to 8) Forward delay Maximum hops
NBNS	137	Next-hop address (up to 8) Forwarding VLANs (up to 32)
NBDD	138	Next-hop address (up to 8) Forwarding VLANs (up to 32)
Generic	user-configured	Next-hop address (up to 8) Forwarding VLANs (up to 32)

UDP Relay and RIF Stripping

Routing Information Field (RIF) stripping is required for transparent bridge ports in source route environments and may also be useful in non-source route environments. For an introduction to RIF stripping, see Chapter 21, “Managing Token Ring.”

In a source route environment, where RIF stripping is enabled for transparent bridging to Ethernet, UDP relay clients should not be more than one switch away from the DHCP server. (In RIF stripping, 2 bytes are stripped from the RIF and each bridge adds 2 bytes to the RIF. Packets with a RIF greater than 2 bytes are discarded.)

In non-source route environments, RIF stripping may be required if DHCP clients are token ring stations. Token ring stations may have packets with RIFs even though source routing is not enabled on the station. RIF stripping is required if there is bridging to Ethernet, FDDI, or 802.3 LANE anywhere along the path between the client and the DHCP server. RIF stripping should be enabled on the first non-token ring port in the path. The number of bridges on the path does not matter.

UDP Relay Hardware/Software Support

The UDP forwarding feature has the following hardware/software support:

- UDP relay is supported on any OmniSwitch or Omni Switch/Router (OmniS/R).
- To relay DHCP requests from authentication clients in a default group to a DHCP server in an authenticated group, the **avlbootpmode** command must be used in addition to the **relayc** command described in this chapter. See the Authentication Services chapter of the *Switched Network Solutions User Manual* for information about the **avlbootpmode** command.

UDP Relay Configuration Screen

To configure any of the UDP relays, use the **relayc** command. The **relayc** command is listed in the IP submenu. (For more information about IP commands, see Chapter 30, “IP Routing.”) The screen display is similar to the following:

UDP Relay Configuration

```
1) BOOTP/DHCP Enabled      : No
2) NBNS Enabled            : No
3) NBDD Enabled            : No
4) +Generic Services Menu
```

Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw) :

Use the UDP Relay Configuration screen to enable any of the relays and display more configuration options for enabled relays. The following sections describe each UDP service and how to configure each of the relays using the User Interface (UI). A UDP statistics screen may also be displayed.

◆ Note ◆

For general information about the UI, see Chapter 8, “The User Interface.”

BOOTP/DHCP Relay

The switch supports a UDP relay function that allows Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) packets to pass between AutoTracker Groups.

◆ Note ◆

A BOOTP/DHCP relay may be configured for authenticated groups as well. See *BOOTP/DHCP Relay and Authentication* on page 31-5 and the Authentication Services chapter of the *Switched Network Solutions User Manual*.

Through UI software, you can turn the relay function on or off and specify the IP addresses of DHCP servers, the delay before the relay forwards a request, and the maximum number of hops a packet may be forwarded through the network.

Alternately the relay function may be provided by an external router connected to the switch; in this case, the relay would be configured on the external router.

Overview of DHCP

DHCP provides a framework for passing configuration information to Internet hosts on a TCP/IP network. It is based on the Bootstrap Protocol (BOOTP), adding the ability to automatically allocate reusable network addresses and additional configuration options. DHCP consists of the following two components:

- A protocol for delivering host-specific configuration parameters from a DHCP server to a host.
- A mechanism for allocating network addresses to hosts.

DHCP is built on a client-server model in which a designated DHCP server allocates network addresses and delivers configuration parameters to dynamically configured hosts. It supports the following three mechanisms for IP address allocation:

Automatic	DHCP assigns a permanent IP address to a host.
Dynamic	DHCP assigns an IP address to a host for a limited period of time (or until the host explicitly relinquishes the address).
Manual	The network administrator assigns a host's IP address and DHCP simply conveys the assigned address to the host.

A particular network will use one or more of these mechanisms, depending on the policies of the network administrator.

For information about configuring DHCP servers, see the IP Control chapter of the *Switched Network Solutions User Manual*.

DHCP and the OmniSwitch or OmniS/R

The unique characteristics of the DHCP protocol require a good plan before setting up the switch in a DHCP environment. Since DHCP clients initially have no IP address, placement of these clients in an AutoTracker VLAN is hard to determine. In simple networks (i.e., one group, one VLAN) AutoTracker rules do not need to be deployed to support the BOOTP/DHCP relay functionality.

In multiple group configurations, AutoTracker rules can be deployed to strategically support the relay function. Two types of AutoTracker IP policies are appropriate for DHCP environments. The first is the IP protocol policy that puts all IP type frames into a single VLAN regardless of network address. The second is the IP network policy that groups IP users based on their specific IP address.

Besides AutoTracker rules, the network administrator must be aware that some network environments may contain DHCP-ready and non-DHCP clients. Such configurations are supported by the switch's BOOTP relay function.

BOOTP/DHCP Relay and Source Routing

In source route environments (where VLAN framing type is set for source routing) and DHCP clients are not directly attached to the switch but have one or more bridges between them, the **mpm.cmd** or **mpx.cmd** file must be modified so that replies from the DHCP server can get through the bridge.

Typically a router caches the client's RIF information for source routing when the client responds to an ARP, but if the client does not yet know its IP address it cannot reply to an ARP and no RIF information is cached on the router. Unicast replies to the client before the RIF is cached are discarded by the router. Forcing the BOOTP reply to be broadcast eliminates this problem.

Use the **edit** command to make this change to the **mpm.cmd** or **mpx.cmd** file (see Chapter 11, "Managing Files," for instructions on using the **edit** command).

Add the following command:

```
bootpBcastReply=1
```

Reboot the switch to force the broadcast. Replies from the DHCP server to the client will be broadcast from the router as STE or ARE packets so they can be sent through the bridge.

BOOTP/DHCP Relay and Authentication

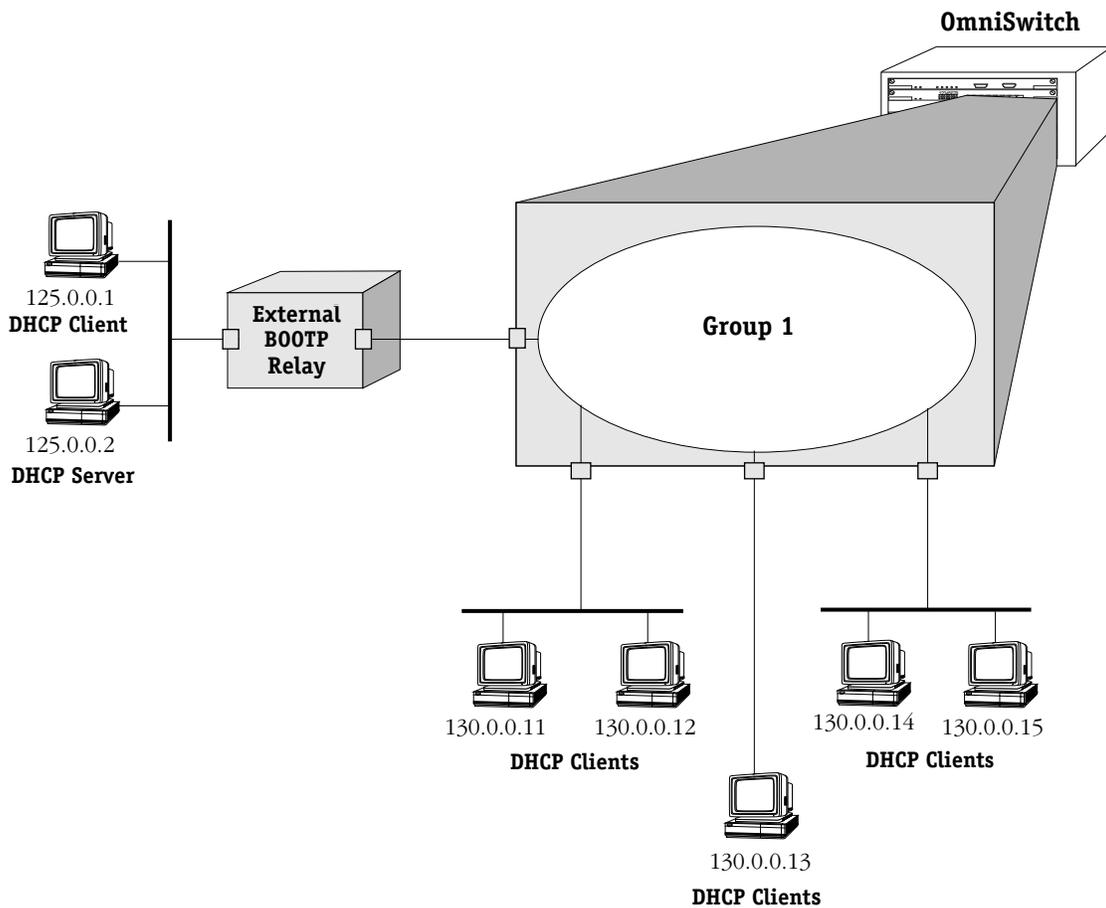
Authentication clients may use DHCP to get an IP address. For Telnet authentication clients, an IP address is required for authentication. The DHCP server may be located in the default group, an authenticated group, or both. If authentication clients will be getting an IP address from a DHCP server located in an authenticated group, a BOOTP/DHCP relay should be set up using the **relayc** command described in this chapter.

In addition, the router port address of the authenticated group must also be configured for the relay through the **avlbootpmode** command. See the Authentication Services chapter of the *Switched Network Solutions User Manual* for more information about this command.

External BOOTP Relay

The BOOTP relay may be configured on a router that is external to the switch. In this application example the switched network has a single AutoTracker Group configured with multiple segments. All of the network hosts are DHCP-ready, meaning they obtain their network address from the DHCP server. The DHCP server resides behind an external network router, which supports the BOOTP relay functionality.

One requirement for routing DHCP frames is that the router must support BOOTP relay functionality to be able to forward DHCP frames. In this example, BOOTP relay is supported within an external router, which forwards request frames from the incoming router port to the outgoing router port attached to the OmniSwitch.



DHCP Clients are Members of the Same VLAN

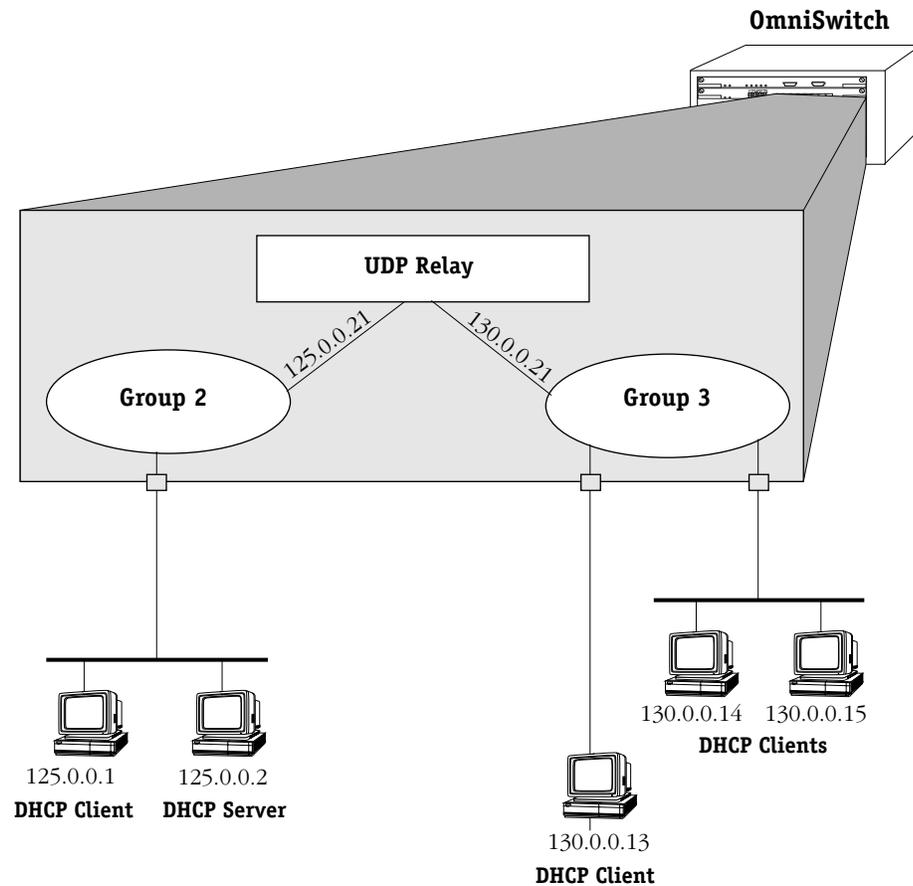
The external router inserts the subnet address of the first hop segment into the DHCP request frames from the DHCP clients. This subnet address allows the DHCP server to locate the segment that the requesting client resides on. In this example, all clients attached to the OmniSwitch are DHCP-ready and will have the same subnet address (130.0.0.0) inserted into each of the requests by the router's BOOTP relay function. The DHCP server will assign a different IP address to each of the clients. The switch does not need an IP address assigned and all DHCP clients will be members of either a default VLAN or an IP protocol VLAN.

Internal BOOTP/DHCP Relay

The internal BOOTP/DHCP relay is configured using the UDP forwarding feature in the switch, available through the **relayc** command. See *UDP Relay Configuration Screen* on page 31-3.

Example 1

This application example shows a network with two AutoTracker Groups, each with multiple segments. All network clients are DHCP-ready and the DHCP server resides on just one of the groups. This example is much like the first application example, except that the BOOTP relay function is configured inside the switch.



DHCP Clients in Two Groups

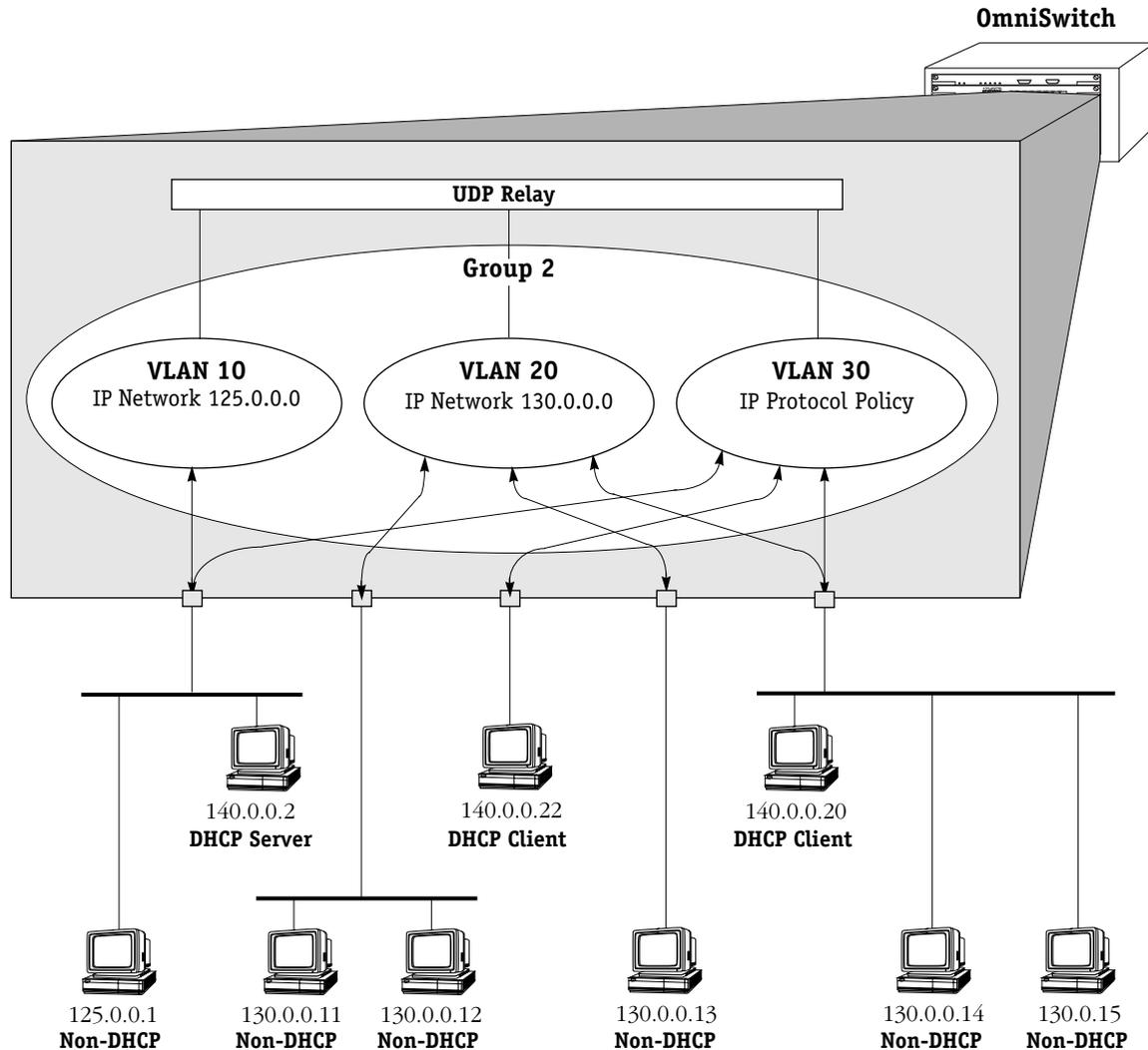
During initialization, each network client forwards a DHCP request frame to the DHCP server using the local broadcast address. For those stations locally attached, the frame will simply be switched.

In the example above, the DHCP server and clients in the same group must be members of the same VLAN so that the policies match (they could also all be members of the default VLAN). One way to accomplish this is to use an IP protocol policy that places all IP frames in the same VLAN. An IP network policy would not work in this case because the DHCP clients will not have an IP network address until *after* they communicate with the DHCP server.

Because the clients in group 3 are not on the same segment as the DHCP server, they must request an IP address via the BOOTP relay routing entity in the switch. When a DHCP request frame is received by the BOOTP relay entity, it will be forwarded from group 3 to group 2. All the DHCP-ready clients in group 3 must be members of the same VLAN, and the switch must have the BOOTP relay function configured.

Example 2

This application example has a single group in a network with a mix of DHCP-ready and non-DHCP clients. DHCP-ready and non-DHCP clients can coexist in the same network, group, or segment. There are two types of AutoTracker policies defined within the group—IP address and IP protocol.



AutoTracker IP Policy Places DHCP Clients in Same VLAN

Whenever AutoTracker receives an IP frame, it examines the frame for an IP network layer policy match. In the case of DHCP, the client generates an IP frame without an IP address. Without an IP address, AutoTracker will not be able to place the client into a VLAN based on IP address. Therefore, the client will become a member of the VLAN defined by a general IP Protocol policy (i.e., VLAN 30).

In this example, the VLAN defined by an IP protocol policy is used *as a mechanism to group the DHCP server and associated clients*. The DHCP server is local, so all clients requesting an IP address will be allocated an IP address on the same subnet.

◆ Note ◆

This configuration works if you require only one DHCP subnet. All clients received on the same router port will be assigned to the same VLAN.

Note that the client's request frames will also be received and forwarded by the BOOTP relay if it is configured.

The non-DHCP workstations will be assigned to VLANs defined by Network Address policies. These workstations already have manually configured IP addresses. They don't require a server to dynamically assign them an address. AutoTracker will move these workstations into the VLANs with IP network address policies (VLAN 10 and VLAN 20).

It is true that these non-DHCP workstations also match the IP protocol policy. However, Network Address policies have precedence over IP protocol policies. If AutoTracker finds a match on a Network Address policy, it does not look for a protocol policy match.

Enabling BOOTP/DHCP Relay

To enable UDP relay for BOOTP/DHCP:

At the prompt for the UDP Relay Configuration screen (the UDP Relay Configuration screen is displayed using the **relayc** command described in *UDP Relay Configuration Screen* on page 31-3), enter the following:

1=y

The screen redisplay with more configuration options for BOOTP/DHCP.

UDP Relay Configuration

```

1) BOOTP/DHCP Enabled           : Yes
  11) Server Address(list/add/delete) : UNSET
  12) Forward Delay              : 3
  13) Maximum Hops              : 4
2) NBNS Enabled                 : No
3) NBDD Enabled                 : No
4) +Generic Services Menu

```

Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw) :

The parameters are defined here.

Server Address

This parameter allows you to list, add, or delete the server address(es) to which the BOOTP/DHCP relay will forward. The default is **UNSET**. When you have configured at least one valid address, the value redisplay as **SET**. Up to 8 addresses may be configured. *The server address cannot be an internal DHCP server configured through the IP Control feature. For more information about IP Control, see the **Switched Network Solutions User Manual**.*

Forward Delay

The amount of time (typically in seconds, but determined by the client) the BOOTP/DHCP relay will wait before forwarding a request to the server address. This delay gives a local server a chance to respond to a client before the relay forwards it further out in the network. This value may range from 1 to 65535.

Maximum Hops

The maximum number of relays that a packet can go through while traversing the network. This limit keeps packets from “looping” through the network. Set this value to the maximum number of BOOTP/DHCP relays you expect packets to traverse. This value may range from 1 to 16.

Configuring BOOTP/DHCP Relay Parameters

At least one server address must be configured for the BOOTP/DHCP relay. To configure the server address:

1. On the UDP Relay Configuration screen prompt, enter

11=a

A screen displays similar to the following:

FORWARD TO Server List

Item	Server address	Server Name (if known)
------	----------------	------------------------

Enter IP address or host name of server to be added to the list ['h' for help/<ret> to exit]

2. Enter the IP address, which may be a specific host on the network or a subnet broadcast address. The address should be in dotted decimal format (i.e., 198.206.181.12) or hexadecimal address (i.e., 0xc6ceb501). Alternately you may enter a host name (i.e., system.com) if the DNS resolver is enabled on the switch through the **res** command. The screen redisplay with the entry.
3. Repeat the previous step to add all the addresses to which you want to forward to. Press **Enter** when you are finished adding addresses. The screen redisplay with the Server Address field set to **SET**.
4. Make any changes to Forward Delay or Maximum Hops.
5. Enter **s** to save your changes. If the relay has just been enabled, the system initializes the relay. If the relay is already running, it is stopped and reinitialized with the changes.
6. Enter **q** to quit the UDP Relay Configuration screen.

By default, Alcatel's implementation of BOOTP rejects packets less than 300 bytes. To prevent BOOTP from discarding packets smaller than 300 bytes add the following line to the **mpm.cmd** or **mpx.cmd** file:

bootpSizeCheck=0

This line must appear before the **cminit** line.

NetBIOS Relays

The switch supports a UDP relay function that allows Network Basic Input/Output System (NetBIOS) messages to be sent across groups or VLANs.

Overview of NetBIOS

NetBIOS is an applications interface that allows computers on Ethernet or token ring LANs to communicate with one another. An enhanced version of the protocol is used by networking operating systems such as LAN Manager and Windows NT.

With NetBIOS, each client and host in the LAN has a unique NetBIOS name. Stations in a NetBIOS network broadcast queries to verify that their names are unique on the LAN. Names may be verified by using the NetBIOS Name Server (NBNS) protocol, which sends messages to a well-known UDP port (137). Name requests are sent to an IP subnet broadcast address or the unicast address of the server.

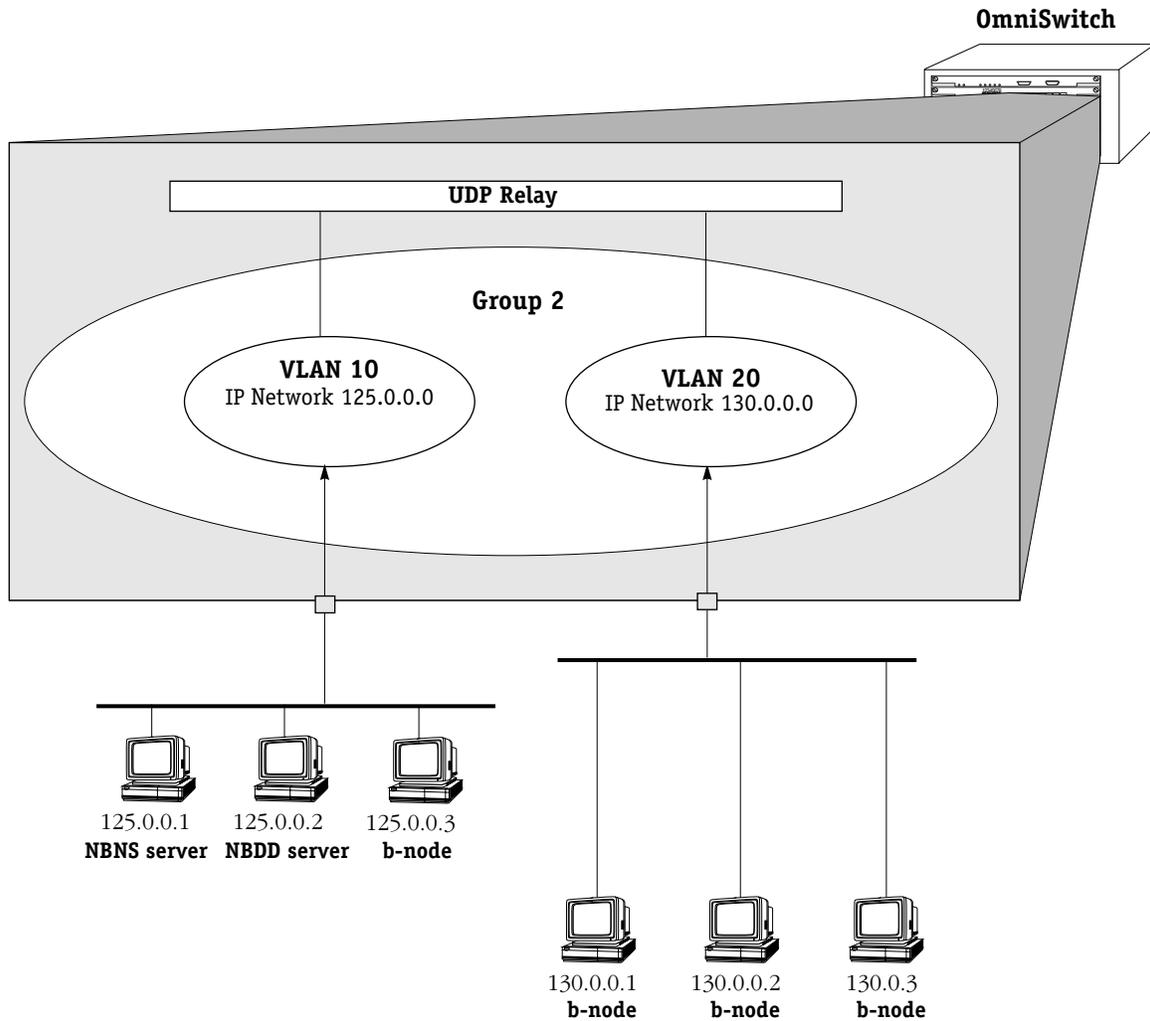
The NetBIOS protocol also has a datagram service that allows an application to exchange datagrams with a specific application or to broadcast and receive datagrams on a VLAN. A NetBIOS Datagram Distribution (NBDD) server may be installed in the network to provide this service, which uses a well-known UDP port number (138).

NetBIOS may be configured to run over TCP/IP using the various modes defined in RFC_1001 and RFC_1002. These modes are defined in terms of *nodes* and determine how NetBIOS stations (or nodes) in the network register their NetBIOS names and resolve (or map) these names to IP addresses. Each NetBIOS PC has a node type. The nodes are defined as follows:

- Broadcast node (b-node)—These nodes use broadcast for name registration and resolution. Since routers do not forward broadcast traffic, b-node clients in different networks will not be able to communicate
- Point-to-point node (p-node)—In this environment, each station knows the address of the server. Unicast queries are sent directly to the name and datagram servers. This method does not use broadcast.
- Mixed-mode node (m-node)—This mode uses a combination of b-node and p-node.

NetBIOS Relay Application

The UDP relay function in the switch extends b-node functionality across the internet. An example application is shown here.



NetBIOS Relay Application

In this example, NBNS and NBDD relays should be configured to forward to VLAN 10 and VLAN 20. The VLANs must be selected for forwarding, or you can configure the subnet address of the VLANs as next-hop addresses. The server addresses could be configured as next-hop addresses, but since the assignment of the NBNS and NBDD servers are by definition dynamic, configuring the VLAN number or the IP address of the VLAN ensures that the relay will function even if a server address changes.

Configuring NBNS Relay

Each NetBIOS PC has a name unique for its local network. If you are using NetBIOS broadcast queries to resolve names and NetBIOS clients are located in different groups or VLANs, you should configure UDP relay for NBNS.

The relays are enabled from the UDP Relay Configuration screen and are configured in similar ways. The UDP Relay Configuration screen is displayed using the **relayc** command described in *UDP Relay Configuration Screen* on page 31-3. To enable the NBNS relay, enter **2=y**. (To enable the NBDD relay, enter see *Configuring NBDD Relay* on page 31-16.)

The UDP Relay Configuration screen redisplay similar to the following:

```

UDP Relay Configuration
1) BOOTP/DHCP Enabled           : Yes
  11) Server Address{list/add/delete} : UNSET
  12) Forward Delay              : 3
  13) Maximum Hops               : 4
2) NBNS Enabled                 : Yes
  21) Next-hop Address {list/add/delete} : UNSET
  22) Forward to VLANs {list/add/delete} : UNSET
3) NBDD Enabled                 :No
4) +Generic Services Menu

```

Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw) :

Either a Next-hop Address *or* a Forward to VLANs value must be configured for the relay.

Next-hop Address

Use this parameter to list, add, or delete the server address(es) to which the NBNS UDP relay will forward. The default is **UNSET**. The value redisplay as **SET** when at least one address is configured. Up to 8 addresses may be configured. You can list, add, or delete addresses by entering **21=l**, **21=a**, or **21=d** on the command line.

Forward to VLANs

Use this parameter to list, add, or delete VLANs to which the NBNS UDP relay will forward. This default is **UNSET**. This value redisplay as **SET** when at least one VLAN is configured. Up to 32 VLANs may be configured. You can list forwarding VLANs, or add or delete VLANs from the forwarding list by entering **22=l**, **22=a**, or **22=d** on the command line. Entries marked with an asterisk indicate the VLANs to which the relay will forward.

Next-Hop Addresses for NBNS

At least one next-hop address (or a forwarding VLAN as described in *Forwarding VLANs for NBNS Relay* on page 31-15) must be configured.

To *add* a next-hop address for NBNS relay:

1. On the UDP Relay Configuration screen command, enter the following:

21=l

A screen similar to the following displays:

FORWARD TO Server List		
Item	Server address	Server Name (if known)
1)	172. 28. 5.212	

Enter IP address or host name of server to be added to list ['h' for help/<ret> to exit]:

2. Enter the IP address of the next hop. Enter the address in dotted decimal format (i.e., 198.206.181.12), a hexadecimal address (i.e., 0xc6ceb501). A host name (i.e., system.com) may be entered if the DNS resolver is enabled using the **res** command.

◆ Note ◆

This address may be the unicast address of the server or a subnet broadcast address of the subnet where the server is located. Using a unicast address is not recommended because an NBNS by definition may shift part or all of its responsibility to another node in the network segment.

3. Enter any additional addresses up to a maximum of 8. Press **<Enter>** to return to the UDP Relay Configuration screen.
4. Enter **s** to save the changes.

To *delete* next-hop addresses for the NBNS relay:

1. Enter **22=d** at the command prompt of the UDP Relay Configuration screen. The FORWARD TO Server List displays.
2. Enter the item number that corresponds to the entry that you want to delete. Repeat this step to delete any additional entries.
3. Press **<Enter>** to return to the UDP Relay Configuration screen.
4. Enter **s** to save the changes.

Forwarding VLANs for NBNS Relay

At least one forwarding VLAN (or a next-hop address as described in *Next-Hop Addresses for NBNS* on page 31-14) must be configured for NBNS relay.

To *select* forwarding VLANs for NBNS relay:

1. On the command line of the UDP Relay Configuration screen, enter the following:

22=i

A screen similar to the following displays:

```

Available/Selected VLANS
Item  Group ID:VLAN ID      MASK      IP ADDR
  1)   1:1                255.255. 0. 0    172. 23. 9.105  *
* = selected for forwarding

```

Enter item number of VLAN to be selected ['h'f or help/<ret> to exit] :

2. Enter the item number of the group/VLAN that you want to select. Repeat this step for all the groups/VLANs you want to select.
3. Press **<Enter>** to return to the command line for the UDP Relay Configuration screen.
4. Enter **s** to save the changes.

To *deselect* forwarding VLANs:

1. On the UDP Relay Configuration screen, enter

22=d

The Available/Selected VLANs screen displays.

2. Enter the item number of the group/VLAN that you want to select. Repeat this step for all the groups/VLANs you want to select.
3. Press **<Enter>** to return to the command line for the UDP Relay Configuration screen.
4. Enter **s** to save the changes.

Configuring NBDD Relay

If you want to send NetBIOS datagrams across networks, you should enable the NBDD relay. To enable the NBDD relay, enter **3=y** at the command prompt of the UDP Relay Configuration screen. The screen redisplay is similar to the following:

```

                                UDP Relay Configuration
1) BOOTP/DHCP Enabled           : Yes
   11) Server Address{list/add/delete} : UNSET
   12) Forward Delay              : 3
   13) Maximum Hops               : 4
2) NBNS Enabled                 : Yes
   21) Next-hop Address {list/add/delete} : UNSET
   22) Forward to VLANs {list/add/delete} : UNSET
3) NBDD Enabled                 : Yes
   31) Next-hop Address {list/add/delete} : UNSET
   32) Forward to VLANs {list/add/delete} : UNSET
4) +Generic Services Menu

```

Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw) :

Either a Next-hop Address *or* a Forward to VLANs value must be configured for the relay.

Next-hop Address

Use this parameter to list, add, or delete the server address(es) to which the NBNS UDP relay will forward. The default is **UNSET**. This value redisplay as **SET** when at least one address is configured. Up to 8 addresses may be configured. You can list, add, or delete addresses by entering **31=l**, **31=a**, or **31=d** on the command line.

Forward to VLANs

Use this parameter to list, add, or delete VLANs to which the NBNS UDP relay will forward. This default is **UNSET**. This value changes to **SET** when at least one VLAN is configured. Up to 32 VLANs may be configured. You can list forwarding VLANs, or add or delete VLANs from the forwarding list by entering **32=l**, **32=a**, or **32=d** on the command line. Entries marked with an asterisk indicate the VLANs to which the relay will forward.

Next-Hop Addresses for NBDD

At least one next-hop address (or a forwarding VLAN as described in *Forwarding VLANs for NBDD Relay* on page 31-18) must be configured for the relay.

To *add* a next-hop address for NBDD relay:

1. At the command prompt for the UDP Relay Configuration screen, enter the following:

32=a

A screen similar to the following displays:

```

FORWARD TO Server List
Item      Server address      Server Name (if known)
1)        172. 28.  5.212

```

Enter IP address or host name of server to be added to list ['h' for help/<ret> to exit]:

2. Enter the IP address of the next hop. Enter the address in dotted decimal format (i.e., 198.206.181.12), a hexadecimal address (i.e., 0xc6ceb501). A host name (i.e., system.com) may be entered if the DNS resolver is enabled using the **res** command.

◆ Note ◆

This address may be the unicast address of the server or a subnet broadcast address of the subnet where the server is located. Using a unicast address is not recommended because an NBNS by definition may shift part or all of its responsibility to another node in the network segment.

3. Enter any additional addresses up to a maximum of 8. Press **<Enter>** to return to the UDP Relay Configuration screen.
4. Enter **s** to save the changes.

To *delete* next-hop addresses for the NBDD relay:

1. Enter **32=d** at the command prompt of the UDP Relay Configuration screen. The FORWARD TO Server List displays.
2. Enter the item number that corresponds to the entry that you want to delete. Repeat this step to delete any additional entries.
3. Press **<Enter>** to return to the UDP Relay Configuration screen.
4. Enter **s** to save the changes.

Forwarding VLANs for NBDD Relay

You may select or deselect VLANs to which the NBDD relay will forward. At least one forwarding VLAN (or a next-hop address as described in *Next-Hop Addresses for NBDD* on page 31-17) must be configured for the relay.

To *select* forwarding VLANs for NBDD relay:

1. On the command line of the UDP Relay Configuration screen, enter the following:

32=a

A screen similar to the following displays:

```
Available/Selected VLANS
Item  Group ID:VLAN ID  MASK  IP ADDR
  1)   1:1          255.255. 0. 0  172. 23. 9.105  *
* = selected for forwarding
```

Enter item number of VLAN to be selected [**h** or **f** or **help**/**<ret>** to exit] :

2. Enter the item number of the group/VLAN that you want to select. Repeat this step for all the groups/VLANs you want to select.
3. Press **<Enter>** to return to the command line for the UDP Relay Configuration screen.
4. Enter **s** to save the changes.

To *deselect* forwarding VLANs:

1. On the UDP Relay Configuration screen, enter

32=d

The Available/Selected VLANs screen displays. Asterisks indicate VLANs selected for forwarding.

2. Enter the item number of the group/VLAN that you want to deselect. Repeat this step for all the groups/VLANs you want to deselect.
3. Press **<Enter>** to return to the command line for the UDP Relay Configuration screen.
4. Enter **s** to save the changes.

Generic Service UDP Relay

UDP relay may be configured for generic services. Generic services may include applications such as Trivial File Transfer Protocol (TFTP), Domain Name System (DNS), IEN-116 Name Server. You will need to know the well-known UDP port number if you want to configure these services.

Generic Services Menu

To configure a relay for a generic service, on the command line for the UDP Relay Configuration screen, enter **4**. A menu similar to the following displays:

```
4) +Generic Services Menu
   41) +Modify existing Generic Services Menu
   42) +Delete existing Generic Service Menu
   43) +Add new Generic Service Menu
```

Submenu Command {Item/?/Help/Quit/Redraw} {Redraw} :

Adding a Generic Service

Use the Add new Generic Service Menu to create a new generic service. On the Generic Services Menu, enter **43**. A screen similar to the following displays:

```
43) +Add new Generic Service Menu
   431) Description of new Service      :
   432) Forwarded port                  : UNSET
   433) Next-hop Address {list/add/delete} : UNSET
   434) Forward to VLANs {list/add/delete} : UNSET
```

Command {Item/?/Help/Quit/Done/Redraw} {Redraw} :

The required parameters are Forwarded port, and *either* Next-hop Address *or* Forward to VLANs. A description of the generic service is optional.

The **Done** command on this screen saves the current changes but does not activate the relay. The relay will be reinitialized and activated with the changes when **Save** is entered on the UDP Relay Configuration screen.

Description of new Service

A description of the service you want to configure.

Forwarded port

The corresponding well-known UDP port number for the service. For example, TFTP uses port 69. The default is **UNSET**. When you set this parameter, the relevant port number displays.

Next-hop Address

Use this parameter to list, add, or delete the server address(es) to which the NBNS UDP relay will forward. The default is **UNSET**. Up to 8 addresses may be configured. The value redisplay as **SET** when at least one address is configured. You can list, add, or delete addresses by entering **433=l**, **433=a**, or **433=d** on the command line.

Forward to VLANs

Use this parameter to list, add, or delete VLANs to which the NBNS UDP relay will forward. This default is **UNSET**. This value redisplay as **SET** when at least one VLAN is configured. Up to 32 VLANs may be configured. You can list forwarding VLANs, or add or delete VLANs from the forwarding list by entering **434=l**, **434=a**, or **434=d** on the command line.

To configure a generic service:

1. On the Add new Generic Service menu, enter a description of the generic service. For example:

431=TFTP

2. Enter the relevant UDP port number. For example:

432=69

3. At least one next-hop address must be configured. To add an address, enter:

433=a

The screen displays similar to the following:

FORWARD TO Server List

Item	Server address	Server Name (if known)
------	----------------	------------------------

Enter IP address or host name of server to be added to list ['h' for help/<ret> to exit]:

4. Enter the next-hop address in dotted decimal format (i.e., 198.206.181.12), a hexadecimal address (i.e., 0xc6ceb501). A host name (i.e., system.com) may be entered if the DNS resolver is enabled using the **res** command.
5. When you are finished entering next-hop addresses, press **<Enter>** to return to the prompt for the Add new Generic Services menu.
6. Select any VLANs for the relay to forward to. At the prompt, enter

434=a

A screen similar to the following displays:

Available/Selected VLANs

Item	Group ID:VLAN ID	MASK	IP ADDR	
1)	1:1	255.255. 0. 0	172. 23. 9.105	*

* = selected for forwarding

Enter item number of VLAN to be selected ['h'f or help/<ret> to exit] :

7. Enter the item number of the group/VLAN that you want to select. Repeat this step for all the groups/VLANs you want to select. An asterisk displays next to all selected VLANs.
8. Press **<Enter>** to return to the Add new Generic Services menu. Add any other generic services in this way.
9. Enter **d** to keep the current changes and return to the Generic Services menu. Enter **d** to return to the UDP Relay Configuration screen.
10. Enter **s** to save the changes and reinitialize the relay.

Modifying a Generic Service

Use the Configured Generic Services screen to modify an existing generic service. On the Generic Services Menu, enter **41**. A screen similar to the following displays:

Configured Generic Services					
Item	State	Port Number	Description	Servers/Vlans	
(1)	enabled	80	TFTP	198.172. 5.	4

Enter item number of service to be modified ['h' for help/<ret> to exit] :

The parameters are defined here.

Item

A unique number assigned by the switch to the generic service in the order the services were configured using the Add new Generic Service screen.

State

The current state of the service, enabled or deleted. The service is enabled as soon as it is added using the Add new Generic Service screen.

Port Number

The well-known UDP number configured for the generic service on the Add new Generic Service screen.

Description

The description of the generic service configured on the Add new Generic Service screen.

Servers/Vlans

The servers or VLANs that the relay will forward to.

To modify an existing generic service:

1. On the Configured Generic Services screen, enter the item number of the relevant service. The Modify existing Generic Services Menu displays similar to the following:

```

41) +Modify existing Generic Service Menu
    411) Description of Service being modified : TFTP
    412) Forwarded port                       : 80
    413) Next-hop Address {list/add/delete}   : SET
    414) Forward to VLANs {list/add/delete}   : SET
  
```

Command {Item/?/Help/Quit/Done/Redraw} {Redraw} :

2. Modify any of the parameters in the same way you configured them (described in *Adding a Generic Service* on page 31-19).
3. Enter **d** to keep the current changes and return to the Generic Services Menu. (The relay will not be initialized with the changes until you save them on the UDP Relay Configuration screen.)

4. Enter **d** to return to the UDP Relay Configuration screen.
5. Enter **s** to save the changes and reinitialize the relay.

Deleting a Generic Service

To delete a generic service:

1. On the Generic Services Menu, enter **42**. The Configured Generic Services screen displays similar to the following:

Configured Generic Services				
Item	State	Port Number	Description	Servers/Vlans
(1)	enabled	80	TFTP	198.172. 5. 4

Enter item number of service to be deleted [**h** for help/<ret> to exit] :

The parameters are defined in *Modifying a Generic Service* on page 31-21.

2. Enter the item number of the service you want to delete. A message similar to the following displays:

Are you sure you want to delete item 1? [**y/n**] (n) :

3. Enter **y** to delete the service. The Configured Generic Services screen redisplay with the State parameter changed to **deleted**. At this point, the service is marked for deletion but has not actually been deleted from the configuration.

Configured Generic Services				
Item	State	Port Number	Description	Servers/Vlans
(1)	deleted	80	TFTP	198.172. 5. 4

Enter item number of service to be deleted [**h** for help/<ret> to exit] :

4. Select any other services to be marked for deletion. Press **<Enter>** to return to the Generic Services Menu.
5. Enter **q** to return to the UDP Relay Configuration screen.
6. Enter **s** to save the changes and delete the selected service(s).

Viewing UDP Relay Statistics

Use the **relays** command to display statistics about configured UDP relays. The **relays** command is listed in the IP submenu. For information about other IP commands, see Chapter 30, “IP Routing.”

The screen display for UDP statistics is similar to the following:

UDP RELAY PACKETS RECEIVED/TRANSMITTED						
SERVICE	PORT	PKTS RCVD	RCV RATE(pkts/s)	PKTS XMTD	XMT RATE(pkts/s)	
1	67/68	0	0.000	0	0.000	
2	137	6	0.010	0	0.000	

NOTE: Rates are average number of packets/s since last query.
Time since last query: 0 days, 0 hours, 10 minutes, 6 seconds.

UDP RELAY TRANSMIT PACKETS DISCARDED					
SERVICE	RVC PORT	DEST VLAN/SVR		PKTS	
1	67/68	172. 28.	5. 21	0	
1	67/68	198.172.	34. 2	0	
1	67/68	198.172.	34. 5	0	
2	137	172. 23.	9.105	6	
2	137	172. 28.	5.212	6	

The fields are defined here.

SERVICE. The number assigned by the switch to the UDP service, in order that the services were configured.

PORT. The well-known UDP port number associated with the type of service. For example, BOOTP/DHCP is 67/68. This number is manually configured for generic services.

PKTS RCVD. The total number of packets received by the relay for the indicated service.

RCV RATE(pkts/s). The average rate, in packets per second, that packets were received for the indicated service since the last time the **relays** command was entered.

PKTS XMTD. The total number of packets transmitted from the relay for the indicated service.

XMT RATE(pkts/s). The average rate, in packets per second, that packets were transmitted for the indicated service since the last time the **relays** command was entered.

RVC PORT. The UDP port number associated with the service

DEST VLAN/SVR. The IP address of the VLANs to which the indicated relay is forwarding. Forwarding VLANs are configurable for each type of relay.

PKTS. The number of packets forwarded to the indicated VLAN.

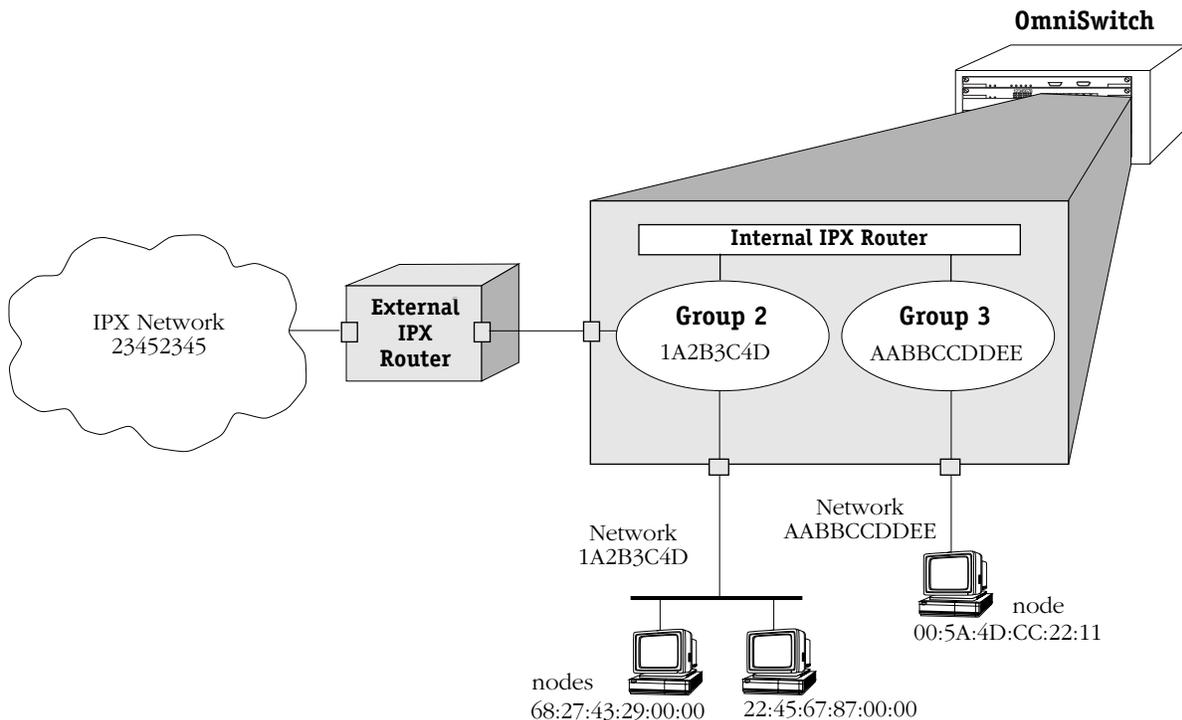
32 IPX Routing

Introduction

This chapter gives an overview of Internetwork Packet Exchange (IPX) routing and includes information about configuring static IPX routes as well as configuring Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) filters and timers. IPX is a layer 3 protocol developed by Novell for interconnecting NetWare clients and servers. (NetWare is Novell's network server operating system.) IPX routing requires at least one IPX router port to be configured on the switch.

When IPX routing is enabled on the switch, the switch will be able to exchange routing information with IPX routers in the network, and stations connected to groups and VLANs with virtual IPX router ports will be able to communicate. Groups or VLANs that do not have IPX router ports with IPX routing enabled cannot communicate with each other.

In the example shown here, stations connected to each group will be able to communicate if a virtual IPX router port is created for each group and each router port on the switch has IP routing enabled. Stations in group 2 and group 3 will also be able to communicate with stations attached to the external IPX router if a static route to that router is configured on the switch or the switch learns about the external router through IPX RIP or SAP.



IPX Routing Overview

In IPX routing, the switch builds routing tables to keep track of optimal destinations for traffic it receives that is destined for remote IPX networks. The switch sends and receives routing messages, or advertisements, to/from other routers in the network. When the switch receives an IPX packet, it looks up the destination network number in its routing table. If the network is directly connected to the switch, the switch also checks the destination node address. The network number consists of eight hex digits, and the node address is typically the MAC address of the end station or server.

Creating routing tables is performed by switch software unless a Hardware Routing Engine (HRE) or HRE-X is installed. The HRE or HRE-X significantly improves routing performance. See Chapter 1, “Omni Switch/Router Chassis and Power Supplies,” and Chapter 6, “The MPM,” for information about the HRE-X and HRE respectively.

IPX is associated with additional protocols built into the switch software. These are described in the next section.

IPX Protocols

The switch supports the following IPX protocols:

- **SPX** (Sequenced Packet Exchange) is a Transport-layer protocol that provides a reliable end-to-end communications link by managing packet sequencing and delivery. SPX does not play a direct role in IPX routing; it simply guarantees the delivery of routed packets.
- **IPX RIP** (Routing Information Protocol) is a layer 3 protocol used by NetWare routers to exchange IPX routing information. IPX RIP functions similarly to IP RIP. IPX RIP uses two metrics to calculate the best route: hop count and ticks. An IPX router periodically transmits packets containing the information currently in its own routing table to neighboring IPX RIP routers in order to advertise the best route to an IPX destination.
- **SAP** (Service Advertising Protocol) is a layer 3 protocol used by NetWare routers to exchange IPX routing information. SAP is similar in concept to IPX RIP. Just as RIP enables NetWare routers to exchange information about routes, SAP enables NetWare devices to exchange information about available network services. NetWare workstations use SAP to obtain the network addresses of NetWare servers. IPX routers use SAP to gather service information and then share it with other IPX routers.

Setting Up IPX Routing on the Switch

IPX routing is enabled on a per-port basis by creating a virtual IPX router port for a group/VLAN. The switch does not do any routing unless the virtual IPX router port has IPX routing enabled (routing is enabled by default). The steps for setting up IPX routing on the switch are given here:

Step 1. Configuring a Virtual Router Port

A virtual IPX router port may be created when you set up or modify a group/VLAN through the **crgrp** command or **modvl** command described in Chapter 24, “Managing Groups and Virtual Ports.” To create a virtual router port, you enable IPX routing and specify a network address for the router port.

◆ **Note** ◆

IP and IPX routing may be enabled on the same port.

IPX router ports on the switch must also be configured with a particular encapsulation type for Ethernet: 802.3, 802.2 or LLC, SNAP, or Ethernet II.

Step 2. Configuring Optional IPX Routing Parameters

Optional configuration for IPX routing includes the following:

- Static routes. These are routes that are manually added to the routing table and may be used rather than dynamic routes that are learned through RIP or SAP.
- IPX RIP and SAP filters. IPX RIP and SAP filters may be configured and displayed. The default timers for RIP and SAP may also be modified. Extended RIP and SAP packets may also be configured.

The IPX Submenu

The **ipx** command in the Networking menu is used to access a submenu containing all the IPX-related commands. For more information about the Networking menu, see Chapter 30, “IP Routing.”

To display the IPX submenu, enter the following commands:

```
IPX
?
```

If you have enabled the verbose mode, you don't need to enter the question mark (?).

A screen similar to the following displays:

Command	IPX Menu
ipxr	View IPX routes
ipxs	View IPX stats and errors
ipxsap	View IPX SAP bindery
aipxsr	Add an IPX static route
ripxsr	Remove an IPX static route
ipxoff	Turn off the IPX router complex
ipxon	Turn on the IPX router complex
ipxflush	Flush IPX router RIP and/or SAP tables
ipxping	IPX Ping a system
ipxfilter	Add/delete an IPX RIP/SAP filter
ipxf	Display IPX RIP/SAP filters
ipxserialf	Enable/Disable IPX Serialization Packet Filtering
ipxspooof	Enable/Disable IPX Watchdog Spoofing
spxspooof	Enable/Disable SPX Keepalive Spoofing
ipxtype20	Turn on/off forwarding of IPX Type 20 packets
ipxtimer	Add/Delete SAP and RIP timers
ipxt	Display SAP and RIP timers
ipxdrt	Turn on/off a default route for IPX
ipxext	Turn on/off extended IPX RIP and SAP packets

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

This chapter describes all of the above commands. The remaining sections of this chapter cover each of the above commands in the order in which they appear in the IPX submenu.

Viewing the IPX Routing Table

The `ipxr` command is used to display the IPX Routing Table. The entries in the table show the routes entered by the IPX RIP protocol and the static routes that you may have entered manually. All entries in the table are sorted by destination network. The IPX Routing Table can contain a maximum of 2,010 routes.

Displaying All Entries in the IPX Routing Table

To display all entries in the IPX Routing Table, enter the following command:

```
ipxr
```

A screen similar to the following displays:

Displaying all (4) routes:

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL
3333	e8024.0000c021a5b8	1	3	N	Y	N	N	N	7:1
5555	5555.Direct	0	1	N	N	N	N	Y	4:1
e8024	e8024.Direct	0	1	N	N	N	N	Y	7:1
3041c204	e8024.0000c021a5b8	1	3	N	Y	N	N	N	7:1

The fields on this screen have the following meanings:

Dest Net

The destination network IPX address.

Router

The IPX address (network.node) of the next hop router to reach the destination network.

Hops

The number of routers between this node and the destination network.

Delay

The number of “ticks” between this node and the destination network. A “tick” is about 1/18th of a second.

Static

Whether this route was statically defined (see the `aipxsr` command).

Aged

Indicates if this route has timed out. Once a route times out it is kept in the routing table for 10 “ticks.” Once the 10 “ticks” expire, the route is deleted.

Redir

Indicates that a route to an IPX network that was formerly reachable via a direct interface has been replaced by an alternate route.

Viewing the IPX Routing Table

Chg

The information in this route has recently been updated, but the new information has not yet been forwarded to neighbor routers.

Dir

Indicates that this is a local interface (direct route) as opposed to a route to a destination network.

GP:VL

The first number is the Group associated with this entry; the second number is the VLAN associated with this entry. This identifies the interface used when sending traffic to the destination network.

Using IPXR with Frame Relay or ISDN Boards

The following additional column heading appears in the `ipxr` display when a Frame Relay or ISDN board is installed in the switch:

s/p/vc or Peer ID

The Slot, Port and Virtual Connection (i.e., DLCI) identifiers or the PPP Peer ID of the interface on which the routing information was received.

Here is an example of a display generated by the `ipxr` command in this situation:

Displaying all (12) routes:

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL	s/p/vc Peer ID
100	100.Direct	0	1	N	N	N	N	Y	3:1	
120	120.Direct	0	1	N	N	N	N	Y	4:1	
5000	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/100
5556	8484.0020da2200f4	1	2	N	N	N	N	N	6:1	P1
8484	8484.Direct	0	1	N	N	N	N	Y	6:1	
26dc012a	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/220
55555555	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/100
66666666	66666666.Direct	0	1	N	N	N	N	Y	5:1	
95000095	120.0020da092ef5	2	3	N	N	N	N	N	4:1	5/3/100

In this example, traffic destined for Network 5000 will go through Slot 5, Port 3, DLCI 100 which is associated with the interface on Group 4.

Displaying a List of Specific IPX Routes

You can limit the number of routes that are displayed by the `ipxr` command by using an extra argument along with the command. To find out if a route to a particular destination network is known, simply include the network number on the command line. (The examples shown below came from a switch that contained a Frame Relay board and an ISDN board.)

Here is an example for destination network 5000 (the command used is: `ipxr 5000`):

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL	s/p/vc
5000	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/100

To display only those routes learned from a particular interface, you can specify the interface number on the command line. You can also further specify the slot/port/vc or PPP Peer ID.

This is an example for Interface 3:1 (the command used was: `ipxr 3:1`):

Displaying routes for interface 3:1

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL	s/p/vc
100	100.Direct	0	1	N	N	N	N	Y	3:1	

This is an example for Interface 4:1 5/3/100 (the command used was: `ipxr 4:1 5/3/100`):

Displaying routes for interface 4:1

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL	s/p/vc
5000	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/100
55555555	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/100
95000095	120.0020da092ef5	2	3	N	N	N	N	N	4:1	5/3/100

This is an example for Interface 6:1 P1 (the command used was: `ipxr 6:1 P1`):

Displaying routes for interface 6:1

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL	s/p/vc
5556	8484.0020da2200f4	1	2	N	N	N	N	N	6:1	P1

Viewing IPX Statistics

The **ipxs** command is used to display data on IPX statistics and errors.

To display information about IPX statistics and errors, enter the following command:

```
ipxs
```

A screen similar to the following displays:

IPX Statistics and Errors:

IPX is ON

IPX Input Statistics:

```
pkts rcvd           = 3280
pkts delivered locally = 3161
pkts discarded      = 0
input header errors  = 0
```

IPX Output Statistics:

```
pkts sent           = 4731
pkts generated locally = 4681
pkts discarded      = 0
pkts with no route found = 1
HRE pkts sent       = 0
```

There are 2 IPX interfaces defined.

Stats for IPX Router Interface on (Group:VLAN) 3:1, Net address 3333

Interface name is IPX Router 3333

```
state           = ON           status      = UP
state changes   = 1500        type        = BROADCAST
rtr encapsulation = FD
```

RIP is ON: sent = 1527, rcvd = 1568, update interval = 60 secs.

SAP is ON: sent = 1, rcvd = 1568, update interval = 60 secs.

Stats for IPX Router Interface on (Group:VLAN) 4:1, Net address 5555

Interface name is IPX Router 5555

```
state           = ON           status      = UP
state changes   = 1500        type        = BROADCAST
rtr encapsulation = EN
```

RIP is ON: sent = 1571, rcvd = 1, update interval = 60 secs.

SAP is ON: sent = 1533, rcvd = 1, update interval = 60 secs.

The fields (and the subfields) on this screen have the following meanings:

IPX

Indicates whether IPX routing is “ON” or “OFF.”

IPX Input Statistics

pkts rcvd: The number of packets received.

pkts delivered locally: The number of received packets delivered to local IPX applications (RIP and SAP).

pkts discarded: The number of discarded packets.

input header errors: The number of packets discarded due to IPX packet header errors.

IPX Output Statistics

pkts sent: The number of packets forwarded (not including fast path routed packets).

pkts generated locally: The number of packets forwarded that were generated by local IPX applications (RIP and SAP).

pkts discarded: The number of discarded packets.

pkts with no route found: The number of packets that could not be forwarded because a route to the destination IPX network could not be found.

Stats for IPX Router Interface

state: State of the IPX router for this interface (ON or OFF).

status: Status of the interface (UP or DOWN).

type: The type of interface (BROADCAST or POINT-TO-POINT).

rtr encapsulation: Router port encapsulation used for this interface (EN=Ethernet, FD=FDDI, TR=Token Ring).

state changes: The number of state changes that have occurred on this interface (up to down, down to up).

RIP

sent: The number of RIP packets sent.

received: The number of RIP packets received.

update interval: The RIP update timer interval for this interface. If a WAN interface is configured as a Triggered RIP/SAP interface, this field will contain the word "triggered." Triggered interfaces transmit information only once, when the change occurs.

SAP

sent: The number of SAP packets sent.

received: The number of SAP packets received.

update interval: The SAP update timer interval for this interface. If a WAN interface is configured as a Triggered RIP/SAP interface, this field will contain the word "triggered." Triggered interfaces transmit information only once, when the change occurs.

Viewing the IPX SAP Bindery

The **ipxsap** command is used to display a listing of the servers in the SAP Bindery, sorted by server name.

To display a list of SAP servers, enter the following command:

```
ipxsap
```

A screen similar to the following displays:

Displaying all (3) entries in the SAP bindery:

Server Name	Type	Address	Hp	Sckt	GP:VL
Develop	0004	67.000000000001	1	0451	3:1
Finance	026b	67.000000000001	1	0005	2:1
Marketing	0278	67.000000000001	1	4006	2:1

The fields on this screen have the following meanings:

Server Name

The name of the server offering this service.

Type

The service type being offered (as defined by Novell).

Address

The IPX address of this server (network.node).

Hp

The number of networks between this node and the server.

Sckt

The Novell socket number to which this service is attached.

GP:VL

The first number is the Group associated with this entry, and the second number is the VLAN associated with this entry.

Using IPXSAP with Frame Relay or ISDN Boards

The following additional column heading appears in the **ipxsap** display when a Frame Relay or ISDN board is installed in the switch.

s/p/vc or Peer ID

The Slot, Port and Virtual Connection (i.e., DLCI) identifiers or the PPP Peer ID of the interface on which the server information was received.

Here is an example of a display generated by the **ipxsap** command in this situation:

Displaying all (3) entries in the SAP bindery:

Server Name	Type	Address	Hp	Sckt	GP:VL	s/p/vc Peer ID
HR	0004	200.000000000022	1	0451	3:1	5/3/100
Sales	026b	200.000000000022	1	0005	2:1	5/3/220
Support	0278	200.000000000022	1	4006	2:1	5/3/220

Displaying a List of Specific SAP Servers

You can limit the number of SAP server names that is displayed by the **ipxsap** command by using an extra argument with the command.

To display only those servers from a specific interface, simply include the interface number on the command line. The following is an example for Interface 2:1 (the command used was **ipxsap 2:1**):

Displaying all SAPs for interface 2:1:

Server Name	Type	Address	Hp	Sckt	GP:VL
Finance	026b	67.000000000001	1	0005	2:1
Marketing	0278	67.000000000001	1	4006	2:1

To display a specific type of server, simply include a Server Type value (in hex) on the command line. The following is an example for 26b (the command used was **ipxsap 26b**):

Displaying SAP entries of type 0x26b:

Server Name	Type	Address	Hp	Sckt	GP:VL
Finance	026b	67.000000000001	1	0005	2:1

To find out if a particular server is known, simply include all, or just a portion of, the server name on the command line. The server name (or portion thereof) must be entered inside of quotation marks. The following is an example for an entry of "nance" (the command used was **ipxsap "nance"**):

Displaying SAP entries whose names contain the substring "nance":

Server Name	Type	Address	Hp	Sckt	GP:VL
Finance	026b	67.000000000001	1	0005	2:1

Adding an IPX Static Route

The **aipxsr** command is used to add IPX static routes to the switch's IPX Routing Table. You might want to add a static route to send traffic from a node in an OmniSwitch VLAN to an external IPX network address (such as an address reached through an external network router attached to the switch).

In order to add a static route, you will need to know the host/net and the gateway which will be used to route traffic there.

Follow the steps below to add an IPX static route.

1. Enter **aipxsr**.

A screen similar to the following displays:

Do you want to see the current route table? (y or n) (y) :

2. Enter **y** at this prompt (or press **<Enter>**) to display the current routing table.

A screen similar to the following displays:

Displaying all (4) routes:

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL
3333	e8024.0000c021a5b8	1	3	N	Y	N	N	N	7:1
5555	5555.Direct	0	1	N	N	N	N	Y	4:1
e8024	e8024.Direct	0	1	N	N	N	N	Y	7:1
3041c204	e8024.0000c021a5b8	1	3	N	Y	N	N	N	7:1

Destination IPX network :

Enter the IPX address of the network to which you are setting up a route.

3. The following prompt displays:

IPX network of next hop :

Enter the IPX network address of the next hop. This is the number that appears before the dot under the "Router" heading in the IPX Route Table.

4. The following prompt displays:

IPX node address of next hop (format - xx:xx:xx:xx:xx:xx)

Enter the IPX node address of the next hop.

5. A message will confirm the addition of the static route:

Route successfully added

Removing an IPX Static Route

The **ripksr** command is used to remove IPX static routes from the switch's IPX Routing Table. Follow the steps below to remove an IPX static route.

1. Enter **ripksr**.

A screen similar to the following displays:

```
Do you want to see the current route table?
(y or n) (y) : y
```

2. Enter **y** at this prompt (or press **<Enter>**) to display the current routing table.

A screen similar to the following displays:

```
Displaying all (4) routes:
```

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL
3333	e8024.0000c021a5b8	1	3	N	Y	N	N	N	7:1
5555	5555.Direct	0	1	N	N	N	N	Y	4:1
e8024	e8024.Direct	0	1	N	N	N	N	Y	7:1
3041c204	e8024.0000c021a5b8	1	3	N	Y	N	N	N	7:1
aaaaaa	304.0020da05f694	1	1	Y	N	N	Y	N	7:1

```
Destination IPX network :
```

3. Enter the name of the destination IPX network you want to remove.

A message will confirm the deletion of the static route:

```
Route successfully deleted.
```

Turning the IPX Router Complex On and Off

The **ipxoff** command is used to turn off the IPX Router Complex, which disables IPX routing on the switch.

To turn off IPX routing, enter the following command:

```
ipxoff
```

A screen similar to the following displays:

```
IPX turned off.
```

The **ipxon** command is used to turn on the IPX Router Complex, which enables IPX routing on the switch.

To turn on IPX routing, enter the following command:

```
ipxon
```

A screen similar to the following displays:

```
IPX turned on.
```

Flushing the IPX RIP/SAP Tables

The **ipxflush** command is used to flush the IPX RIP Routing and SAP Bindery Tables.

Follow the steps below to flush both the IPX tables.

1. Enter **ipxflush**.

A screen similar to the following displays:

```
Flush tables (RIP routing and SAP bindery) in:  
{ RIP and SAP(b),  
  RIP only(r),  
  SAP only(s)} (b) :
```

2. Enter **b** (or just press Enter) to flush both tables. Enter **r** to flush just the Routing Table.
Enter **s** to flush just the SAP Bindery Table.

You will be returned to the system prompt.

Using the IPXPING Command

The **ipxping** command is used to test the reachability of certain types of IPX nodes. The software supports two different types of IPX pings:

- Novell-defined, which can test the reachability of NetWare servers currently running the NetWare Loadable Module called IPXRTR.NLM. This type *cannot* be used to reach NetWare workstations running IPXODI. Novell uses a unique type of ping for this purpose (implemented by their IPXPNG.EXE program) which is not currently supported by the switch software. Other vendors' switches may respond to this type of ping.
- Alcatel-proprietary, which can test the reachability of OmniSwitches or Omni Switch/Routers on which IPX routing has been enabled.

Network devices that do not recognize the specific type of IPX ping request sent from the switch will not respond at all. The lack of a response does not necessarily mean that a specific network device is inactive or missing. Therefore, you might want to try using both types before concluding that the network device is "unreachable."

◆ Note ◆

The **ipxping** command does not work over FDDI trunking with Token Ring SNAP or LLC encapsulation. It does work with Token Ring SNAP or LLC encapsulation over other media types.

Follow the steps below to issue an IPX ping request.

1. Enter **ipxping**.

A screen similar to the following displays:

Dest Net () : 304

Enter the Destination Network of the node that you want to ping.

2. The following prompt displays:

Dest Node (format - xx:xx:xx:xx:xx:xx) () : 00:20:da:05:f6:94

Enter the Destination Node that you want to ping.

◆ Note ◆

If you are attempting to ping an interface that is specified with a noncanonical address, you must specify a noncanonical address for the ping.

3. The following prompt displays:

Count (0 for infinite) (1) : 245

Enter a number to indicate the number of packets to be sent out. An entry of 0 (zero) will create an infinite count (press **<Enter>** to cancel). The default count is 1 (one).

4. The following prompt displays:

Size (64) :

Enter a number to indicate the number of data bytes included in the packet. The default size is 64.

5. The following prompt displays:

Timeout (1) :

Enter the number of seconds to wait for a response. The default timeout is 1.

6. The following prompt displays:

Type (n for Novell, x for Xylan) (n) :

Enter the type of IPX ping to be issued. The default is the Novell type.

7. After answering the previous prompt, a message similar to the following displays:

**IPX Ping starting, hit <RETURN> to stop
PING 304.00:20:da:05:f6:94: 64 data bytes**

```
[0      ] .....  
[50     ] .....  
[100    ] .....  
[150    ] .....  
[200    ] .....
```

**---304.00:20:da:05:f6:94 IPXPING Statistics---
245 packets transmitted, 245 packets received, 0% packet loss**

You may also elect to bypass the above prompts. To do so, simply include the options on the command line in the exact order in which they appear in the prompts. You will be prompted for any options you leave out. Therefore, the syntax for the command is:

ipxping [destnet] [destnode] [count] [size] [timeout] [type]

For example, the following command string will send 100 Novell-type pings, using 64 data bytes per packet with a timeout of 1 second, to an IPX server with MAC address of 00:00:c0:21:a5:b8 on IPX network e8024:

ipxping e8024 00:00:c0:21:a5:b8 100 64 1 n

Configuring IPX RIP/SAP Filtering

The `ipxfilter` command is used to add or delete an IPX RIP or SAP Output or Input filter. The IPX RIP/SAP Filtering feature give you a means of controlling the operation of the IPX RIP/SAP protocols. By using IPX RIP/SAP filters, you can minimize the number of entries put in the IPX RIP Routing and SAP Bindery Tables, improve overall network performance by eliminating unnecessary traffic, and control users' access to NetWare services.

Five types of IPX RIP/SAP filters are available:

1. **RIP Input** filters control which networks are allowed into the routing table when IPX RIPs are received.
2. **RIP Output** filters control the list of networks included in routing updates sent out an interface. These filters control which networks the router advertises in its IPX RIP updates.
3. **SAP Input** filters control the SAPs received by the router prior to a router accepting information about a service. The router will filter all incoming service advertisements received before accepting information about a service.
4. **SAP Output** filters control which services are included in SAP updates sent by the router. The router applies the SAP output filters prior to sending SAP packets.
5. **GNS Output** filters control which servers are included in the GNS responses sent by the router.

Here are some example uses of IPX RIP/SAP filters:

- RIP Input and Output filters can be used to isolate entire network segments (and/or routers) in order to make the network appear differently to the different segments.
- RIP Input and Output filters can be used to reduce the amount of WAN traffic needed to advertise routes that shouldn't be used by a particular network segment.
- SAP Input and Output filters can be used to improve the performance of IPX in a WAN environment by limiting the amount of SAP traffic. For example, because printing is generally a local operation, there's no need to advertise print servers to remote networks. A SAP filter can be used in this case to restrict "Print Server Advertisement" SAPs.

◆ Important Note ◆

All types of IPX Filters can be configured either to *allow* or to *block* traffic. The default setting for all filters is to allow traffic. Therefore, you will typically only have to define a filter to block traffic. However, defining a filter to allow certain traffic may be useful in situations where a more generic filter has been defined to block the majority of the traffic. For example, you could use a filter to allow traffic from a specific host on a network where all other traffic has been blocked. A discussion of the precedence of "Allow" filters appears later in this section. Keep in mind that precedence applies only to "allow" filters, *not* to "block" filters.

You can apply filters to *all* router interfaces by defining a "global" filter, or you can limit the filter to *specific* interfaces. In addition, for WAN networks, you can apply filters to a specific Frame Relay virtual circuit (DLCI) or PPP Peer. Each of these options is described under individual heading in this section.

Adding a “Global” IPX RIP/SAP Filter

Follow the steps below to add a “global” IPX RIP or SAP filter.

1. Enter **ipxfilter**.

A screen similar to the following displays:

Selecting global IPX filter:

Add or delete entry {add(a), delete(d)} (a) :

Enter **a** (or just press **<Enter>**) to select to add a filter.

2. The following prompt displays:

**Filter type {SAP output(so),
SAP input(si),
RIP Output(ro),
RIP Input(ri),
GNS output(go)} (so) :**

Enter **so** (or just press **<Enter>**) to add a SAP Output filter. Enter **si** to add a SAP Input filter. Enter **ro** to add a RIP Output filter. Enter **ri** to add a RIP Input filter. Enter **go** to add a GNS Output filter.

3. The following prompt displays:

Filter action {block(b), allow(a)} (a) :

Enter **a** (or press **<Enter>**) to define the filter to allow traffic. Enter **b** to define the filter to block traffic.

4. The following prompt displays:

IPX network (default: all networks):

Enter the IPX network address (in hexadecimal format) that is to be used (or press **<Enter>** to use the default of “all networks”).

5. The following prompt displays:

IPX network mask (default: FFFFFFFF) :

Enter the IPX network mask (in hexadecimal format) to be used (or press **<Enter>** to use the default mask of FFFFFFFF). *If you selected the default of “all networks” in the previous step, this step is skipped.*

6. The following prompt displays:

IPX node address (default: all nodes):

Enter the IPX node address (in hexadecimal format) to be used (or press **<Enter>** to use the default of “all nodes”).

7. The following prompt displays:

IPX node mask (default: all F's) :

Enter the IPX node mask (in hexadecimal format) to be used (or just press **<Enter>** to use the default mask of all F's). *If you selected the default of “all nodes” in the previous step, this step is skipped.*

- The following prompt displays:

SAP service type (default: all services) :

Enter the SAP service type (in hexadecimal format) as defined by NetWare (or press **<Enter>** to use the default of all services).

- A message will confirm the addition of the filter:

ipxfilter successfully added

Adding an IPX RIP/SAP Filter for a Specific Group or VLAN

Follow the steps below to add an IPX RIP or SAP Output or Input filter for a specific Group or VLAN.

- Enter the Group and VLAN numbers after the command like this: **ipxfilter 1:1**.

A screen similar to the following displays:

Selecting IPX filter for interface 1:1:

Add or delete entry {add(a), delete(d)} (a) :

Enter **a** (or press **<Enter>**) to select to add a filter.

- The following prompt displays:

**Filter type {SAP output(so),
SAP input(si),
RIP Output(ro),
RIP Input(ri),
GNS output(go)} (so) :**

Enter **so** (or press **<Enter>**) to add a SAP Output filter. Enter **si** to add a SAP Input filter. Enter **ro** to add a RIP Output filter. Enter **ri** to add a RIP Input filter. Enter **go** to add a GNS Output filter.

- The following prompt displays:

Filter action {block(b), allow(a)} (a) :

Enter **a** (or press **<Enter>**) to define the filter to allow traffic. Enter **b** to define the filter to block traffic.

- The following prompt displays:

IPX network (default: all networks):

Enter the IPX network address (in hexadecimal format) that is to be used (or press **<Enter>** to use the default of "all networks").

- The following prompt displays:

IPX network mask (default: FFFFFFFF) :

Enter the IPX network mask (in hexadecimal format) to be used (or just press **<Enter>** to use the default mask of FFFFFFFF). *If you selected the default of "all networks" in the previous step, this step is skipped.*

- The following prompt displays:

IPX node address (default: all nodes):

Enter the IPX node address (in hexadecimal format) to be used (or just press **<Enter>** to use the default of "all nodes").

7. The following prompt displays:

IPX node mask (default: all F's) :

Enter the IPX node mask (in hexadecimal format) to be used (or just press **<Enter>** to use the default mask of all F's). *If you selected the default of "all nodes" in the previous step, this step is skipped.*

8. The following prompt displays:

SAP service type (default: all services) :

Enter the SAP service type (in hexadecimal format) as defined by NetWare (or just press **<Enter>** to use the default of all services).

9. A message will confirm the addition of the filter:

ipxfilter successfully added

Using Filters with Frame Relay or ISDN Boards

If the Group or VLAN you enter (such as 1:1 used in the above example) refers to a WAN interface like Frame Relay or PPP, you'll be asked if you want the filter applied to a specific WAN endpoint.

10. This prompt appears after the previous prompt for "SAP Service Type":

Do you wish to apply this filter to a specific WAN endpoint? (n):

Enter **y** to select to apply this filter to a specific WAN endpoint.

11. The following prompt displays:

Frame Relay VC or PPP Peer {vc(v), peer(p)} (v):

Enter **v** (or just press **<Enter>**) to apply this filter to a Frame Relay Virtual Circuit. Proceed to the next step.

Enter **p** if you want to apply this filter to a PPP Peer. Skip to the last step.

12. If you chose to apply a filter to a Frame Relay VC, this prompt displays:

Slot/port:

Enter the slot and port to which you want to apply this filter (for example, **3/1**).

Enter the VC to which you want to apply this filter.

13. If you chose to apply a filter to a PPP Peer, this prompt displays:

Peer ID:1

Enter the Peer ID to which you want to apply this filter (for example, **1**).

Deleting an IPX RIP/SAP Filter

Follow the steps below to delete an existing IPX RIP or SAP filter.

1. Enter `ipxfilter`.

A screen similar to the following displays:

Selecting global IPX filter:

Add or delete entry {add(a), delete(d)} (a) :

Enter `d` to select to delete a filter.

2. A screen similar to the following displays:

Displaying all filters:

#	Type	Net/Mask	Node/Mask	Svc	Md	GP:VL (s/p/vc) (Peer ID)
1	SAP OUT	67/ffffff	00000000001/ffffffff	ALL	B	global
2	SAP IN	67/ffffff	00000000001/ffffffff	0278	B	1:1
3	RIP IN	67/ffffff			B	global

Entry number to delete? (default: none) : 1

This screen contains a list of the existing IPX RIP/SAP filters. The fields on this screen are described in the next section (see *Displaying IPX RIP/SAP Filters* on page 32-23).

3. Enter the index number of the filter you want to delete. If you decide at this point that you want to abort out of the deletion process, simply press `<Enter>` to accept the default of "none."
4. A message will confirm the deletion of the filter:

`ipxfilter successfully deleted.`

Displaying IPX RIP/SAP Filters

The `ipxf` command is used to display a list of all existing IPX RIP and SAP filters. See *Adding a "Global" IPX RIP/SAP Filter* on page 32-19 for complete information on creating these filters. You can enter optional parameters with the `ipxf` command to display specific filters.

Displaying a List of All IPX Filters

To display a listing of all existing IPX RIP and SAP filters, enter the following command:

```
ipxf
```

A screen similar to the following displays:

Displaying all filters:

#	Type	Net/Mask	Node/Mask	Svc	Md	GP:VL (s/p/vc) (Peer ID)
1	SAP OUT	67/ffffff	00000000001/ffffffff	ALL	B	global
2	SAP IN	67/ffffff	00000000001/ffffffff	0278	B	1:1
3	RIP IN	67/ffffff			B	global
4	SAP IN	All Networks	All Nodes	ALL	B	3:1 (P1)

This screen contains a list of the existing IPX RIP and SAP filters. The fields on this screen have the following meanings.

#
The index number assigned to identify each filter.

Type
The type of filter. The five types are: RIP IN, RIP OUT, SAP IN, SAP OUT, and GNS OUT.

Net/Mask
The IPX network address to be filtered ("All networks" means all networks are filtered).

Node/Mask
The IPX node address to be filtered ("All nodes" means all nodes are filtered). This field does not apply to RIP IN or RIP OUT filters.

Svc
The SAP service type (shown as a hexadecimal number) on which the filter is applied, as defined by Novell. By default, all services will be filtered. (Note: This field does not apply to RIP IN or RIP OUT filters.)

Md
The Mode of operation for the filter: A to Allow, B to Block.

GP:VL (s/p/vc) or (Peer ID)

The first number (**GP**) is the Group associated with this entry. The second number (**VL**) is the VLAN associated with this entry. When a filter applies to all interfaces, this field will say “global.” If an entry refers to a Frame Relay interface, column headings for slot, port, and virtual circuit (**s/p/vc**) may be displayed when the filter is applied to a particular virtual circuit rather than to the entire VLAN. If an entry refers to a PPP interface, the Peer ID (**Peer ID**) may be displayed when the filter is applied to a particular PPP Peer.

Displaying a List of “Global” IPX Filters

To display a listing of just the global IPX filters, enter the following command:

```
ipxf global
```

A screen similar to the following displays:

Displaying global filters:

#	Type	Net/Mask	Node/Mask	Svc	Md	GP:VL (s/p/vc) (Peer ID)
1	SAP OUT	67/ffffff	000000000001/ffffffff	ALL	B	global
3	RIP IN	67/ffffff			B	global

Displaying a List of Specific IPX Filters

To display a listing of IPX RIP or SAP filters for a specific interface, you can specify other parameters along with the **ipxf** command. The format for the command in this case is:

```
ipxf <type> <GP:VL>
```

The type is one of these codes:

ri	for RIP INput
ro	for RIP OUTput
si	for SAP INput
so	for SAP OUTput
go	for GNS OUTput

For example, to display a list of the filters defined for Group 1, VLAN 1, you would enter:

```
ipxf 1:1
```

A screen similar to the following displays:

Displaying filters for interface 1:1:

#	Type	Net/Mask	Node/Mask	Svc	Md	GP:VL (s/p/vc) (Peer ID)
2	SAP IN	67/ffffff	000000000001/ffffffff	0278	B	1:1

As another example, to display a list of all global RIP Input filters, you would enter:

```
ipxf ri global
```

A screen similar to the following displays:

Displaying all global RIP INPUT filters:

#	Type	Net/Mask	Node/Mask	Svc	Md	GP:VL (s/p/vc) (Peer ID)
3	RIP IN	67/ffffff			B	global

IPX RIP/SAP Filter Precedence

Whenever you use multiple “allow” filters you must first define a filter to block all RIPs or SAPs. Then, all of the seceding “allow” filters of the same type must be *at least* as specific in all areas in order for the filters to work. Note that filtering precedence is related only to “allow” filters. Multiple “block” filters can be defined with varying specificity in each of the areas of the filter. The filtering done by the configurable parameters (Net/Mask, Node/Mask, Service/Mode) in the “allow” filter must be at least as specific as the filtering defined in the “block” filter.

As an example, consider a switch that knows of multiple Type 4 SAPs on various networks, including a network with an address of “40.” The switch also knows of various types of SAPs on Network 40. For this example, you want to block all SAPs coming from Network 40, but you want to allow all Type 4 SAPs, including the ones that come from Network 40.

To meet these objectives, you must configure the filters like this:

#	Type	Net/Mask	Node/Mask	Svc	Md	GP:VL
1	SAP IN	40/ffffff	all nodes	ALL	B	global
2	SAP IN	40/ffffff	all nodes	4	A	global

The filters shown below will *not* work for our example because in Filter 2 the type of service is *less* specific than the type defined in Filter 1. All Type 4 SAPs will be blocked by the filter.

#	Type	Net/Mask	Node/Mask	Svc	Md	GP:VL
1	SAP IN	All networks	all nodes	4	B	global
2	SAP IN	40/ffffff	all nodes	ALL	A	global

The following filters will also *not* work because in Filter 2 the network and netmask are *less* specific than the network and netmask defined in Filter 1. All SAPs from Network 40 will be blocked by the filter.

#	Type	Net/Mask	Node/Mask	Svc	Md	GP:VL
1	SAP IN	40/ffffff	all nodes	ALL	B	global
2	SAP IN	All networks	all nodes	4	A	global

Configuring IPX Serialization Packet Filtering

The **ipxserialf** command is used to enable and disable IPX Serialization Packet filtering on any or all WAN routing services. This feature can be used to reduce traffic on WAN links by preventing the transmission of NetWare serialization packets.

Novell uses a serialization mechanism to make sure that licensed copies of NetWare are not improperly copied to multiple servers. NetWare's built-in copy protection scheme transmits serialization packets between file servers which contain unique serialization numbers. These packets are sent out at about 66-second intervals. If a server detects duplicate serialization identifiers, it broadcasts a copyright violation message to all users and to the console log. The major problem with this protection scheme for dial-on-demand links, such as ISDN, is the generation of traffic that continuously reactivates the WAN link.

Enabling IPX Serialization Filtering

Follow the steps below to enable IPX Serialization Packet Filtering.

1. Enter **ipxserialf**.

A screen similar to the following displays:

View the current status of all WAN routing services? (y or n) (n) :

Enter **y** if you do want to see the current filtering status. Enter **n** (or press **<Enter>**) if you entered this command by mistake or if you don't need to see the current status.

2. A screen similar to the following displays:

<u>Group</u>	<u>IPX Serialization Filtering</u>
3	Disabled
4	Disabled

Enter Group (default: all WAN) :

This screen shows the WAN routing Groups that exist in the switch and the current status of the IPX Serialization packet filtering for these groups.

Enter a Group number to proceed to enable IPX Serialization filtering for that Group.

Or, press **<Enter>** to select to enable filtering for *all* WAN routing services.

3. The following prompt displays:

Enable IPX Serialization Filtering? (y or n) (n) :

Enter **y** to select to enable IPX Serialization Filtering.

Enter **n** (or press **<Enter>**) if you do *not* want to enable Serialization Filtering.

4. The following prompt displays:

Enable IPX Serialization Filtering on all WAN routing services? (y or n) (n) :

This prompt requires you to verify that you want to enable filtering in order to avoid the situation of accidental filtering of IPX Serialization packets. This example prompt asks if you want to disable filtering on all WAN routing services. If you had entered a specific Group number, the prompt would refer to that particular Group.

Enter **y** to enable IPX Serialization Filtering.

5. Filtering will then become active. A message will appear indicating that IPX Serialization Filtering is enabled, either on all WAN routing services or for a specific Group:

IPX Serialization Filtering is now enabled on all WAN routing services

Disabling IPX Serialization Filtering

Follow the steps below to disable IPX Serialization Packet Filtering.

1. Enter `ipxserialf`.

A screen similar to the following displays:

View the current status of all WAN routing services? (y or n) (n) :

Enter **y** if you do want to see the current filtering status. Enter **n** (or press **<Enter>**) if you entered this command by mistake or if you don't need to see the current status.

2. A screen similar to the following displays:

Group	IPX Serialization Filtering
3	Enabled
4	Enabled

Enter Group (default: all WAN) :

This screen shows the WAN routing Groups that exist in the switch and the current status of the IPX Serialization packet filtering for these groups.

Enter a Group number to proceed to disable IPX Serialization filtering for that Group.

Or, just press **Enter** to select to proceed to disable filtering for *all* WAN routing services.

3. The following prompt displays:

Enable IPX Serialization Filtering? (y or n) (n) :

Enter **n** (or press **<Enter>**) to select to disable Serialization Filtering.

4. The following prompt displays:

Disable IPX Serialization Filtering on all WAN routing services? (y or n) (n) :

This prompt requires you to verify that you want to disable filtering. This example prompt asks if you want to disable filtering on all WAN routing services. If you had entered a specific Group number, the prompt would refer to that particular Group.

Enter **y** to disable IPX Serialization Filtering.

5. A message will appear indicating that IPX Serialization Filtering is disabled, either on all WAN routing services or for a specific Group:

IPX Serialization Filtering is now disabled on all WAN routing services

Configuring IPX Watchdog Spoofing

The **ipxspoo** command is used to enable and disable IPX Watchdog Spoofing on any or all WAN routing services. The use of this feature is explained below:

Novell's IPX Watchdog Protocol, which is used by NetWare to maintain network node and server connections, can consume significant network bandwidth and thereby incur costs on expensive dial-on-demand, pay-per-packet WAN links. The OmniSwitch provides an IPX Watchdog Spoofing feature to prevent Watchdog packets from initiating connections on WAN links in situations where no other data is ready to be transferred.

The IPX Watchdog Spoofing feature enables the switch to respond to a NetWare server's Watchdog "Query" requests on behalf of a remote client, thus spoofing the requests. The spoofing action occurs when the switch "sees" an incoming Watchdog packet destined for an interface on which spoofing has been enabled. The switch responds to the server by sending out a valid Watchdog response. Spoofing thus maintains the required Watchdog function while avoiding the cost of making and maintaining a WAN link.

In some situations, the use of the IPX Watchdog Spoofing feature can make a NetWare server "believe" that an inactive session is still active. This occurrence can cause connectivity problems by denying login rights to legitimate users. Therefore, if you use the spoofing feature on networks that also limit the number of IPX or SPX sessions, you should utilize NetWare's "auto-logoff" function to minimize inappropriate denials of legitimate logins.

Enabling IPX Watchdog Spoofing

Follow the steps below to enable IPX Watchdog Spoofing.

1. Enter **ipxspoo**.

A screen similar to the following displays:

View the current spoofing status of all WAN routing services? (y or n) (n) :

Enter **y** if you do want to see the current IPX spoofing status. Enter **n** (or just press **Enter**) if you entered this command by mistake or if you don't need to see the current status.

2. A screen similar to the following displays:

Group	IPX Spoofing
3	Disabled
4	Disabled

Enter Group (default: all WAN) :

Enter a Group number to proceed to enable IPX spoofing for that particular Group.

Or, just press **Enter** to proceed to enable IPX spoofing for *all* WAN routing services.

3. The following prompt displays:

Enable Spoofing? (y or n) (n) :

Enter **y** to proceed to enable IPX spoofing.

4. The following prompt displays:

Enable IPX Spoofing on all WAN routing services? (y or n) (n) : y

This prompt requires you to verify that you want to enable spoofing in order to avoid the situation of accidental spoofing of IPX packets.

This example prompt asks if you want to enable spoofing on all WAN routing services. If you had entered a specific Group number, the prompt would refer to that particular Group.

Enter **y** to enable IPX Watchdog Spoofing.

- IPX Spoofing will then become active. A message will appear indicating that IPX Watchdog Spoofing is enabled, either on all WAN routing services, or for a specific Group:

IPX Spoofing is now enabled on all WAN routing services

Disabling IPX Watchdog Spoofing

Follow the steps below to disable IPX Watchdog Spoofing.

- Enter **ipxspoo**.

A screen similar to the following displays:

View the current spoofing status of all WAN routing services? (y or n) (n) :

Enter **y** if you do want to see the current IPX spoofing status. Enter **n** (or just press **<Enter>**) if you entered this command by mistake or if you don't need to see the current status.

- A screen similar to the following displays:

Group	IPX Spoofing
3	Enabled
4	Enabled

Enter Group (default: all WAN) :

Enter a Group number if you want to disable IPX spoofing for that particular Group.

Or, press **<Enter>** to disable IPX spoofing for *all* WAN routing services.

- The following prompt displays:

Enable Spoofing? (y or n) (n) :

Enter **n** (or just press **<Enter>**) to proceed to disable IPX spoofing.

- The following prompt displays:

Disable IPX Spoofing on all WAN routing services? (y or n) (n) : y

This prompt requires you to verify that you want to disable spoofing. This example prompt asks if you want to disable spoofing on all WAN routing services. If you had entered a specific Group number, the prompt would refer to that particular Group.

Enter **y** to disable IPX Watchdog Spoofing.

- IPX Spoofing will then become inactive. A message will appear indicating that IPX Watchdog Spoofing is disabled, either on all WAN routing services, or for a specific Group:

IPX Spoofing is now disabled on all WAN routing services

Configuring SPX Keepalive Spoofing

The `spxspoof` command is used to enable and disable SPX Keepalive Spoofing on any or all WAN routing services. The use of this feature is explained below:

Novell's SPX Keepalive Protocol, which is used by NetWare to maintain SPX connections between end nodes, can also consume significant network bandwidth and thereby incur unnecessary costs on expensive dial-on-demand, pay-per-packet WAN links. The OmniSwitch provides a SPX Keepalive Spoofing feature to prevent keepalive packets from keeping WAN links active when they are not otherwise needed for data transmissions.

The SPX Spoofing feature enables the switch to respond to client/server keepalive packets on the behalf of the remote clients/servers. SPX spoofing thereby effectively stops keepalive packets from crossing a WAN link while maintaining existing SPX connections.

SPX-Packet Tolerance Counting

NetWare's SPX and SPXII watchdog and keepalive packets unfortunately are not labeled with a unique packet type. Therefore, valid acknowledge packets or window-update packets could be mistaken for keepalive packets. To prevent blocking of critical packets, a packet tolerance counting mechanism is employed by the Spoofing feature to count SPX packets.

When active, the Spoofing feature observes all watchdog and keepalive packets as they go between network endpoints. If successive packets are found to have the same sequence number, acknowledge number, and "alloc" number, spoofing will not begin until the specified SPX-packet tolerance count has been reached. Only watchdog packets which have the ACK_REQUESTED bit set will have an effect on the SPX-packet tolerance counter.

Once the specified tolerance count has been reached, spoofing of watchdog packets will begin and all keepalive packets will be dropped. Refer to *Controlling IPX Type 20 Packet Forwarding* on page 32-32 for help on using NetWare's configurable parameters to change the frequency and number of keepalive/watchdog packets sent.

Enabling SPX Keepalive Spoofing

Follow the steps below to enable SPX Keepalive Spoofing.

1. Enter `spxspoof`.

A screen similar to the following displays:

View the current spoofing status of all WAN routing services? (y or n) (n) :

Enter **y** if you do want to see the current SPX spoofing status. Enter **n** (or press **<Enter>**) if you entered this command by mistake or if you don't need to see the current status.

2. A screen similar to the following displays:

<u>Group</u>	<u>SPX Spoofing</u>
3	Disabled
4	Disabled

Enter Group (default: all WAN) :

Enter a Group number to proceed to enable SPX spoofing for that particular Group.

Or, press **<Enter>** to proceed to enable SPX spoofing for *all* WAN routing services.

3. The following prompt displays:

Enable Spoofing? (y or n) (n) :

Enter **y** to proceed to enable spoofing.

- The following prompt displays:

Enable SPX Spoofing on all WAN routing services? (y or n) (n) : y

This prompt requires you to verify that you want to enable spoofing in order to avoid the situation of accidental spoofing of SPX packets. This example prompt asks if you want to enable SPX spoofing on all WAN routing services. If you had entered a specific Group number, the prompt would refer to that particular Group.

Enter **y** to enable spoofing.

- SPX Spoofing will then become active. A message will appear indicating that SPX Spoofing is enabled, either on all WAN routing services, or for a specific Group:

SPX Spoofing is now enabled on all WAN routing services

Disabling SPX Keepalive Spoofing

Follow the steps below to disable SPX Keepalive Spoofing.

- Enter **spxspoof**.

A screen similar to the following displays:

View the current spoofing status of all WAN routing services? (y or n) (n) :

Enter **y** if you do want to see the current SPX spoofing status. Enter **n** (or press **<Enter>**) if you entered this command by mistake or if you don't need to see the current status.

- A screen similar to the following displays:

Group	SPX Spoofing
3	Enabled
4	Enabled

Enter Group (default: all WAN) :

Enter a Group number to proceed to disable SPX spoofing for that particular Group.

Or, just press **<Enter>** to proceed to disable SPX spoofing for *all* WAN routing services.

- The following prompt displays:

Enable Spoofing? (y or n) (n) :

Enter **n** to proceed to disable spoofing.

- The following prompt displays:

Disable SPX Spoofing on all WAN routing services? (y or n) (n) : y

This prompt requires you to verify that you want to disable spoofing in order to avoid the situation of accidental spoofing of SPX packets. This example prompt asks if you want to disable SPX spoofing on all WAN routing services. If you had entered a specific Group number, the prompt would refer to that particular Group.

Enter **y** to disable spoofing.

- SPX Spoofing will then become inactive. A message will appear indicating that SPX Spoofing is disabled, either on all WAN routing services, or for a specific Group:

SPX Spoofing is now disabled on all WAN routing services

Controlling IPX Type 20 Packet Forwarding

The `ipxtype20` command is used to control the forwarding of IPX Type 20 packets. The default setting is to *not* forward IPX Type 20 packets. You can use the `ipxtype20` command to explicitly enable the forwarding of Type 20 packets for individual interfaces routing IPX traffic.

Type 20 packets contain the value 20 (14 hex) in the “packet type” field of the IPX header. Novell has defined the use of these packets to support certain protocol implementations, such as NetBIOS. As these packets are broadcasted and propagated across networks, the addresses of those networks (up to 8) are stored in the packet’s data area.

The reason why forwarding of Type 20 packets is normally “off” is that they can cause problems in highly redundant IPX networks by causing what appears to be a broadcast storm. This problem is aggravated whenever misconfigured PCs are added to a network.

Follow the steps below to enable IPX Type 20 packet forwarding on a given interface.

1. Enter `ipxtype20`.

A screen similar to the following displays:

```
Do you want to see the status of IPX Type 20 packet forwarding?  
(y or n) (y) :
```

2. Enter a **y** at this prompt (or press **<Enter>**) to display the current handling of IPX Type 20 packets on all configured IPX interfaces.

A screen similar to the following displays:

```
GP:VL   Type20 Packet Forwarding  
-----  
3:1     off  
4:1     off
```

```
group:vlan () :
```

3. Enter the Group and VLAN numbers associated with the IPX interface for which you wish to enable Type 20 packet forwarding. For example, you could enter **3:1**.

A screen similar to the following displays:

```
Currently, Group 3:Vlan 1 has IPX Type 20 packet forwarding off.  
“on” or “off” (off) :
```

4. Enter **on** to turn IPX Type 20 packet forwarding “on” for this interface. The default is “off”.

A screen similar to the following displays:

```
IPX Type 20 packet forwarding on 3:1 has been changed to on.
```

You may also elect to bypass the above prompts. To do so, simply include the Group and/or VLAN number and the word “on” (or “off”) as part of the command line.

For example, to turn forwarding “on” for Group 4, VLAN 1, enter `ipxtype20 4 on`.

A screen similar to the following displays:

```
IPX Type 20 packet forwarding on 4:1 has been changed to on.
```

If you enter the `ipxtype20` command with options for an interface that is not configured for IPX, a message similar to the following will appear:

```
Group 1:Vlan 1 isn't configured for IPX.
```

```
Usage: ipxtype20 [group:vlan] [on | off]
```

Configuring NetWare to Minimize WAN Connections

If you have access to NetWare's control parameters, you can "fine-tune" your network to minimize traffic on WAN links such as ISDN connections or Frame Relay lines. Doing so will reduce the costs associated with each connection that is made. Some suggested approaches are described below.

1. NetWare Directory Services (NDS), included in NetWare 4.x, includes a time synchronization protocol. By default, NetWare servers send time synchronization packets every 10 minutes. To help cut down on unnecessary connections that result from the time synchronization protocol, you could load the NLM (NetWare Loadable Module) named TIME-SYNC.NLM onto your NetWare time servers. This NLM will allow you to modify the update interval of the time synchronization packets.
2. NDS also introduces more traffic in order to maintain replicas of NDS partitions. The NLMs named DSFILTER.NLM and PINGFILT.NLM can be used to modify NDS synchronization updates.
3. NetWare's IPX Watchdog protocol monitors the connection status of NetWare clients and transmits reports when a connection fails to respond. You could modify the following three Watchdog parameters on your NetWare file servers to help cut down the costs associated with the IPX protocol:
 - SET NUMBER OF WATCHDOG PACKETS (the default is 10, range is 5 to 100 packets).
 - SET DELAY BETWEEN WATCHDOG PACKETS (the default is 59.3 seconds, range is 9.9 seconds to 10 minutes and 26.2 seconds).
 - SET DELAY BEFORE FIRST WATCHDOG PACKET (the default is 4 minutes 56.6 seconds, range is 15.7 seconds to 20 minutes and 52.3 seconds).
4. There are two basic categories of timeouts which can cause extra network traffic and/or loss of SPX connections:
 - If a data packet goes unacknowledged, it is re-transmitted a certain number of times before the connection is aborted.
 - When a connection is idle and the SPX Watchdog is enabled, system packets are sent periodically, and if not eventually acknowledged, the connection is aborted.
5. The following parameters can be modified in the NET.CFG file to determine when packets should be resent or when connections should be aborted:
 - MINIMUM SPX RETRIES determines how many unacknowledged transmit requests are allowed before assuming the connection has failed.
 - SPX VERIFY TIMEOUT determines how often (in ticks) the SPX protocol sends a packet to the other side of a connection to indicate that it is still alive.
 - SPX LISTEN TIMEOUT specifies how long (in ticks) the SPX protocol waits without receiving a packet from the other side of the connection before it requests the other side to send a packet to ascertain whether the connection is still valid.
 - SPX ABORT TIMEOUT specifies how long (in ticks) the SPX protocol waits without receiving any response from the other side of the connection before it terminates the session.

6. Novell has developed a workaround that can be used to disable the SPX Watchdog mechanism. This workaround could be used instead of enabling the SPX Spoofing feature on your switch. SPWXDOG.NLM is a patch that is used to disable NetWare's SPX Watchdog mechanism on 3.x and 4.x servers. The patch adds the following file server set parameter:

“set spx watchdogs=ON/OFF” (The default is ON.)

To fully disable SPX Watchdog packets, the remote client/server should also disable Watchdogs. IPXODI v3.02 and IPX.NLM support a NET.CFG parameter to disable SPX Watchdogs (“spx watchdog=off”).

Configuring RIP and SAP Timers

The standard time between broadcasts of RIP and SAP messages is 60 seconds. This default may be modified in order to alleviate network congestion or facilitate the discovery of network resources.

Adding a RIP and SAP Timer

1. To adjust the time between RIP and SAP messages, enter the following command at the system prompt:

```
ipxtimer
```

The following prompt displays:

```
Add or delete entry {add(a), delete(d)} (a) :
```

2. Enter **a** and the following prompt displays:

```
Group: (global) : 1
```

3. Enter the group number or leave the field blank and press Enter. If you do not enter a group number, the SAP and RIP timers will be adjusted for all groups on the switch.

The following prompt displays:

```
RIP timer (1..180 secs): (60) :
```

4. Enter the desired value or press **<Enter>** to configure the default value, which is 60 seconds. The following prompt displays:

```
SAP timer (1..180 secs): (60) :
```

5. Enter the desired value or press **<Enter>** to configure the default value, which is 60 seconds. The following message displays:

```
ipxtimer successfully added
```

Viewing RIP and SAP Timers

To view the RIP and SAP timers that have been configured through the **ipxtimer** command, enter the following command:

```
ipxt
```

A screen similar to the following displays:

#	Group	RIP Timer (secs)	SAP Timer (secs)
1	1	30	15
2	global	45	45

The fields are defined as follows:

Group

Displays the group number or **global** to indicate all groups.

RIP Timer (secs)

Displays the RIP timer configured for the group using the **ipxtimer** command.

SAP Timer (secs)

Displays the SAP timer configured for the group using the **ipxtimer** command.

Configuring Extended RIP and SAP Packets

Larger RIP and SAP packets may be transmitted so that congestion in the network is reduced. Other switches and routers in the network must support larger packet size if this feature is configured on the switch.

Use the **ipxext** command to enable or disable extended packets or to view the current status of extended packet transmission.

Enabling or Disabling Extended RIP and SAP Packets

To enable larger RIP and SAP packets, enter the following command:

```
ipxext on
```

To disable larger RIP and SAP packets, enter the following command:

```
ipxext off
```

Viewing the Current Status of Extended Packets

To display the current status of this feature, enter the following command:

```
ipxext
```

When the feature is disabled (the default), the following message displays:

```
IPX extended RIPs and SAPs off
```

When the feature is enabled, the following message displays:

```
IPX extended RIPs and SAPs on
```

Configuring an IPX Default Route

A default IPX route may be configured for packets destined for networks unknown to the switch. If RIP messages are disabled, packets can still be forwarded to a router that knows where to send them. Use the **ipxdrtr** command to add a default route, view the status of a default route, or disable the default route.

Adding an IPX Default Route

To configure a default route, use the **ipxdrtr** command with the relevant network ID. For example:

```
ipxdrtr 222
```

If the network ID indicates a direct network on the switch, the MAC address must also be specified, and the following prompt will display:

```
IPX node address of next hop (format - xx:xx:xx:xx:xx:xx) :
```

Enter the relevant address.

Viewing the Status of an IPX Default Route

To view the status of the default route, enter the **ipxdrtr** command. A message similar to the following displays:

```
IPX default route: 00000222 00:20:da:99:88:77
```

Disabling an IPX Default Route

To disable the default route, enter the following:

```
ipxdrtr off
```

If you enter the **ipxdrtr** command again, the following message displays:

```
IPX default route is disabled
```

33 Managing ATM Access Modules

ATM access, or uplink, ports allow switch traffic to connect to a native ATM network. In typical configurations, LAN traffic from Ethernet or Token Ring devices is translated and switched out an ATM access port to an ATM-based network. (An ATM-based network is comprised of pure ATM switches, such as OmniSwitches with Cell Switching Modules (CSMs) installed.)

You can configure several services on these ATM access ports to facilitate communication between the access port and an ATM switched port. These services include LAN Emulation, Classical IP, and Point-to-Point bridging. The configuration of these services is described in Chapter 36, “Configuring ATM Services.”

ATM access modules include all ASM modules, ATM circuit emulation modules (ASM-CE), and FCSM modules on the OmniSwitch and all ASX modules on the Omni Switch/Router. ATM access modules provide OC-3, OC-12, DS3, and E3 User-to-Network (UNI) connections that typically attach to an ATM switch. An ATM switch, such as an OmniSwitch with Cell Switching Modules (CSMs), also supports UNI connections, but can also support Private Network-to-Network Interface (PNNI) and Interim Interswitch Signalling Protocol (IISP) connections.

This chapter provides overview information and configuration instructions for ATM access ports. It focuses on the ATM layer configuration parameters, specifically for OC-3 and OC-12 ATM access ports. The OmniSwitch also supports ATM DS-3 and E3 access ports. However the configuration of ATM DS-3 and E3 access ports is covered in more detail Chapter 54, “Managing DS3/E3 Modules.” The following are modules containing ATM access ports:

ATM DS3/E3 Ports. ATM DS3 and E3 modules require different port configuration procedures than the directions in this chapter. These ports have a separate menu for physical-level parameters. This menu is described in Chapter 54, “Managing DS3/E3 Modules.”

Circuit Emulation Modules. Only the ATM uplink port on a circuit emulation module is an ATM access port. Instructions for configuring that port are in this chapter. Instructions for configuring other ports on the ASM-CE can be found in Chapter 34, “Managing Circuit Emulation Modules.”

FCSM Access ports. See *FCSM ATM Access Ports* on page 33-5.

CSM Ports. CSM ports support pure ATM switching traffic. These ports connect ATM switches together and can connect to ATM access ports, such as those on ATM access modules. CSM ports are described in Chapters 40 through 47.

Three Generations of Modules

In Release 3.0 a second generation of ATM access modules was released that uses an advanced Segmentation and Reassembly (SAR) ASIC known as "SAHI." These modules have many improvements over the first generation of ASM modules, including larger transmit and receive buffers, support for non-zero VP, and traffic shaping.

A third-generation ATM access module, the ASX-M-622RF-1W, was released in 4.4 that uses a SAR ASIC known as "Maker." This module provide full-rate OC-12 support and Virtual Channel (VC)-based traffic shaping.

All OmniSwitch and Omni Switch/Router ATM access modules are described in the tables below and on the following pages.

Early Generation OmniSwitch ATM Access Modules

Module	Port Number/Type	Speed Supported (per port)	VC-Based or Bandwidth Allocation Traffic Shaping Supported?	Non Zero VP Supported?
ASM-155F	1 or 2 SC	155 Mbps	No	No
ASM-155C	1 or 2 RJ-45	155 Mbps	No	No
ASM-DS3	1 or 2 BNC	44.736 Mbps	No	No
ASM-E3	1 or 2 BNC	34.368 Mbps	No	No
ASM-CE-155F	5 total: 1 SC 2 T1 or E1 2 serial	SC: 155 Mbps T1:1.544 Mbps E1: 2.048 Mbps Serial: 56 - 2048 Kbps	No	No
ASM-CE-DS3	5 total: 1 DS3 2 T1 or E1 2 serial	DS3: 44.736 Mbps T1:1.544 Mbps E1: 2.048 Mbps Serial: 56 - 2048 Kbps	No	No
ASM-CE-E3	5 total: 1 E3 2 T1 or E1 2 serial	E3: 34.368 Mbps T1:1.544 Mbps E1: 2.048 Mbps Serial: 56 - 2048 Kbps	No	No
FCSM-I	2 logical (not physical) ports	155 Mbps	No	No

SAHI-Based ATM Access Modules

Module (Chassis)	Port Number/Type	Speed Supported (per port)	VC-Based or Bandwidth Allocation Traffic Shaping Supported?	Non Zero VP Supported?
ASM2-155F (OmniSwitch)	1 or 2 SC	155 Mbps	Bandwidth Allocation	Yes
ASM2-155RF (OmniSwitch)	1 or 2 SC port pairs (each port pair acts as one port)	155 Mbps	Bandwidth Allocation	Yes
ASM2-622F (OmniSwitch)	1 or 2 SC	622 Mbps	Bandwidth Allocation	Yes
ASM2-622RF (OmniSwitch)	1 or 2 SC port pairs (each port pair acts as one port)	622 Mbps	Bandwidth Allocation	Yes
ASM2-DS3 (OmniSwitch)	1 or 2 BNC	44.736 Mbps	Bandwidth Allocation	Yes
ASM2-E3 (OmniSwitch)	1 or 2 BNC	34.368 Mbps	Bandwidth Allocation	Yes
FCSM II (OmniSwitch)	1 logical (not physical) port	622 Mbps	Bandwidth Allocation	Yes
ASX-155FM/FS/FH (Omni Switch/Router)	1 or 2 SC	155 Mbps	Bandwidth Allocation	Yes
ASX-155RFM/RFS-1W (Omni Switch/Router)	1 SC port pair (the port pair acts as one port)	155 Mbps	Bandwidth Allocation	Yes
ASX-DS3 (Omni Switch/Router)	1 or 2 BNC	44.736 Mbps	Bandwidth Allocation	Yes
ASX-E3 (Omni Switch/Router)	1 or 2 BNC	34.368 Mbps	Bandwidth Allocation	Yes
ASX-622RFM/RFS-1W (Omni Switch/Router)	1 SC port pair (the port pair acts as one port)	622 Mbps	Bandwidth Allocation	Yes

Omni Switch/Router Maker-Based ATM Access Modules

Module	Port Number/Type	Speed Supported (per port)	VC-Based or Bandwidth Allocation Traffic Shaping Supported?	Non Zero VP Supported?
ASX-M-622RF-1W	1 SC port pair (the port pair acts as one port)	622 Mbps	VC-Based	Yes

FCSM ATM Access Ports

Although the FCSM does not contain any physical ports, it does contain an internal ATM access port that can be viewed and configured through switch software. This port is functionally the same as an ASM module port. However, instead of connecting to an ATM switch through cable, this logical port is hardwired into the ATM cell matrix.

You can view statistics and configure ATM services, such as LAN Emulation and Classical IP, on this internal port. By creating ATM services on this port, you provide a bridge between devices on LAN interfaces (Ethernet, Token Ring) and those connected to the native ATM network. This FCSM logical port would display as port 1 for the slot in which the FCSM port is installed. For example, if the FCSM is installed in slot 3, then this uplink port would display as port **3/1**.

This internal ATM access port is directly connected to an OC-3c/STM-1 (FCSM I) or OC-12c/STM-4c (FCSM II) port that is functionally the same as a CSM port. Logically, these two ports are two halves of the same port; User Interface software displays them as part of the same port.

In some command displays you may also note that there is a *second* FCSM port on the FCSM I. (The FCSM II has only one internal port.) If the FCSM I were installed in slot 3, this second port would display as port **3/2**. This second internal port also contains an ATM access half and a CSM half. It is used to pass control signals. Unlike the first FCSM port, this second port is only partially configurable (i.e., SAR and frame buffer sizes only). If you increase default buffer sizes on this second port you may place limitations on your ATM configuration.

When you set Quality of Service (QoS) Parameters on an FCSM module with the **cvc** command (described in *Creating a Virtual Channel Connection* on page 33-15) or the **mvc** command (described in *Modifying a Virtual Channel Connection* on page 33-22), you are setting traffic shaping on the ASM side of the internal port *and* setting policing on the CSM side of the port.

The following table summarizes the functions of each FCSM port:

FCSM Ports

	Port 1 (FCSM I)	Port 1 (FCSM II)	Port 2 (FCSM I)
ASM half	ATM Services Port	ATM Services Port and Management Data (ILMI, UNI signaling, PNNI)	Management Data (ILMI, UNI signaling, PNNI)
CSM half	Connects ATM Service Port to Cell Matrix	Connects ATM Service Port to Cell Matrix and Management Data (ILMI, UNI signaling, PNNI)	Management Data (ILMI, UNI signaling, PNNI)

◆ Important Note ◆

Signaling is not supported on non zero VPIs on the FCSM-II.

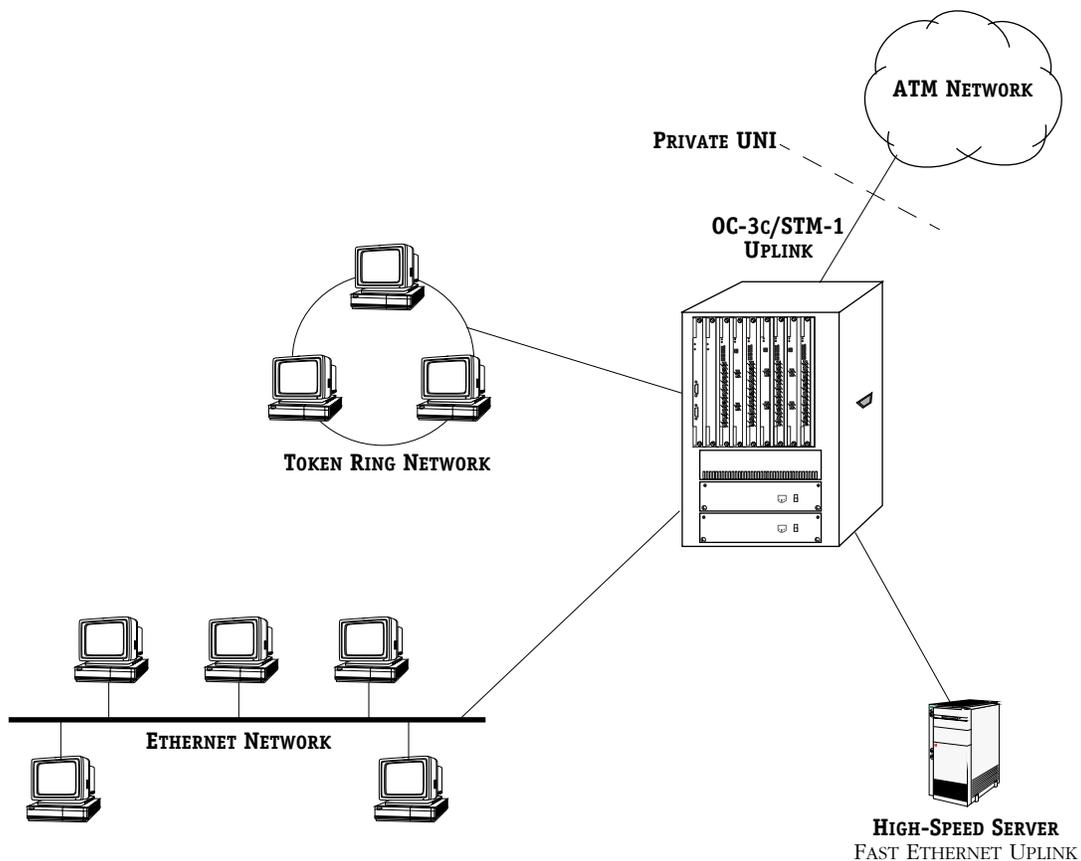
LAN Switch with ATM Uplinks

The OmniSwitch and Omni Switch/Router can switch frames from LAN interfaces such as Ethernet and Token Ring to an ATM-based network. It supports ATM uplink connections that are compatible with User-to-Network (UNI) versions 3.1 and 3.0 to provide comprehensive LAN-to-ATM internetworking. These ATM uplink connections provide connectivity to a native ATM network.

Typically, you will configure services on ATM access ports in order to bridge LAN traffic (Ethernet and Token Ring) onto the ATM network. LAN traffic enters the switch through an Ethernet or Token Ring port and exits through an ATM access port. It is on such an access port that you configure one of several ATM services.

These services include LAN Emulation (LANE), Point-to-Point Bridging (PTOP), Classical IP, Trunking, and VLAN clusters. ATM services may be configured through the **cas** command or, in the case of LANE, they can be brought up on-the-fly through auto-activation. The **cas** command and all ATM service types are described in detail in Chapter 36, "Configuring ATM Services." Auto-activated LANE services are described in Chapter 35, "LANE Server Configuration."

The network in the illustration below shows an OmniSwitch switching traffic for Ethernet, Token Ring, Fast Ethernet, and ATM uplink interfaces. It serves as a LAN switch while having an OC-3 uplink to the ATM network.



OmniSwitch as a LAN-to-ATM Internetworking Device

The ATM Menu

User Interface commands for configuring and monitoring ATM access ports are in the ATM menu. The ATM menu displays as shown below. To view the ATM Menu, type **atm** at any prompt.

Command	ATM Management Menu
vap	View the list of ATM ports configurations
map	Modify an ATM port configuration
vvc	View virtual channel connections
cvc	Create a virtual channel connection
mvc	Modify a virtual channel connection
dvc	Delete a virtual channel connection
vva	View virtual atm addresses
cva	Create a virtual atm address
mva	Modify a virtual atm address
dva	Delete a virtual atm address
vlat	View ATM LANE LE_ARP table
vat	View ATM CIP Arp Table
aat	Add static ATM Arp entry for CIP
dat	Delete static ATM Arp entry for CIP
vss	View ATM Service statistics
vls	View atm layer statistics table
vlrs	View atm layer rx error statistics table
vlts	View atm layer tx error statistics table
vcs	View atm connection statistics table
vcrs	View atm connection rx error statistics table
vcts	View atm connection tx error statistics table
vbwg	View the bandwidth group table
mbwg	Modify the bandwidth group table
vgptovc	View group to VC mapping table (Scaling)
vnac	View current number of atm connections
vnapc	View current number of atm PTOMP connections
atmlsem	Enables or Disables LEC debugs

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

This menu contains commands that can be used with ATM uplink modules, Frame-to-Cell Switching modules (FCSM modules), and Cell Switching Modules (CSM modules). The commands in the menu operate differently for ATM access modules, FCSM modules, and CSM modules.

This chapter describes ATM menu commands as they apply to ATM access ports. The commands are different when used with CSM modules. See Chapter 41, “Managing Cell Switching Modules (CSMs),” for information on how these commands apply to CSM modules.

Several commands apply to the ATM service commands that can be set up on ATM access ports. These commands include those for Classical IP (**vat**, **aat**, **dat**), LAN Emulation (**vlat** and **atmlsem**), 1483 scaling (**vgptovc**), and the **vss** command. These commands are described in Chapter 36, “Configuring ATM Services.”

◆ Important Note ◆

The ASX-M-622RF-1W uses 16-bit counters for ATM Service Data Units (SDUs) on the **vcs**, **vls**, **vcrs**, and **vcts** commands to display SDU statistics. If these counters reach 65536 they will reset to zero (0) and continue counting. This limitation does *not* affect the **vlts** and **vlrs** commands.

Modifying an ATM Access Port Configuration

Use the **map** command to alter ATM access port configuration settings. Ports are configured with default settings until you modify them using the **map** command. To use this command, enter **map** followed by the slot and port number of the ATM access port you want to modify. For example, to change settings for port 1 on the module in slot 5, you would enter:

```
map 5/1
```

A screen similar to the following displays:

Slot 5 Port 1 Configuration

```

1) Description (30 chars max)           : ATM PORT
2) Conn Type { PVC(1), SVC(2)          : SVC

    30) Sig version { 3.0(1) 3.1(2) }   : 3.1
    31) Signaling VCI (0..1023)         : 5
    32) ILMI Enable {(False(1),True(2)) : True
    33) ESI (12 hex-chars)              : 0020da79efbf
    34) ILMI VCI (0..1023)              : 16
    35) ILMI Polling {(Off(1),On(2))    : Off

3) Max VCCs (1-1023)                   : 1023
4) Max VCI bits (5..10)                 : 10
   41) Max VPI bits (0..5 )             : 0
5) UNI Type                             : Private
6) Tx SAR Buffer Size (4096-131072)     : 16384
7) Rx SAR Buffer Size (4096-131072)     : 16384
8) Tx Frame Buffer Size (1800-16384)    : 4600
9) Rx Frame Buffer Size (1800-16384)    : 4600
10) PI Scramble {(False(1),True(2))    : True
11) Timing Mode {(Loop(1),Local(2))    : Local
12) Loopback Config { NoLoop(1), DiagLoop(2),
    LineLoop(3) }                       : NoLoop
13) Phy media { SONET(1),SDH(2)}       : SONET

```

Enter (option=value/save/cancel) : cancel

You change a value in the field by entering the line number for the value, an equal sign (=), and then the new value for the variable. For example, to change the **Description** field variable to read “Switch Uplink Port,” you would enter a **1** (the line number for **Description**), an equal sign, and then the new description as follows:

```
1=Switch Uplink Port
```

The variables in the **map** command screen are explained in the following sections.

Description

A textual description of this ATM access port. The description may be up to 30 characters long. This identifier will be used in displays for other software commands.

Conn Type

Indicates whether connections established on this port will be Permanent Virtual Circuits (PVCs) or Switched Virtual Circuits (SVCs). You create PVCs through the **cvc** command, which is described in *Creating a Virtual Channel Connection* on page 33-15. PVC information is stored in flash memory on the MPM module; if you restart the switch, the PVC would be restored.

Switched Virtual Circuits, or SVCs, are learned by the switch through communication with the ATM attached devices. SVCs are built up and taken down based on demands for virtual connections by ATM end devices. If an SVC connection is lost or the switch is restarted, then the circuit is lost and the source device must request the connection again.

The type of connection you choose can affect the type of ATM services you can set up on a port. For example, LANE requires SVC connections, and VLAN clusters requires PVC connections.

Enter a **1** to select PVC, or enter a **2** to select an SVC.

SVC Configuration Options. If you select SVC, you will see an additional menu of options. The items in this menu are described as follows:

Sig Version

The version of the User-to-Network Interface (UNI) used on this port. The OmniSwitch and Omni Switch/Router are compliant with ATM Forum UNI specifications versions 3.0 and 3.1 (the default). You select which version your ATM network supports. (The signaling version you are using must match the signalling version being used on the network.) To set this port for UNI version 4.0, see *Configuring UNI 4.0 on an ATM Access Port* on page 33-13 for more information.

◆ Important Note ◆

If you change the **Signaling Ver** from UNI 3.0 to UNI 3.1 (or vice versa), then you *must* reboot the switch.

Signalling VCI

The Virtual Channel Identifier (VCI) used for signaling. For ATM access ports, this VCI is typically set to 5. The range is 0 to 1023.

ILMI Enable

Indicates whether you want to enable Integrated Local Management Interface (ILMI). Normally ILMI should be enabled. The only reasons not to enable ILMI are if the ATM network switch does not support ILMI or if the ATM network switch is unable to register the network prefix with the switch in a timely manner. The disadvantage of disabling ILMI is that the ATM network switch needs to have a static route configuration to map the ATM address of the switch port to its port configuration. In this case, you will need to enter the full ATM address instead of just the End Station Identifier (ESI).

ESI

The 6-byte End Station Identifier (ESI) for this port. This value, which functions like a MAC address for this port, is used by the ATM switch to identify this particular ATM access port.

In software releases prior to 4.1, the ESI assigned to each ATM access port used the base MAC address for the module and the slot/port number (e.g., 2/1). This method created a problem if the ATM access module moved between different slots since the ESIs changed because the physical port number changed.

In release 4.1 and later, the method for assigning an ESI changed. The base MAC address is still used, but the interface number is used instead of the slot/port number. If an ATM access module is moved between different slots, the interface number remains the same and thus the ESI is maintained.

With this change, there could be some backward compatibility problems when upgrading to Release 4.1 and later since the ESI of the ATM access ports will change. However, this change will only affect SVC-based PTOp and trunking services since the remote station stores the old ESI in its system. PVC-based services are not affected.

ILMI VCI

The Virtual Channel Identifier (VCI) that will be reserved for ILMI management signaling on this port. The range is 0 to 1023.

ILMI Polling

The ILMI status messages sent out at regular intervals (about every 3-5 seconds) from this port. If you want to enable ILMI polling, select the **On** option. If you want to disable ILMI polling, select the **Off** option. The default value for **ILMI Polling** is **Off**.

Max VCCs

The maximum number of Virtual Channel Connections (VCCs) allowed on this port. This parameter is not configurable; it will always read **1023**. Each port can support up to 1023 virtual connections. You configure these VCCs through the **cvc** command, which is described in *Creating a Virtual Channel Connection* on page 33-15.

Max VCI Bits

The maximum number of bits that can be used for Virtual Channel Identifiers (VCIs) created on this port. The ASX-M-622RF-1W and SAHI-based ATM access modules (described in *SAHI-Based ATM Access Modules* on page 33-3) support 5 to 10 bits per Virtual Channel on each port. This option is *not* configurable on early-generation ATM access modules (described in *Early Generation OmniSwitch ATM Access Modules* on page 33-2). For these modules, this field will always read **10**.

The maximum number of Virtual Channels is 2^n-1 where n is the maximum VCI bits.

◆ Note ◆

The total bits available for VPIs and VCIs is 10 on the ASX-M-622RF-1W and SAHI-based ATM access modules. You can specify how many bits are allotted for VPIs and how many are for VCIs, but the total must be 10 for the ASX-M-622RF-1W and SAHI-based ATM access modules.

Max VPI bits

The maximum number of bits that can be used for Virtual Path Identifiers (VPIs) created on this port. On the ASX-M-622RF-1W and SAHI-based ATM access modules (described in *SAHI-Based ATM Access Modules* on page 33-3), you can set this field to 0 (the VPI will be equal to 0 and all 10 bits will be used for the VCI) or you can configure 1 to 5 bits per Virtual Path on each port. This option is not displayed on Early Generation ATM access modules (described in *Early Generation OmniSwitch ATM Access Modules* on page 33-2) and therefore is *not* configurable on these modules.

If this field is not set to 0, then the maximum number of Virtual Paths is 2^n-1 where n is the maximum VPI bits.

UNI Type

Specifies the type of User-to-Network Interface (UNI) that this port supports. ATM supports both Private and Public UNI connections, but typically Private is used for ATM uplink, or access, connections to an ATM switch. Only **Private** is supported on this port.

Tx SAR Buffer Size and Rx SAR Buffer Size

The size of the segmentation cell buffer (**Tx SAR Buffer Size**) and the reassembly cell buffer (**Rx SAR Buffer Size**) on this UNI. These buffers comprise the entire Segmentation and Reassembly (SAR) buffer for this ATM access port.

◆ Important Note ◆

You *cannot* configure these fields on any Omni Switch/Router ATM access module (including the ASX-M-622RF-1W) or on any OmniSwitch ASM2 module.

On OmniSwitch ASM modules, sizes can range from 4,096 to 131,072 bytes. On OmniSwitch ASM2 and Omni Switch/Router ATM access modules, the size is fixed at 131,072 bytes (128 K).

SAR buffers are located in memory on the ATM board. On ASM modules, this memory can be factory-configured to either 512K or 2MB. On 512K boards, SAR buffer sizes are by default set to 8K. On 2MB boards, SAR buffer sizes are by default set to 16K. If you swap a 512k board for a 2 MB board, then you may need to reconfigure these buffer sizes. In addition, if the board swap changes the port type (e.g., single mode to multimode, OC-3 to DS-3) or the SAR type, then the switch will automatically detect the change and reset the segment size to the default for the new board.

A SAR buffer size of 8K should be sufficient for Ethernet-only connections. Connections to interfaces that use larger packets, such as FDDI and LAN Emulation services, require SAR buffer sizes of at least 16K and probably 32K for best performance.

The number of virtual circuits required should also be considered when choosing the SAR buffer size. The number of virtual connections possible depends on two conditions:

- a. The size of available SRAM (512K or 2 MB). The more memory available, the more connections can be supported.
- b. The size of the Segmentation and Reassembly (SAR) cell buffer (i.e, the value indicated in this field). As the SAR buffer size increases, the number of virtual circuits that can be supported decreases.

◆ Important Note ◆

If you change a SAR buffer size, you need to reboot the switch for the change to take effect

Tx Frame Buffer Size

The size of the transmit frame buffer, or the maximum size of packets that can be transmitted from ATM to the switch backplane. This value can range from 1800 to 131,072 bytes, but must be less than or equal to the **Tx SAR Buffer Size**. This value should be greater than or equal to the **Tx Maximum Frame Size** (set through the **cvc** command) of all connections on this port.

◆ Note ◆

This field is not relevant to the ASX-M-622RF-1W.

Rx Frame Buffer Size

The size of the receive frame buffer on this UNI, or the maximum size of packets that can be received from the switch backplane. This value can range from 1800 to 131,072 bytes, but must be less than or equal to the **Rx SAR Buffer Size** and should be greater than or equal to the **Rx Maximum Frame Size** (set through the **cvc** command) of all connections on this port.

◆ Note ◆

This field is not relevant to the ASX-M-622RF-1W.

Pl Scramble

Payload scramble. This option determines whether chip hardware on the module will perform cell scrambling/descrambling, which randomizes cell payloads. Payload scrambling helps avoid continuous non-variable bit patterns and improves cell delineation. Cell delineation is the process used to determine cell boundaries by finding the Header Error Control (HEC) in cell headers. By default, payload scrambling is enabled as required by UNI specifications.

Timing Mode

This parameter allows you to specify which clock the switch will use for this port. The choices are **Local** and **Loop**. Local is the transmit, or internal, clock. The local clock is generated by this switch; this is the default setting for ATM access ports. Loop is the receive, or external, clock. In a loop configuration, this port derives clocking from a remote device, such as an ATM switch or another Alcatel ATM access port.

Your choice of timing mode may be determined by the device to which this port is connected. Some ATM switches require uplink ports to generate their own clock. Other ATM switches require uplink ports to use their clock.

◆ Note ◆

If you set an ATM access port to **loop** and you are connecting it to another ATM uplink, or access, port (i.e., not a pure ATM switch port), then that other port must be on an Alcatel switch.

Loopback Config

The loopback configuration for this port. In live network situations, use the **NoLoop** option, which is the default. The other two loopback configurations, **DiagLoop** and **LineLoop**, are intended mainly for debugging or test situations. The following provides more detail on the three loopback configurations:

- NoLoop** No loopback occurs between receive and transmission paths.
- DiagLoop** Interface transmission path is connected to receive path at the connectors. The port receives its own transmission rather than the signal coming over the cable.
- LineLoop** The interface receive path is looped to the transmission path at the connectors. The signal on the receive connector is not passed into the UNI and processed.

Phy media

The type of physical media standard used for this port. In North America, ATM broadband services are delivered over Synchronous Optical Network (SONET) facilities. SONET is a high-speed fiber optic system that uses Synchronous Transfer Signal Level 1 (STS-1).

Outside North America, ATM broadband services use Synchronous Digital Hierarchy (SDH). SDH is a high-speed fiber optic system that uses Synchronous Transfer Mode (STM-1). The OmniSwitch and Omni Switch/Router support both SONET and SDH fiber systems. You select the system with which you want this port to be compatible.

Configuring UNI 4.0 on an ATM Access Port

Follow the steps below to configure an ATM access port for UNI 4.0 signaling.

1. Delete the **asm.img** file with the **rm** command and load the **asm_mpg.img** file with the **load** command or through FTP. (The **asm.img** file does not support UNI 4.0 signaling.) For more information on deleting and loading image files, please refer to Chapter 11, “Managing Files.”
2. Add the following line to your command file (**mpm.cmd** on an MPM-1G, **mpx.cmd** on an MPX, **mpmc.cmd** on an MPM-C, or **mpm3.cmd** on an MPM-III):

```
atm_load_mpg=1
```

This line *must* come before the **cmunit** line. (See Chapter 11, “Managing Files,” for more information on editing the command file.)

3. Reboot your switch by using the **reboot** command. (See Chapter 12, “Switch Security,” for more information on the **reboot** command.)
4. Log on to your switch.
5. Enter

```
ui
```

at the CLI prompt to enter the User Interface (UI).

6. Enter **map** followed by the slot and port number you want to configure UNI 4.0 signaling. For example, to configure Port 1 in Slot 2, enter

```
map 2/1
```

at the system prompt. A screen similar to the following will be displayed.

Slot 2 Port 1 Configuration

```
1) Description (30 chars max)           : ATM PORT
2) Conn Type { PVC(1), SVC(2)           : SVC

    30) Sig version { 3.0(1) 3.1(2), 4.0(3) } : 3.1
    31) Signaling VCI (0..1023)           : 5
    32) ILMI Enable {(False(1),True(2))}  : True
    33) ESI (12 hex-chars)                : 0020da79efbf
    34) ILMI VCI (0..1023)                 : 16
    35) ILMI Polling {(Off(1),On(2))}      : Off

3) Max VCCs (1-1023)                     : 1023
4) Max VCI bits (5..10)                   : 10
   41) Max VPI bits (0..5)                 : 0
5) UNI Type                               : Private
6) Tx SAR Buffer Size (4096-131072)       : 16384
7) Rx SAR Buffer Size (4096-131072)       : 16384
8) Tx Frame Buffer Size (1800-16384)      : 4600
9) Rx Frame Buffer Size (1800-16384)      : 4600
10) PI Scramble {(False(1),True(2))}     : True
11) Timing Mode {(Loop(1),Local(2))}     : Local
12) Loopback Config { NoLoop(1), DiagLoop(2),
    LineLoop(3) }                          : NoLoop
13) Phy media { SONET(1),SDH(2)}         : SONET
```

Enter (option=value/save/cancel) : cancel

7. Enter

30=3

at the **map** command prompt to change the signaling to UNI 4.0.

8. Enter any other configuration changes. When you are done, enter

save

at the **map** command prompt to save your settings.

Creating a Virtual Channel Connection

The **cvc** command allows you to create a Permanent Virtual Circuit (PVC) for a physical port and logical VCI that you specify.

◆ Important Note ◆

Although the **cvc** command is supported on ATM access modules, Alcatel recommends that you create your PVC when you create your ATM service with the **cas** command. See Chapter 36, "ATM Services," for more information on the **cas** command.

On early-generation ATM access modules (see *Early Generation OmniSwitch ATM Access Modules* on page 33-2), the syntax is as follows:

```
cvc <slot>/<port> <vci>
```

On the ASX-M-622RF-1W and SAHI-based ATM access modules (see *SAHI-Based ATM Access Modules* on page 33-3), the syntax is as follows:

```
cvc <slot>/<port> [<vpi>/]<vci>
```

If you do not specify a Virtual Path Identifier (VPI) number, then a VPI of 0 will be created.

For example, to create a PVC with a VPI of 1 and a Virtual Channel Identifier (VCI) of 100 on ASX-622FM-1W Port 1 in Slot 2, enter:

```
cvc 2/1 1/100
```

at the system prompt. The initial message will be followed by a screen of options similar to the following:

```
Slot 2 Port 1 Connection VPI 1 VCI 100 Configuration
Available bandwidth: Tx=81056 Rx=81056
1) Description (30 chars max)                : Connection 1/100
2) Tx QoS Class { Unspecified(0) }           : Unspecified
3) TX Best Effort { False (1), True (2) }     : True
4) Tx Traffic Descriptor { NoCLPNoSCR(2) }    : NoCLP NoSCR
   20) Peak Cell Rate (cells/sec) for CLP=0+1 : 81056
5) Rx QoS Class { Unspecified(0) }           : Unspecified
6) RX Best Effort { False (1), True (2) }     : True
7) Rx Traffic Descriptor { NoCLPNoSCR(2) }    : NoCLP NoSCR
   30) Peak Cell Rate (cells/sec) for CLP=0+1 : 81056
14) Tx Maximum Frame Size                    : 4520
15) Rx Maximum Frame Size                    : 4520
Enter (option=value/save/cancel) :
```

The menu options for the **cvc** command are described below.

◆ **Note** ◆

The ASX-M-622RF-1W has additional parameters for traffic shaping. See *Traffic Shaping Parameters for the ASX-M-622RF-1W Module* on page 33-19 for documentation on these parameters.

Description: (30 chars max)

A textual description for this virtual circuit. The description may be up to 30 characters long. This description will be used in displays for other software commands to identify this virtual circuit.

Tx QoS Class

The Quality of Service (QoS) for cells transmitted (from source to destination) on this virtual circuit. For ATM uplink connections to an ATM switch only the **Unspecified** QoS is supported. This QoS transmits data on a best effort basis; bandwidth is not guaranteed, but as much data as possible will be transmitted as long as bandwidth is available.

◆ **Note** ◆

This field is not relevant to the ASX-M-622RF-1W.

Tx Best Effort

This field indicates whether you want this port to transmit traffic on a “best effort” basis or to use a Peak Cell Rate (PCR) parameter to transmit traffic. If you select True (option **2**), then the port will transmit traffic if any bandwidth is available on the port. If you select False (option **1**), then the Peak Cell Rate (PCR) parameter will be used to transmit traffic on this VCC. You enter a PCR value in line 20 of this screen. If data cannot be sent at the PCR you specify, then no data will be sent on the VCC.

◆ **Note** ◆

This field is not relevant to the ASX-M-622RF-1W.

Tx Traffic Descriptor

The traffic descriptor to be used. The traffic descriptor determines which traffic parameters you specify. Only the **NoCLPNoSCR** traffic descriptor is supported. **NoCLPNoSCR** requires you to enter the Peak Cell Rate (PCR) on line 20. However, if you select **True** on line 3 (**Tx Best Effort**), then the PCR will not be used to determine traffic flow, and traffic will be transmitted on a best effort basis.

◆ **Note** ◆

This field is not relevant to the ASX-M-622RF-1W.

Peak Cell Rate (cells/sec) for CLP=0+1

This value is only relevant if you enter **False** on line 3, **Tx Best Effort**. In this field you specify the Peak Cell Rate (PCR), in cells per second, allowed for traffic transmitted on this VCC. The PCR is the fastest cell rate allowed on the connection. When using Peak Cell Rate, the bandwidth of an ATM uplink port can be partitioned among multiple connections, each with a dedicated bandwidth. The ATM driver calculates the best rate nearest to the requested rate that the ATM hardware can support. This rate is shown using the **vvcc** command. The CLP=0+1 in this field means that both high priority (CLP=0) and low priority (CLP=1) cells will be checked for PCR. Chapter 41, “Managing Cell Switching Modules (CSMs),” of this manual contains further information on CLP, which is the acronym for “Cell Loss Priority.”

Rx Qos Class

The Quality of Service (QoS) for cells received (from destination to source) on this virtual circuit. For ATM uplink connections to an ATM switch only the **Unspecified** QoS is supported. This QoS receives data on a best effort basis; bandwidth is not guaranteed, but as much data as possible will be received as long as bandwidth is available.

Rx Best Effort

This field indicates whether you want this port to receive traffic on a “best effort” basis or to use a Peak Cell Rate (PCR) parameter. If you select True (option **2**), then the port will receive traffic if any bandwidth is available on the port. If you select False (option **1**), then the PCR parameter will be used. You enter a PCR value in line 20 of this screen. If data cannot be received at the PCR you specify, then this VCC will not be operational.

◆ **Note** ◆

This option is not available on SAHI-based (see *SAHI-Based ATM Access Modules* on page 33-3) ATM access modules. See *Traffic Shaping (ASM2/ASX Modules)* on page 33-60 for setting traffic shaping on these modules.

RX Traffic Descriptor

The traffic descriptor to be used. Only the **NoCLPNoSCR** traffic descriptor is supported. **NoCLP-NoSCR** requires you to enter the Peak Cell Rate (PCR) on line 20. However, if you select **True** on line 6 (**Rx Best Effort**), then the PCR will not be used to determine traffic flow, and traffic will be received on a best effort basis.

Peak Cell Rate (cells/sec) for CLP=0+1

This value is only relevant if you enter **False** on line 6, **Rx Best Effort**. In this field you specify the Peak Cell Rate (PCR), in cells per second, allowed for traffic received on this VCC. The PCR is the fastest cell rate allowed on the connection. When using PCR, the bandwidth of an ATM uplink port can be partitioned among multiple connections each with dedicated bandwidth. The ATM driver calculates the best rate nearest to the requested rate that the ATM hardware can support. This rate is shown using the **vvcc** command. The CLP=0+1 in this field means that both high priority (CLP=0) and low priority (CLP=1) cells will be checked for PCR.

Tx Maximum Frame Size

The maximum frame size for traffic transmitted on this connection. Frames are composed of ATM cells. You specify the largest possible frame size, in bytes, in the field. If a frame exceeds this size, it will be discarded and counted as an error in statistics tables. The value in this field must be greater than zero (0), but less than the **Tx Frame Buffer Size**, which is specified through the **map** command.

◆ **Note** ◆

This field is not relevant to the ASX-M-622RF-1W.

Rx Maximum Frame Size

The maximum frame size for traffic received on this connection. Frames are composed of ATM cells. You specify the largest possible frame size, in bytes, in the field. If a frame exceeds this size it will be discarded and counted as an error in statistics tables. The value in this field must be greater than zero (0), but less than the **Rx Frame Buffer Size**, which is specified through the **map** command.

◆ **Note** ◆

This field is not relevant to the ASX-M-622RF-1W.

Traffic Shaping Parameters for the ASX-M-622RF-1W Module

The **cvc** command for the ASX-M-622RF-1W module contains additional and modified parameters for VC-based traffic shaping. The syntax is the same as for SAHI-based modules. (See *Creating a Virtual Channel Connection* on page 33-15 for more information.) For example, to create a PVC with a VPI of 1 and VCI of 100 on ASX-M-622RF-1W Port 1 in Slot 2, you would enter

```
cvc 2/1 1/100
```

at the system prompt. A screen similar to the following would be displayed.

Slot 2 Port 1 Connection VPI 1 VCI 100 Configuration

Available bandwidth: Tx=81056 Rx=81056

- | | |
|--|--------------------|
| 1) Description (30 chars max) | : Connection 1/100 |
| 2) Requested Tx QoS Class { Unspecified UBR(0),
Class1 CBR(1), Class3 VBR_RT(3), Class4 VBR_NRT(4)} | : Unspecified |
| 3) Requested TX Best Effort { False (1), True (2) } | : True |
| 4) Requested Tx Traffic Descriptor { NoCLPNoSCR(2),
NoCLPSCR (5) | : NoCLPNoSCR |
| 20) Peak Cell Rate (cells/sec) for CLP=0+1 | : 1412831 |
| 5) Requested Rx QoS Class { Unspecified(0) } | : Unspecified |
| 6) Requested RX Best Effort { False (1), True (2) } | : True |
| 7) Requested Rx Traffic Descriptor { NoCLPNoSCR(2) } | : NoCLP NoSCR |
| 30) Peak Cell Rate (cells/sec) for CLP=0+1 | : 1412831 |

Enter (option=value/save/cancel) :

The additional and modified parameters for the **cvc** command on the ASX-M-622RF-1W are described on the following page. Please refer to *Creating a Virtual Channel Connection* on page 33-15 for all other parameters.

2) Requested TX QoS Class

This field specifies the type of traffic and its priority on this connection. Some traffic types require higher priority than others because any disruption in the connection will cause unacceptable results. For example, voice and video should use Constant Bit Rate (CBR) transport and be given a higher priority than other less time-sensitive traffic. On the other hand, data connections can tolerate some delay in the connection. Data traffic usually requires Unspecified Bit Rate (UBR) transport. UBR is the default value for this option.

The following transport values are available (the numbering on the screen indicates the priority level of the traffic):

- Unspecified UBR (0)** Unspecified Bit Rate
- Class 1 CBR (1)** Constant Bit Rate
- Class 3 VBR_RT (3)** Variable Bit Rate, Real Time
- Class 4 VBR_NRT (4)** Variable Bit Rate, Non-Real Time

Please note that if you select **VBR_RT** or **VBR_NRT**, then you should select **NoCLPSCR** for the Requested and Acceptable Tx Traffic Descriptor parameters (Options 4 and 13, respectively).

4) Requested Tx Traffic Descriptor

The traffic descriptor bundle to be used with this Class of Service. The traffic descriptor bundle you choose here determines which traffic parameters you will specify. The traffic parameters will include the Peak Cell Rate (PCR) and may also include the Sustained Cell Rate (SCR) and Maximum Burst Size (MBS). Each traffic descriptor bundle available is described in more detail in Chapter 41, “Managing Cell Switching Modules (CSMs).”

The traffic descriptor along with the Class of Service you choose determines the Generic Cell Rate Algorithm (GCRA), or “leaky bucket,” that will be used to police this connection. The following traffic descriptor bundles and prompts are available:

NoCLPNoSCR No Cell Loss Priority, No Sustaining Cell Rate (the default). The traffic descriptor suboptions are shown below.

- 4) Requested Tx Traffic Descriptor { NoCLPNoSCR(2),
NoCLPNoSCR (5) : NoCLP NoSCR
20) Peak Cell Rate (cells/sec) for CLP=0+1 : 1412831

The Peak Cell Rate (PCR) will be checked on the aggregate of CLP=0 and CLP=1 traffic. the default is 1412831.

NoCLPSCR No Cell Loss Priority, Sustaining Cell Rate. The traffic descriptor suboptions are shown below.

- 4) Requested Tx Traffic Descriptor { NoCLPNoSCR(2),
NoCLPSCR (5) : NoCLP NoSCR
20) Peak Cell Rate (cells/sec) for CLP=0+1 : 1412831
21) Sustaining Cell Rate (cells/sec) for CLP=0+1 : 50000
22) Maximum Burst Rate (cells) for CLP=0+1 : 100000

The Peak Cell Rate (PCR) will be checked on the aggregate of CLP=0 and CLP=1 (CLP=0+1) traffic. The default PCR is 1412831. The Sustaining Cell rate (SCR) will be checked on the aggregate of CLP=0 and CLP=1 traffic. The default SCR is 50000. (SCR must be less than PCR.) The Maximum Burst Size (MBS) will be checked on the aggregate of CLP=0+1 traffic. The MBS default setting is 100000 cells.

The following sections describe the traffic parameter prompts that display after you select a traffic descriptor bundle.

Peak Cell Rate

The following is a sample prompt display:

20) Peak Cell Rate (cells/sec) for CLP=0+1 : 1412831

In this field, you specify the Peak Cell Rate (PCR), in cells per second allowed on this virtual connection. The PCR is the fastest cell rate allowed on the connection. The switch will use this parameter as part of the traffic contract for this virtual circuit. A cell rate above the rate you indicate here will denote a violation of the traffic contract and the leaky bucket algorithm will determine which enforcement action take. Note that the PCR will be enforced on CLP=0+1 or CLP=0 cell flows; this prompt will indicate which cell flow is checked.

Sustaining Cell Rate

The following is a sample prompt display:

21) Sustaining Cell Rate (cells/sec) for CLP=0+1 : 50000

In this field, you specify the Sustaining Cell Rate (SCR), in cells per second allowed on this virtual connection. The SCR is highest average cell rate allowed on the circuit. The switch will use the parameter as part of the traffic contract for this virtual circuit. An average cell rate above the rate you indicate here will denote a violation of the traffic contract and the leaky bucket algorithm will determine which enforcement action take. Note that the SCR will be enforced on CLP=0+1 or CLP=0 cell flows; this prompt indicates which cell flow is checked.

Maximum Burst Rate

The following is a sample prompt display:

22) Maximum Burst Rate (cells) for CLP=0+1 : 100000

In this field, you specify the Maximum Burst Size (MBS), in cells allowed on this virtual connection. The MBS is the largest single burst of cells allowed on the connection. The switch will use this parameter as part of the traffic contract for this virtual circuit. A burst size above the value you indicate here will denote a violation of the traffic contract and the leaky bucket algorithm will determine which enforcement action to take. Note that the MBS will be enforced on CLP=0+1 or CLP=0 cell flows; this prompt indicates which cell flow is checked.

Modifying a Virtual Channel Connection

You can modify any parameters for a virtual circuit that you previously configured. The **mvc** command enables you to modify a virtual circuit. It uses the same screens and allows you to change the same parameters as the **cvc** command.

On early-generation ATM access modules (see *Early Generation OmniSwitch ATM Access Modules* on page 33-2), the syntax is as follows:

```
mvc <slot>/<port> <vci>
```

On the ASX-M-622RF-1W and SAHI-based ATM access modules (see *SAHI-Based ATM Access Modules* on page 33-3), the syntax is as follows:

```
mvc <slot>/<port> [<vpi>/]<vci>
```

If you do not specify a Virtual Path Identifier (VPI) number, then a VPI of 0 will be assumed.

For example, to modify a PVC with a VPI of 1 and a Virtual Channel Identifier (VCI) of 100 on an ASX-622FM-1W (SAHI-based) Port 1 in Slot 2, enter:

```
mvc 2/1 1/100
```

For more information on the **mvc** screens and parameters, see *Creating a Virtual Channel Connection* on page 33-15.

Deleting a Virtual Channel Connection

You use the **dvc** command to delete Permanent Virtual Circuits (PVCs) on ATM access ports. On early-generation ATM access modules (see *Early Generation OmniSwitch ATM Access Modules* on page 33-2), the syntax is as follows:

```
dvc <slot>/<port> <vci>
```

On the ASX-M-622RF-1W and SAHI-based ATM access modules (see *SAHI-Based ATM Access Modules* on page 33-3), the syntax is as follows:

```
dvc <slot>/<port> [<vpi>/]<vci>
```

If you do not specify a Virtual Path Identifier (VPI) number, then a VPI of 0 will be assumed.

For example, to delete a PVC with a VPI of 1 and a Virtual Channel Identifier (VCI) of 100 on an ASX-622FM-1W (SAHI-based) Port 1 in Slot 2, enter:

```
dvc 2/1 1/100
```

After you specify to delete a circuit, you will receive a message asking you to confirm the deletion:

```
Remove ATM Slot 2 Port 1 Connection 1/100 (n)? :
```

Stop the deletion by pressing **<Enter>** or entering **N** at this prompt. A message similar to the following displays:

```
ATM Slot 2 Port 1 Connection 1/100 not removed
```

Confirm the deletion by entering a **Y** at the confirmation prompt. The VCI or VPI/VCI will be removed and a message similar to the following displays:

```
Removing ATM Slot 2 Port 1 Connection VPI 1 VCI 100, please wait...
```

```
ATM Slot 2 Port 1 Connection VPI 1 VCI 100 removed
```

Creating a Virtual ATM Address

The **cva** command allows you to create a virtual ATM address in this switch. To create an ATM address, enter **cva** followed by the a 40-character ATM address.

The following command creates the address **1234342525675845624198645276452354672456**

```
cva 1234342525675845624198645276452354672456
```

and displays a screen similar to the following:

```
Connection Address 1234342525675845624198645276452354672456 Configuration
```

```
1) Description (30 chars max)                : Address 2
2) Tx QoS Class { Unspecified UBR(0),        : Unspecified
   Class1 CBR(1), Class3 VBR_RT(3), Class4 VBR_NRT(4)}
3) TX Best Effort { False (1), True (2) }    : True
4) Requested Tx Traffic Descriptor { NoCLPNoSCR(2),
   NoCLPSCR (5)                               : NoCLPNoSCR
   20) Peak Cell Rate (cells/sec) for CLP=0+1 : 353208
5) Requested Rx QoS Class { Unspecified(0) } : Unspecified
6) Requested RX Best Effort { False (1), True (2) } : True
7) Requested Rx Traffic Descriptor { NoCLPNoSCR(2) } : NoCLP NoSCR
   30) Peak Cell Rate (cells/sec) for CLP=0+1 : 353208

14) Tx Maximum Frame Size                    : 4520
15) Rx Maximum Frame Size                    : 4520
```

```
Enter (option=value/save/cancel) :
```

The options in this screen are the same as those used in the **cvc** command. Refer to the section, *Creating a Virtual Channel Connection* on page 33-15 for a description of these parameters.

◆ Important Note ◆

On all ATM access modules except for the ASX-M-622RF-1W, the only Transmit QoS Class (Option 2) available is Unspecified (UBR).

Once you have set up values in these fields you should enter **save** and press <Return>. The ATM address will then be created with the values you entered and the following message will display:

```
Creating address connection, please wait...
```

An index number will be assigned to this address. This index number is useful. It allows you to refer to this address using other commands without typing in the entire 40-byte address. You can see the index number assigned to the address using the **vva** command, which provides information on all configured virtual ATM addresses in the switch. The **vva** command is described in *Viewing Virtual ATM Addresses* on page 33-43.

Modifying Virtual ATM Addresses

You can modify parameters for a virtual ATM address that you previously configured through the **mva** command. The **mva** command uses the same screens and allows you to change the same parameters as the **cva** command.

To begin modifying an ATM address, enter **mva** followed by the index number assigned to the ATM address. You can view the index numbers for ATM addresses through the **vva** command, which is described in *Viewing Virtual ATM Addresses* on page 33-43. For example, you would enter the command

```
mva 2
```

to modify the virtual ATM address with an index number of 2. You can also enter the entire ATM address after the **mva** command if you prefer.

For more information on the **mva** parameters, see *Creating a Virtual Channel Connection* on page 33-15. Once you have set up values you should enter **save** and press <Return>.

Deleting a Virtual ATM Address

To delete an ATM virtual address enter **dva** followed by the index number of the address you want to delete. You can obtain the index number for an address through the **vva** command, which is described in *Viewing Virtual ATM Addresses* on page 33-43. For example, to delete the virtual ATM address with an index number of 4, you would enter:

```
dva 4
```

After you specify to delete an address, you will receive a message asking you to confirm the deletion:

```
Remove Address 4 (n)? :
```

Stop the deletion by pressing <Enter> or entering **N** at this prompt. A message similar to the following displays:

```
address xxxxxxxxyyyyyyyyyyaaaaaaaaabbbbbbbbbb not deleted
```

Confirm the deletion by entering a **Y** at the confirmation prompt. The address will be removed and a message similar to the following displays:

```
address index 4 removed
```

Viewing ATM Port Configuration Information

The **vap** command allows you to view basic information on a single ATM access port or all ATM access ports in a switch chassis. To view ATM access port configuration information, enter **vap** at a system prompt. The following is a sample display.

ATM Port Table

Slot	Port	ATM Port Description	Conn Type	Tran Type	Media Type	UNI Typ	Max VCC	VPI bits	VCI bits
2	1	ATM PORT	SVC	--	--	Pri	1023	0	10
2	2	ATM PORT	PVC	--	--	Pri	1023	0	10
5	1	ATM PORT	SVC	STS12	Multi	Pri	1023	0	10
6	1	ATM PORT	SVC	STS3c	Multi	Pri	1023	0	10

Slot	Port	Loopback Cfg	Tx Clk Source
2	1	NoLoop	LocalTiming
2	2	NoLoop	LocalTiming
5	1	NoLoop	LocalTiming
6	1	NoLoop	LocalTiming

Slot	Port	ATM Network Prefix	End System Identifier	Sig Ver	Sig VCI	ILMI Enable	ILMI VCI	ILMI Poll
2	1	3903488001bc90000101dbd400	0020da98e910	3.0	5	True	16	Off
2	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	1	3903488001bc90000101dbcfa0	0020dace0660	3.1	5	True	16	Off
6	1	000000000000000000000000	0020dab344f0	3.0	5	True	16	Off

Status

Slot	Port	Sscop Up	Sscop Down	Up	Dn	Status
2	1	WED SEP 29 10:03:37 1999	WED SEP 29 10:03 :32 1999	2	1	Up
2	2	-----	-----	0	0	Down
5	1	WED SEP 29 10:10:53 1999	WED SEP 29 10:10 :46 1999	50	49	Up
6	1	-----	-----	0	0	Down

Slot	Port	Ilmi Up	Ilmi Down	Up	Dn	Status
2	1	WED SEP 29 10:03:30 1999	-----	1	0	Up
2	2	-----	-----	0	0	Down
5	1	WED SEP 29 10:02:51 1999	-----	1	0	Up
6	1	-----	-----	0	0	Down

Slot	Port	Phy Up	Phy Down	Up	Dn	Status
2	1	WED SEP 29 10:02:11 1999	-----	1	0	Enb (SVC)
2	2	WED SEP 29 10:01:46 1999	-----	1	0	Enb (CTL)
5	1	WED SEP 29 10:02:25 1999	-----	1	0	Enb (PVC)
6	1	-----	-----	0	0	Dis (R)

Slot	Port	Tx SegSz	Rx Seg Sz	Tx Buff Sz	Rx Buff Sz
2	1	16384	16384	4600	4600
2	2	8192	8192	8192	8192
5	1	131072	131072	4600	4600
6	2	131072	131072	4600	4600

ATM Redundant Port Status

Slot	Port	Primary	Secondary	FailOver	Reason of Last Failover
5	1	Active	Inactive	0	

Slot. The port's slot number.

Port. The port number.

ATM Port Description, Conn Type (Connection type). These fields are described earlier in *Modifying an ATM Access Port Configuration* on page 33-8.

Tran Type. The transmission, or connection, type. Possible transmission types are **STS3c** (OC-3), **STS12c** (OC-12), **DS3**, **E3**, and **--** (unknown type).

Media Type. The physical connector type used on this port. Possible types in this column are **Multi** (multimode fiber), **Single** (single mode fiber), **STP** (shielded twisted pair), **UTP** (unshielded twisted pair), **Coax** (coaxial cable), and **UNKN** (unknown connector).

UNI Typ (UNI type), **Max VCC**, **VPI bits**, **VCI bits** (maximum VCI bits). These fields are described in *Modifying an ATM Access Port Configuration* on page 33-8.

Loopback Cfg. The loopback configuration for this port.

NoLoop	No loopback occurs between receive and transmission paths.
DiagLoop	Interface transmission path is connected to receive path at the connectors. The port receives its own transmission rather than the signal coming over the cable.
LineLoop	The interface receive path is looped to the transmission path at the connectors. The signal on the receive connector is not passed into the UNI and processed.

Tx Clk Source (timing mode). This field is described in *Modifying an ATM Access Port Configuration* on page 33-8.

ATM Network Prefix. The network prefix portion of the ATM address.

End System Identifier. The end station identifier (ESI) portion of the ATM address.

Sig Ver, **Sig VCI**, **ILMI Enable**, **ILMI VCI**, **ILMI Poll**, **Tx Seg Sz** (transmit SAR buffer size), **Rx Seg Sz** (receive SAR buffer size), **Tx Buff Sz** (transmit frame buffer size), **Rx Buff Sz** (receive frame buffer size) are described in *Modifying an ATM Access Port Configuration* on page 33-8.

The following column headings fall under the table heading labeled **Status**.

SSCOP. The current state of the Service-Specific Connection Oriented Protocol (SSCOP). SSCOP operates on the ATM control plane and is a peer-to-peer protocol that helps set up connections and provides a reliable transport mechanism for signaling. The **Sscop Up** and **Sscop Down** columns will indicate the last time SSCOP last came up and went down, respectively. The **Up** and **Dn** (down) columns will indicate the number of times SSCOP came up and went down, respectively. The SSCOP **Status** column will indicate Up or Down. This value will always indicate **Down** if the Connection Type configured on this port is PVC.

ILMI. The Integrated Local Management Interface (ILMI) enabled on this port. The **Ilmi Up** and **Ilmi Down** columns will indicate the last time ILMI last came up and went down, respectively. The **Up** and **Dn** (down) columns will indicate the number of times ILMI came up and went down, respectively. The ILMI **Status** column will indicate Up or Down. This value will always indicate **Dn** if the Connection Type configured on this port is PVC.

Viewing ATM Port Configuration Information

PHY. The operational status of the port. The **Phy Up** and **Phy Down** columns will indicate the last time physical port last came up and went down, respectively. The **Up** and **Dn** (down) columns will indicate the number of times physical port came up and went down, respectively. The **PHY Status** column will indicate whether the port is **Enabled** or **Disabled** and provides information on upper service layers. The port will be enabled if the port is connected on this end and the far end. If there is a disconnection at either end, then the operational status will be **Disabled**. Possible values are as follows:

Enb (PVC)	Port is enabled to support PVCs.
Enb (SVC)	Port is enabled to support SVCs.
Enb (CTL)	Port is enabled to pass control signals.
Dis (R)	The receive is disabled on this port.
Dis (T/R)	Both the transmit and receive are disabled.
Dis (T)	Disabled transmit on this port.

The column headings under the table heading labeled **ATM Redundant Port Status** are only relevant if you have an ATM uplink module with a redundant port.

Primary. Indicates whether the primary port is active or inactive. If the primary port experiences a failover (activating the secondary port), it will remain inactive and will re-activate only when both its failover has been repaired *and* the secondary port experiences a failover

Secondary. Indicates whether the secondary port is active or inactive. If it is active, the primary port has experienced a failover.

FailOver. The total number of failovers that has occurred.

Reason of Last Failover. A brief explanation of the most recent failover. Port failovers occur, for example, when there is a physical disconnection. The following is an example of a **Reason of Last Failover** message: **SgnlLoss Cell Loss**.

Information on the Ports for One ATM Access Module

To view basic information on all ATM access ports in a single ATM access module, you enter the **vap** command along with the slot number for the ATM access module, as follows:

```
vap <slot>
```

where **<slot>** is the slot number where the ATM access module is installed. For example, if you wanted to obtain status information for the module in slot 2, you would enter:

```
vap 2
```

This command displays a screen similar to the following:

```

ATM Port Table

Slot Port      ATM Port Description      Conn Tran Media UNI Max VPI VCI
==== =====
2   1          ATM PORT                  SVC  --  --  Pri 1023 0 10
2   2          ATM PORT                  PVC  --  --  Pri 1023 0 10

Slot Port Loopback Cfg Tx Clk Source
==== =====
2   1    NoLoop    LocalTiming
2   2    NoLoop    LocalTiming

Slot Port      ATM Network Prefix      End System Sig Sig ILMI ILMI ILMI
==== ===== Identifier Ver VCI Enable VCI Poll
2   1  3903488001bc90000101dbd400 0020da98e910 3.0 5  True 16  Off
2   2                N/A                N/A  N/A N/A  N/A  N/A  N/A

Status
=====

Slot Port      Sscop Up      Sscop Down      Up Dn Status
==== =====
2   1  WED SEP 29 10:03:37 1999  WED SEP 29 10:03 :32 1999  2  1  Up
2   2  -----          -----          0  0  Down

Slot Port      Ilmi Up      Ilmi Down      Up Dn Status
==== =====
2   1  WED SEP 29 10:03:30 1999  -----          1  0  Up
2   2  -----          -----          0  0  Down

Slot Port      Phy Up      Phy Down      Up Dn Status
==== =====
2   1  WED SEP 29 10:02:11 1999  -----          1  0  Enb (SVC)
2   2  WED SEP 29 10:01:46 1999  -----          1  0  Enb (CTL)

Slot Port Tx SegSz Rx Seg Sz Tx Buff Sz Rx Buff Sz
==== =====
2   1      16384    16384    4600    4600
2   2      8192     8192     8192     8192

```

Descriptions of the columns included in this display are described earlier in *Viewing ATM Port Configuration Information* on page 33-26.

Information on One Port

To view information on a single ATM access port, you enter the **vap** command along with the slot number for the ATM access module and the port number for which you want to receive information, as follows:

vap <slot>/<port>

where **<slot>** is the slot number where the ATM access module is installed and **<port>** is the port number on the ATM access module. For example, if you wanted to view basic information for port 1 on the ATM access module in slot 2, you would enter:

vap 2/1

This command displays a screen similar to the following:

ATM Port Table

Slot	Port	ATM Port Description	Conn Type	Tran Type	Media Type	UNI Typ	Max VCC	VPI bits	VCI bits
2	1	ATM PORT	SVC	--	--	Pri	1023	0	10

Slot	Port	Loopback Cfg	Tx Clk Source
2	1	NoLoop	LocalTiming

Slot	Port	ATM Network Prefix	End System Identifier	Sig Ver	Sig VCI	ILMI Enable	ILMI VCI	ILMI Poll
2	1	3903488001bc90000101dbd400	0020da98e910	3.0	5	True	16	Off

Status

=====

Slot	Port	Sscop Up	Sscop Down	Up	Dn	Status
2	1	WED SEP 29 10:03:37 1999	WED SEP 29 10:03 :32 1999	2	1	Up

Slot	Port	Ilmi Up	Ilmi Down	Up	Dn	Status
2	1	WED SEP 29 10:03:30 1999	-----	1	0	Up

Slot	Port	Phy Up	Phy Down	Up	Dn	Status
2	1	WED SEP 29 10:02:11 1999	-----	1	0	Enb (SVC)

Slot	Port	Tx SegSz	Rx Seg Sz	Tx Buff Sz	Rx Buff Sz
2	1	16384	16384	4600	4600

Descriptions of the columns included in this display are described earlier in *Viewing ATM Port Configuration Information* on page 33-26.

Viewing SSCOP, ILMI, and PHY

You can view general and detailed Service-Specific Connection Oriented Protocol (SSCOP), Interim Local Management protocol (ILMI), and Physical information on all ATM access ports in a switch, a single ATM access module, and individual ports. The **vap** command is used to provide this information.

Viewing SSCOP, ILMI, and PHY Information on All Ports

To view SSCOP, ILMI, and PHY information on all ATM access ports in a switch, you enter the **vap** command along with the following parameters:

```
vap sip
```

where **s** indicates SSCOP, **i** indicates ILMI, and **p** indicates PHY. This command displays a screen similar to the following:

ATM Port Table											
Slot	Port	ATM Port Description			Conn Type	Tran Type	Media Type	UNI Typ	Max VCC	VPI bits	VCI bits
2	1	ATM PORT			SVC	--	--	Pri	1023	0	10
2	2	ATM PORT			PVC	--	--	Pri	1023	0	10
5	1	ATM PORT			SVC	STS12	Multi	Pri	1023	0	10
6	1	ATM PORT			SVC	STS3c	Multi	Pri	1023	0	10

Slot	Port	Loopback	Cfg	Tx Clk Source
2	1	NoLoop		LocalTiming
2	2	NoLoop		LocalTiming
5	1	NoLoop		LocalTiming
6	1	NoLoop		LocalTiming

Slot	Port	ATM Network Prefix	End System Identifier	System Ver	Sig Ver	Sig VCI	ILMI Enable	ILMI VCI	ILMI Poll
2	1	3903488001bc90000101dbd400	0020da98e910	3.0	5	5	True	16	Off
2	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	1	3903488001bc90000101dbcfa0	0020dace0660	3.1	5	5	True	16	Off
5	1	000000000000000000000000	0020dab344f0	3.0	5	5	True	16	Off

Status										
Slot	Port	Sscop Up			Sscop Down			Up	Dn	Status
2	1	WED SEP 29 10:03:37 1999			WED SEP 29 10:03:32 1999			2	1	Up
2	2	-----			-----			0	0	Down
5	1	WED SEP 29 10:10:53 1999			WED SEP 29 10:10:46 1999			50	49	Up
6	1	-----			-----			0	0	Down

Slot	Port	Ilmi Up			Ilmi Down			Up	Dn	Status
2	1	WED SEP 29 10:03:30 1999			-----			1	0	Up
2	2	-----			-----			0	0	Down
5	1	WED SEP 29 10:02:51 1999			-----			1	0	Up
6	1	-----			-----			0	0	Down

Slot	Port	Phy Up			Phy Down			Up	Dn	Status
2	2	WED SEP 29 10:01:46 1999			-----			1	0	Enb (CTL)

Slot	Port	Phy Up			Phy Down			Up	Dn	Status
5	1	WED SEP 29 10:02:25 1999			-----			1	0	Enb (PVC)
6	1	-----			-----			0	0	Dis (R)

— Output continues on next page —

Viewing ATM Port Configuration Information

Slot	Port	Tx SegSz	Rx Seg Sz	Tx Buff Sz	Rx Buff Sz
2	1	16384	16384	4600	4600
2	2	8192	8192	8192	8192
5	1	131072	131072	4600	4600
6	1	131072	131072	4600	4600

ATM Redundant Port Status

Slot	Port	Primary	Secondary	FailOver	Reason of Last Failover
5	1	Active	Inactive	0	

Additionally, you may enter the parameters for SSCOP, ILMI, and PHY in any order and combination. For example, if you wanted to view only the ILMI and PHY, you enter the **vap** command along with the respective parameters as follows:

vap ip

or

vap pi

This command displays a screen similar to the following:

ATM Port Table					
Status					
Slot	Port	Ilmi Up	Ilmi Down	Up	Dn Status
2	1	WED SEP 29 10:03:30 1999	-----	1	0 Up
2	2	-----	-----	0	0 Down
5	1	WED SEP 29 10:02:51 1999	-----	1	0 Up
6	1	-----	-----	0	0 Down
Slot	Port	Phy Up	Phy Down	Up	Dn Status
2	1	WED SEP 29 10:02:11 1999	-----	1	0 Enb (SVC)
2	2	WED SEP 29 10:01:46 1999	-----	1	0 Enb (CTL)
5	1	WED SEP 29 10:02:25 1999	-----	1	0 Enb (PVC)
6	1	-----	-----	0	0 Dis (R)
Slot	Port	Tx SegSz	Rx Seg Sz	Tx Buff Sz	Rx Buff Sz
2	1	16384	16384	4600	4600
2	2	8192	8192	8192	8192
5	1	131072	131072	4600	4600
6	1	131072	131072	4600	4600
ATM Redundant Port Status					
Slot	Port	Primary	Secondary	FailOver	Reason of Last Failover
5	1	Active	Inactive	0	

Descriptions of the columns included in the two displays above are described earlier in *Viewing ATM Port Configuration Information* on page 33-26.

Viewing SSCOP, ILMI, and PHY Information on One ATM Access Module

To view SSCOP, ILMI, and PHY information on a single ATM access module in a switch, you enter the **vap** command along with the slot number for the ATM access module and the following parameters:

```
vap <slot> sip
```

where **<slot>** is the slot number where the ATM access module is installed, **s** indicates SSCOP, **i** indicates ILMI, and **p** indicates PHY. For example, if you wanted to view SSCOP, ILMI, and PHY information for the module in slot 2, you would enter:

```
vap 2 sip
```

This command displays a screen similar to the following:

ATM Port Table											
Slot	Port	ATM Port Description			Conn Type	Tran Type	Media Type	UNI Typ	Max VCC	VPI bits	VCI bits
2	1	ATM PORT			SVC	--	--	Pri	1023	0	10
2	2	ATM PORT			PVC	--	--	Pri	1023	0	10

Slot	Port	Loopback	Cfg	Tx Clk	Source
2	1	NoLoop		Local	Timing
2	2	NoLoop		Local	Timing

Slot	Port	ATM Network Prefix		End System Identifier	Sig Ver	Sig VCI	ILMI Enable	ILMI VCI	ILMI Poll
2	1	3903488001bc90000101dbd400		0020da98e910	3.0	5	True	16	Off
2	2	N/A		N/A	N/A	N/A	N/A	N/A	N/A

Status										
Slot	Port	Sscop Up			Sscop Down			Up	Dn	Status
2	1	WED SEP 29 10:03:37 1999			WED SEP 29 10:03 :32 1999			2	1	Up
2	2	-----			-----			0	0	Down

Slot	Port	Ilmi Up			Ilmi Down			Up	Dn	Status
2	1	WED SEP 29 10:03:30 1999			-----			1	0	Up
2	2	-----			-----			0	0	Down

Slot	Port	Phy Up			Phy Down			Up	Dn	Status
2	1	WED SEP 29 10:02:11 1999			-----			1	0	Enb (SVC)
2	2	WED SEP 29 10:01:46 1999			-----			1	0	Enb (CTL)

Slot	Port	Tx SegSz	Rx Seg Sz	Tx Buff Sz	Rx Buff Sz
2	1	16384	16384	4600	4600
2	2	8192	8192	8192	8192

Additionally, you may enter the parameters for SSCOP, ILMI, and PHY in any order or combination. For example, if you wanted to view the statistics for only SSCOP and ILMI for a single board, you enter the **vap** command along with the slot number and the respective parameters as follows:

```
vap <slot> si
```

or

```
vap <slot> is
```

Descriptions of the columns included in the display above are described earlier in *Viewing ATM Port Configuration Information* on page 33-26.

Viewing SSCOP, ILMI, and PHY Information on One Port

To view SSCOP, ILMI, and PHY information on a single ATM access port, you enter the **vap** command along with the slot number for the ATM access module, the port number for which you want to receive information, and the following parameters:

```
vap <slot>/<port> sip
```

where **<slot>** is the slot number where the ATM access module is installed, **<port>** is the port number on the ATM access module, **s** indicates SSCOP, **i** indicates ILMI, and **p** indicates PHY. For example, if you wanted to view SSCOP, ILMI, and PHY information for port 1 on the ATM access module in slot 2, you would enter:

```
vap 2/1 sip
```

This command displays a screen similar to the following:

```

ATM Port Table
-----
Slot Port      ATM Port Description      Conn Tran  Media UNI Max VPI VCI
Type Type     Type Type   Type Typ  VCC bits bits
=====
2     1           ATM PORT                  SVC  --   --  Pri 1023 0 10

Slot Port Loopback Cfg Tx Clk Source
=====
2     1     NoLoop      LocalTiming

Slot Port      ATM Network Prefix      End System  Sig Sig  ILMI  ILMI  ILMI
Type Type     Identifier Ver VCI  Enable VCI Poll
=====
2     1     3903488001bc90000101dbd400 0020da98e910 3.0 5   True  16   Off

Status
=====

Slot Port      Sscop Up                Sscop Down                Up Dn Status
=====
2     1     WED SEP 29 10:03:37 1999  WED SEP 29 10:03 :32 1999  2  1  Up

Slot Port      Ilmi Up                Ilmi Down                Up Dn Status
=====
2     1     WED SEP 29 10:03:30 1999  -----  1  0  Up

Slot Port      Phy Up                Phy Down                Up Dn Status
=====
2     1     WED SEP 29 10:02:11 1999  -----  1  0  Enb (SVC)

Slot Port Tx SegSz Rx Seg Sz Tx Buff Sz Rx Buff Sz
=====
2     1           16384    16384    4600     4600

```

Additionally, you may enter the parameters for SSCOP, ILMI, and PHY in any order and combination. For example, if you want to view the statistics for only SSCOP and PHY for a single ATM access port, you enter the **vap** command along with the slot number, the port number for which you want to receive information, and the respective parameters as follows:

```
vap <slot>/<port> sp
```

or

```
vap <slot>/<port> ps
```

Descriptions of the columns included in the display above are described earlier in *Viewing ATM Port Configuration Information* on page 33-26.

Viewing Virtual Channel Connections

The **vvc** command provides information on all VCIs associated with a given FCSM internal logical port or ATM access module port. If you also have CSM modules in an OmniSwitch chassis, then a separate display is shown (below the ATM access ports section) for the VCIs associated with these ATM *switched* ports. Descriptions of CSM module columns can be found in Chapter 41, “Managing Cell Switching Modules (CSMs).”

The syntax for this command is as follows:

```
vvc [<slot>[/<port>]] [-v]
```

If you do not specify the slot or port number, then the statistics for all connections will be displayed. The following is a sample of the output from a **vvc** display for ATM access ports.

```

ATM Connections

```

Slot	Port	VPI	VCI	Connection Description	Conn Type	Circuit Type	Operational Status
3	1	0	100	Connection 100	VCC	PVC	LocalDown
7	1	0	5	Connection 5	VCC	PVC	LocalUp End2endUnknown
7	1	0	16	Connection 16	VCC	PVC	LocalUp End2endUnknown
7	1	0	100	Connection 100	VCC	PVC	LocalDown
7	2	0	100	Connection 100	VCC	PVC	LocalDown
7	2	0	1015	Connection 1015	VCC	PVC	LocalUp End2endUnknown
7	2	0	1016	Connection 1016	VCC	PVC	LocalUp End2endUnknown
7	2	0	1017	Connection 1017	VCC	PVC	LocalUp End2endUnknown
7	2	0	1019	Connection 1019	VCC	PVC	LocalUp End2endUnknown
7	2	0	1022	Connection 1022	VCC	PVC	LocalUp End2endUnknown

The **-v** option provides a verbose option as shown below.

```

ATM Connections

```

Slot	Port	VPI	VCI	Connection Description	Conn Type	Circuit Type	Operational Status
3	1	0	100	Connection 100	VCC	PVC	LocalDown
7	1	0	5	Connection 5	VCC	PVC	LocalUp End2endUnknown
7	1	0	16	Connection 16	VCC	PVC	LocalUp End2endUnknown
7	1	0	100	Connection 100	VCC	PVC	LocalDown
7	2	0	100	Connection 100	VCC	PVC	LocalDown
7	2	0	1015	Connection 1015	VCC	PVC	LocalUp End2endUnknown
7	2	0	1016	Connection 1016	VCC	PVC	LocalUp End2endUnknown
7	2	0	1017	Connection 1017	VCC	PVC	LocalUp End2endUnknown
7	2	0	1019	Connection 1019	VCC	PVC	LocalUp End2endUnknown
7	2	0	1022	Connection 1022	VCC	PVC	LocalUp End2endUnknown

Slot	Port	VPI	VCI	Port Status	Tx Max Frame Sz	Rx Max Frame Sz
7	1	0	5	UP	4600	4600
7	1	0	16	UP	4600	4600
7	1	0	100	UP	4600	4600
7	2	0	100	UP	2000	2000
7	2	0	1015	UP	2048	2048
7	2	0	1016	UP	2048	2048
7	2	0	1017	UP	2000	2000
7	2	0	1019	UP	2048	2048
7	2	0	1022	UP	2048	2048

— Output continues on next page —

Viewing Virtual Channel Connections

Actual Tx Traffic Information

Slot	Port	VPI	VCI	Tx Traffic		Peak	Tx	Best
=====				Descrip	Type	Cell Rate	QoS	Effort
=====				=====		=====	=====	=====
3	1	0	100	NoCLP	NoSCR	0	Uns	True
7	1	0	5	NoCLP	NoSCR	353208	Uns	True
7	1	0	16	NoCLP	NoSCR	353208	Uns	True
7	1	0	100	NoCLP	NoSCR	0	Uns	True
7	2	0	100	NoCLP	NoSCR	0	Uns	True
7	2	0	1015	NoCLP	NoSCR	353208	Uns	True
7	2	0	1016	NoCLP	NoSCR	353208	Uns	True
7	2	0	1017	NoCLP	NoSCR	353208	Uns	True
7	2	0	1019	NoCLP	NoSCR	353208	Uns	True
7	2	0	1022	NoCLP	NoSCR	353208	Uns	True

Actual Rx Traffic Information

Slot	Port	VPI	VCI	Rx Traffic		Peak	Rx	Best
=====				Descrip	Type	Cell Rate	QoS	Effort
=====				=====		=====	=====	=====
3	1	0	100	NoCLP	NoSCR	0	Uns	True
7	1	0	5	NoCLP	NoSCR	353208	Uns	True
7	1	0	16	NoCLP	NoSCR	353208	Uns	True
7	1	0	100	NoCLP	NoSCR	0	Uns	True
7	2	0	100	NoCLP	NoSCR	0	Uns	True
7	2	0	1015	NoCLP	NoSCR	353208	Uns	True
7	2	0	1016	NoCLP	NoSCR	353208	Uns	True
7	2	0	1017	NoCLP	NoSCR	353208	Uns	True
7	2	0	1019	NoCLP	NoSCR	353208	Uns	True
7	2	0	1022	NoCLP	NoSCR	353208	Uns	True

+ ==> PVC Connections

==> MPLS Connections

* ==> SVC Connections which cannot be modified by the user

@ ==> Soft PVC Connections

& ==> Control Connections

VPI. The virtual path identifier for this virtual channel.

VCI. The virtual channel identifier for this virtual channel. For PVCs, this value is specified during the virtual channel creation procedure via the **cvc** command. Some commonly used VCI are 5 (for signalling) and 16 (for ILMI).

Connection Description. A textual description of up to 30 characters for this virtual connection. Entered through the **cvc** command.

Connection Type. Indicates whether this connection is a virtual path or a virtual channel. All ATM access connections, or uplink connections, are virtual channels. Therefore, this column will always display as **VCC** (Virtual Channel Connection).

Circuit Type. The circuit type is configured with the **map** command. All circuit types on a single ATM port will be the same. The circuit type can be either **PVC** (Permanent Virtual Circuit) or **SVC** (Switched Virtual Circuit).

Operational Status. The current operational status of this virtual connection. This status will display as one of the following:

Unknown	The switch cannot tell if either the local or remote end of this connection is operational.
End2endUp	Remote end is operational. This value displays only if the end-to-end status of this connection is known.
End2endDown	Remote end is not operational. This value displays only if the end-to-end status of this connection is known.
LocalUp, End2endUnknown	Only local information is known. The local end of the connection is operational, but the switch cannot tell if the remote end is up or down.

LocalDown

Only local information is known. The local end of the connection is not operational.

◆ Note ◆

PVCs will always have an operational status in which the remote end status is unknown (i.e., **LocalUp,End2endUnknown** or **LocalDown**).

Port Status. This field will display **UP** if the port is up or **DOWN** if it is down.

TX Max Frame Sz and **Rx Max Frame Sz.** Descriptions for these variables are provided in the section, *Creating a Virtual Channel Connection*.

Traffic information is supplied for Transmit (Tx) and Receive (Rx) traffic. These variables are **Tx/Rx Traffic Descrip Type**, **Peak Cell Rate**, **Tx/Rx QoS**, and **Best Effort**. Descriptions for these variables are provided in *Creating a Virtual Channel Connection* on page 33-15.

Information on the Ports for One ATM Access Module

To view status information on virtual circuits in a single ATM access module, you enter the `vc` command along with the slot number for the ATM access module, as follows:

```
vc <slot> [-v]
```

where `<slot>` is the slot number where the ATM access module is installed and `-v` is the option to display verbose mode. For example, if you wanted to view verbose status information for the board in slot 7, you would enter:

```
vc 7 -v
```

This command displays a screen similar to the following:

ATM Connections							
Slot	Port	VPI	VCI	Connection Description	Conn Type	Circuit Type	Operational Status
7	1	0	5	Connection 5	VCC	PVC	LocalUp End2endUnknown
7	1	0	16	Connection 16	VCC	PVC	LocalUp End2endUnknown
7	1	0	100	Connection 100	VCC	PVC	LocalDown
7	2	0	100	Connection 100	VCC	PVC	LocalDown
7	2	0	1015	Connection 1015	VCC	PVC	LocalUp End2endUnknown
7	2	0	1016	Connection 1016	VCC	PVC	LocalUp End2endUnknown
7	2	0	1017	Connection 1017	VCC	PVC	LocalUp End2endUnknown
7	2	0	1019	Connection 1019	VCC	PVC	LocalUp End2endUnknown
7	2	0	1022	Connection 1022	VCC	PVC	LocalUp End2endUnknown

Slot	Port	VPI	VCI	Port Status	Tx Max Frame Sz	Rx Max Frame Sz
7	1	0	5	UP	4600	4600
7	1	0	16	UP	4600	4600
7	1	0	100	UP	4600	4600
7	2	0	100	UP	2000	2000
7	2	0	1015	UP	2048	2048
7	2	0	1016	UP	2048	2048
7	2	0	1017	UP	2000	2000
7	2	0	1019	UP	2048	2048
7	2	0	1022	UP	2048	2048

— Output continues on next page —

Actual Tx Traffic Information

Slot	Port	VPI	VCI	Tx Traffic		Peak	Tx	Best
				Descrip	Type	Cell Rate	QoS	Effort
7	1	0	5	NoCLP	NoSCR	353208	Uns	True
7	1	0	16	NoCLP	NoSCR	353208	Uns	True
7	1	0	100	NoCLP	NoSCR	0	Uns	True
7	2	0	100	NoCLP	NoSCR	0	Uns	True
7	2	0	1015	NoCLP	NoSCR	353208	Uns	True
7	2	0	1016	NoCLP	NoSCR	353208	Uns	True
7	2	0	1017	NoCLP	NoSCR	353208	Uns	True
7	2	0	1019	NoCLP	NoSCR	353208	Uns	True
7	2	0	1022	NoCLP	NoSCR	353208	Uns	True

Actual Rx Traffic Information

Slot	Port	VPI	VCI	Rx Traffic		Peak	Rx	Best
				Descrip	Type	Cell Rate	QoS	Effort
7	1	0	5	NoCLP	NoSCR	353208	Uns	True
7	1	0	16	NoCLP	NoSCR	353208	Uns	True
7	1	0	100	NoCLP	NoSCR	0	Uns	True
7	2	0	100	NoCLP	NoSCR	0	Uns	True
7	2	0	1015	NoCLP	NoSCR	353208	Uns	True
7	2	0	1016	NoCLP	NoSCR	353208	Uns	True
7	2	0	1017	NoCLP	NoSCR	353208	Uns	True
7	2	0	1019	NoCLP	NoSCR	353208	Uns	True
7	2	0	1022	NoCLP	NoSCR	353208	Uns	True

+ ==> PVC Connections
 # ==> MPLS Connections
 * ==> SVC Connections which cannot be modified by the user
 @ ==> Soft PVC Connections
 & ==> Control Connections

Descriptions of the columns included in this display are described earlier in *Viewing Virtual Channel Connections* on page 33-35.

Information on One Port

To view status information on virtual circuits in a single ATM access port, you enter the **vvv** command along with the slot number for the ATM access module and the port number for which you want to receive information, as follows:

```
vvv <slot>/<port> [-v]
```

where **<slot>** is the slot number where the ATM access module is installed, **<port>** is the port number on the ATM access module, and **-v** is the option to display verbose mode. For example, if you wanted to view verbose status information for port 1 on the ATM access module in slot 7, you would enter:

```
vvv 7/1 -v
```

This command displays a screen similar to the following:

```

                        ATM Connections

Slot Port VPI VCI      Connection      Conn Circuit Operational
=====
7   1   0   5      Connection 5      VCC  PVC  LocalUp End2endUnknown
7   1   0  16      Connection 16      VCC  PVC  LocalUp End2endUnknown
7   1   1  100     Connection 100     VCC  PVC  LocalDown

Slot Port VPI VCI      Port      Tx Max      Rx Max
=====
7   1   0   5      UP      4600      4600
7   1   0  16      UP      4600      4600
7   1   0  100     UP      4600      4600

                        Actual Tx Traffic Information

Slot Port VPI VCI      Tx Traffic      Peak      Tx      Best
=====
7   1   0   5      NoCLP NoSCR      353208  Uns True
7   1   0  16      NoCLP NoSCR      353208  Uns True
7   1   1  100     NoCLP NoSCR           0  Uns True

                        Actual Rx Traffic Information

Slot Port VPI VCI      Rx Traffic      Peak      Rx      Best
=====
7   1   0   5      NoCLP NoSCR      353208  Uns True
7   1   0  16      NoCLP NoSCR      353208  Uns True
7   1   1  100     NoCLP NoSCR           0  Uns True

+ ==> PVC Connections
# ==> MPLS Connections
* ==> SVC Connections which cannot be modified by the user
@ ==> Soft PVC Connections
& ==> Control Connections

```

Descriptions of the columns included in this display are described earlier in *Viewing Virtual Channel Connections* on page 33-35.

Information on One Virtual Path

To view status information on a single virtual path, you enter the **vvv** command along with the slot number for the ATM access module, the port number, and the VPI number for the virtual path on which you want information, as follows:

```
vvv <slot>/<port> <vpi> [-v]
```

where **<slot>** is the slot number where the ATM access module is installed, **<port>** is the port number on the ATM access module, **<vpi>** is the virtual path identifier, and **-v** is the option to display verbose mode. For example, if you wanted to view verbose status information for the board in slot 5, port 4, VPI 0, you would enter:

```
vvv 5/4 0 -v
```

This command displays a screen similar to the following:

```

ATM Connections

Slot Port VPI VCI      Connection      Conn Circuit  Operational
=====
7   1   0   5   Connection 5   VCC  PVC   LocalUp End2endUnknown
7   1   0  16   Connection 16  VCC  PVC   LocalUp End2endUnknown

Slot Port VPI VCI      Port      Tx Max      Rx Max
=====
7   1   0   5   UP        4600        4600
7   1   0  16   UP        4600        4600

Actual Tx Traffic Information

Slot Port VPI VCI      Tx Traffic      Peak      Tx      Best
=====
7   1   0   5   NoCLP NoSCR      353208   Uns   True
7   1   0  16   NoCLP NoSCR      353208   Uns   True

Actual Rx Traffic Information

Slot Port VPI VCI      Rx Traffic      Peak      Rx      Best
=====
7   1   0   5   NoCLP NoSCR      353208   Uns   True
7   1   0  16   NoCLP NoSCR      353208   Uns   True

+ ==> PVC Connections
# ==> MPLS Connections
* ==> SVC Connections which cannot be modified by the user
@ ==> Soft PVC Connections
& ==> Control Connections

```

Descriptions of the columns included in this display are described earlier in *Viewing Virtual Channel Connections* on page 33-35.

Information on One Virtual Channel

To view status information on a single virtual channel, you enter the **vvc** command along with the slot number for the ATM access module, the port number, the VPI number, and VCI number for the virtual path on which you want information, as follows:

vvc <slot>/<port> <vpi>/<vci> [-v]

where **<slot>** is the slot number where the ATM access module is installed, **<port>** is the port number on the ATM access module, **<vpi>** is the virtual path identifier, **<vci>** is the virtual channel identifier, and **-v** is the option to display verbose mode. For example, if you wanted to view verbose status information for the board in slot 5, port 4, VPI 0, and VCI 16, you would enter:

vvc 5/4 0/16 -v

This command displays a screen similar to the following:

```

ATM Connections

Slot Port VPI VCI      Connection      Conn Circuit  Operational
=====
7   1   0  16      Connection 16      VCC  PVC  LocalUp End2endUnknown

Slot Port VPI VCI      Port      Tx Max      Rx Max
=====
7   1   0  16      UP        4600        4600

Actual Tx Traffic Information

Slot Port VPI VCI      Tx Traffic      Peak      Tx      Best
=====
7   1   0  16      NoCLP NoSCR        353208  Uns  True

Actual Rx Traffic Information

Slot Port VPI VCI      Rx Traffic      Peak      Rx      Best
=====
7   1   0  16      NoCLP NoSCR        353208  Uns  True

+ ==> PVC Connections
# ==> MPLS Connections
* ==> SVC Connections which cannot be modified by the user
@ ==> Soft PVC Connections
& ==> Control Connections
    
```

Descriptions of the columns included in this display are described earlier in *Viewing Virtual Channel Connections* on page 33-35.

Viewing Virtual ATM Addresses

The **vva** command allows you to view information on all ATM addresses in a switch. The **vva** display provides information on all end system addresses associated with a given FCSM internal logical port or ATM uplink port. The following is sample of the output from a **vva** display.

ATM Addresses		
Addr Indx	ATM Address	Description
1	1234567890987654321234567890987654321234	Address 1
2	1234342525675845624198645276452354672486	Address 2

Addr Indx	VPI	VCI	Conn Type	VC Type	TxMax SDU	Rx Max SDU	Arp Server
1	0	0000	VCC	SVC	4520	4520	False
2	0	0000	VCC	SVC	4520	4520	False

Tx Traffic Information

Addr Indx	Tx Traffic Descriptor	Type	Peak Rate	Tx QoS	Best Effort	Priority
1	NoCLP	NoSCR	353208	Uns	True	UBR
2	NoCLP	NoSCR	353208	Uns	True	UBR

Rx Traffic Information

Addr Indx	Rx Traffic Descriptor	Type	Peak Rate	Rx QoS	Best Effort
1	NoCLP	NoSCR	353208	Uns	True
2	NoCLP	NoSCR	353208	Uns	True

Acceptable Tx Traffic Information

Addr Indx	Tx Traffic Descriptor	Type	Peak Rate	Tx QoS	Best Effort	Priority
1	NoCLP	NoSCR	353208	Uns	True	UBR
2	NoCLP	NoSCR	353208	Uns	True	UBR

Acceptable Rx Traffic Information

Addr Indx	Rx Traffic Descriptor	Type	Peak Rate	Rx QoS	Best Effort
1	NoCLP	NoSCR	353208	Uns	True
2	NoCLP	NoSCR	353208	Uns	True

Addr Indx. An index that you can use to identify ATM addresses in this display. The index numbers are consistent throughout the rows in this display.

ATM Address. The ATM address for which QoS parameters were configured in the **cva** command.

Description. A textual description of up to 30 characters for this virtual connection. Entered through the **cva** command.

VPI. The virtual path identifier for this ATM address.

VCI. The virtual channel identifier for this ATM address. This value is specified during the virtual channel creation procedure via the **cva** command.

Conn Type. Connection Type. Indicates whether this connection is a virtual path or a virtual channel. All ATM access connections, or uplink connections, are virtual channels. Therefore, this column will always display as **VCC** (Virtual Channel Connection).

VC Type. The virtual channel type is configured with the **map** command. All circuit types for each ATM port will be the same. The circuit type can be either **PVC** (Permanent Virtual Circuit) or **SVC** (Switched Virtual Circuit).

Tx Max SDU. The maximum frame size for traffic transmitted on this connection. This value is configured via the **cva** command.

Rx Max SDU. The maximum frame size for traffic received on this connection. This value is configured via the **cva** command.

Arp Server. Indicates whether this address is an ARP server.

Traffic information is supplied for Transmit (Tx) and Receive (Rx) traffic. These variables are **Tx/Rx Traffic Descriptor Type**, **Peak Rate**, **Tx/Rx QoS**, and **Best Effort**. On the ASX-M-622RF-1W module, the **vva** command also displays the **Priority** variable. Descriptions for these variables are provided in the section, *Creating a Virtual Channel Connection* on page 33-15.

Viewing the ATM Layer Statistics Table

The **vl**s command displays the ATM Layer Statistics Table. This table includes information at the ATM Service Data Unit (SDU), ATM cell, and octet level. Information for SDUs, which are composed of cells, are directly related to statistics for cells. When an SDU is counted, the cells in that SDU are counted and then added to the corresponding cell count.

The following is a sample **vl**s display:

ATM Layer Statistics							
Slot	Port	Rx SDUs	Tx SDUs	Rx Cells	Tx Cells	Rx Octets	Tx Octets
2	1	0	6716	0	15775	0	757200
2	2	4104	13108	6945	18357	333360	881136
5	1	0	0	0	0	0	0
5	2	0	0	0	0	0	0

Rx SDUs. The number of Service Data Units received on this port.

Tx SDUs. The number of Service Data Units transmitted on this port.

Rx Cells. The number of cells received on this port. The value is derived from the **Rx SDUs** statistic. Once an SDU is received on the port, the cells in the SDU are counted and added to this statistic.

Tx Cells. The number of cells transmitted on this port. The value is derived from the **Tx SDUs** statistic. Once an SDU is transmitted on the port, the cells in the SDU are counted and added to this statistic.

Rx Octets. The number of octets, or bytes, received in the form of SDUs on this port.

Tx Octets. The number of octets, or bytes, transmitted in the form of SDUs on this port.

Viewing the ATM Layer Rx Error Statistics Table

The **vlrs** command displays the ATM Layer Rx (Receive) Error Statistics Table for each ATM access port. This table includes discard and error information at the ATM Service Data Unit (SDU), or frame, level and the ATM cell level.

Note that statistics for SDUs, which are composed of cells, are directly related to statistics for cells. When an SDU error or discard is counted, the cells in that SDU are counted and then added to the corresponding cell discard or error statistic for each port.

The following is a sample **vlrs** display:

ATM Layer Rx SDU Error Statistics							
Slot	Port	Discards	Errors	Invalid Sz	No Buffers	Trash	CRC Errors
3	1	0	0	0	0	0	0
3	2	0	0	0	0	0	0
7	1	0	0	0	0	0	0
7	2	0	0	0	0	0	0

ATM Layer Rx Cell Error Statistics						
Slot	Port	Discards	Errors	No Buffers	Trash	CRC Errors
3	1	0	0	0	0	0
3	2	0	0	0	0	0
7	1	0	0	0	0	0
7	2	0	0	0	0	0

SDU Discards. The number of Service Data Units (SDU), or frames, that have been discarded due to one of the following reasons: an invalid size error, CRC error, invalid format error, the frame was larger than the receive SAR buffer, or the frame was larger than the maximum size allowed on this port. Invalid size and CRC errors are also displayed in this table and described below. An invalid format error occurs when a frame is received in the wrong format. For example, a PTOF frame may be received that should be in 1483 format but instead is in Private encapsulation. The receive SAR buffer size (**Rx SAR Buffer Size**) is configured through the **map** command. The maximum frame size allowed on this port is configured through the **vcv** or **mvc** command.

SDU Errors. The number of Service Data Units that had one or more of the following errors: invalid size, invalid format, frame larger than SAR buffer size, CRC error, or the frame was larger than that allowed on this port. This error statistic will typically match the **SDU Discards** statistic.

SDU Invalid Size. The number of Service Data Units, or frames, received that are either larger than the receive frame buffer or had an AAL5 length mismatch. One cell in an SDU contains an AAL trailer that includes a length field; an AAL5 mismatch error occurs when that length field is incorrect. The receive frame buffer size (**Rx Frame Buffer Size**) is configured through the **map** command.

SDU No Buffers. The number of SDUs that were discarded because there was no room in the receive frame buffer. Note that the SDUs counted in this statistic are not included in the **Rx SDU Discards** or **Errors** statistics in the **vlrs** display. The receive frame buffer size (**Rx Frame Buffer Size**) may be configured through the **map** command.

SDU Trash. The number of Service Data Units that were discarded at the ATM physical layer. These SDUs were discarded by the Segmentation and Reassembly (SAR) due to a lack of reassembly buffer space. Note that the SDUs counted in this statistic are not included in the **Rx SDU Discards** or **Errors** statistics in the **vlrs** display.

SDU CRC Errors. The number of SDUs received with errors in the CRC (cyclical redundancy check) header. This error is counted in the **Rx SDU Discards** and **Errors** columns of the **vlrs** display.

Cell Discards. The total number of cells discarded as a result of SDU Discards. SDUs are discarded due to invalid size, CRC errors, invalid format, frame size larger than SAR buffer, or frame size larger than allowed on this port. For each SDU discarded, the number of cells within that SDU are counted and then added to this statistic.

Cell Errors. The total number of cells within SDUs that had one or more of the following errors: invalid size, invalid format, frame larger than SAR buffer size, CRC error, or the frame was larger than that allowed on this port. For each errored SDU, the number of cells within that SDU are counted and then added to this statistic.

Cell No Buffers. The total number of cells that were discarded because there was no room in the receive frame buffer. Note that the cells counted in this statistic are not included in the **Rx Cell Discards** or **Errors** statistics in the **vlrs** display.

Cell Trash. The total number of cells that were discarded at the ATM physical layer. These cells were discarded by the Segmentation and Reassembly (SAR) due to a lack of reassembly buffer space. Note that the cells counted in this statistic are not included in the **Rx Cell Discards** or **Errors** statistics in the **vlrs** display.

Cell CRC Errors. The number of cells received with errors in the CRC (cyclical redundancy check) header. This error is counted in the **Rx Cell Discards** and **Errors** columns of the **vlrs** display.

ATM Layer Receive Error Statistics Table For One ATM Access Module

To view the ATM Layer receive error statistics table on a single ATM access module, you enter the **vlrs** command along with the slot number for the ATM access module as follows:

```
vlrs <slot>
```

where **<slot>** is the slot number where the CSM board is installed. For example, if you wanted to obtain status information for the board in slot 3, you would enter:

```
vlrs 3
```

This command displays a screen similar to the following:

ATM Layer Rx SDU Error Statistics							
Slot	Port	Discards	Errors	Invalid Sz	No Buffers	Trash	CRC Errors
3	1	0	0	0	0	0	0
3	2	0	0	0	0	0	0

ATM Layer Rx Cell Error Statistics						
Slot	Port	Discards	Errors	No Buffers	Trash	CRC Errors
3	1	0	0	0	0	0
3	2	0	0	0	0	0

Descriptions of the columns included in this display are described earlier in *Viewing the ATM Layer Rx Error Statistics Table* on page 33-46.

ATM Layer Receive Error Statistics Table For One ATM Access Port

To view ATM Layer receive error statistics on a single ATM access port, you enter the **vlrs** command along with the slot number for the ATM access module and the port number for which you want to receive information, as follows:

vlrs <slot>/<port>

where **<slot>** is the slot number where the ATM access module is installed and **<port>** is the port number on the ATM access module. For example, if you wanted to view status information for port 2 on the ATM access module in slot 3, you would enter:

vlrs 3/2

This command displays a screen similar to the following:

ATM Layer Rx SDU Error Statistics							
Slot	Port	Discards	Errors	Invalid Sz	No Buffers	Trash	CRC Errors
3	2	0	0	0	0	0	0

ATM Layer Rx Cell Error Statistics						
Slot	Port	Discards	Errors	No Buffers	Trash	CRC Errors
3	2	0	0	0	0	0

Descriptions of the columns included in this display are described earlier in *Viewing the ATM Layer Rx Error Statistics Table* on page 33-46.

Viewing the ATM Layer Tx Error Statistics Table

The **vlts** command displays the ATM Layer Tx (Transmit) Error Statistics Table for each port. This table includes discard and error information at the ATM Service Data Unit (SDU), or frame, level and the ATM cell level.

Note that statistics for SDUs, which are composed of cells, are directly related to statistics for cells. When an SDU error or discard is counted, the cells in that SDU are counted and then added to the corresponding cell discard or error statistic.

The following is a sample **vlts** display.

ATM Layer Tx Error Statistics							
Slot	Port	Tx SDU Discards	Tx SDU Errors	Tx SDU No Buffers	Tx Cell Discards	Tx Cell Errors	Tx Cell No Buffers
2	1	0	0	0	0	0	0
2	2	0	0	0	0	0	0
5	1	0	0	0	0	0	0
5	2	0	0	0	0	0	0

Tx SDU Discards. The number of Service Data Units discarded because there was no room in the transmit SAR buffer or the SDU was larger than the transmit frame buffer. Transmit SAR buffer size (**Tx SAR Buffer Size**) and transmit frame buffer size (**Tx Frame Buffer Size**) are configured through the **map** command.

Tx SDU Errors. The number of Service Data Units that were received from the switch back-plane in an invalid format.

Tx SDU No Buffers. The number of SDUs that were discarded because there was no room in the transmit frame buffer to dequeue and attempt to transmit frames. Note that the SDUs counted in this statistic are not included in the **Tx SDU Discards** statistic. The transmit frame buffer size (**Tx Frame Buffer Size**) is configured through the **map** command.

Tx Cell Discards. The total number of cells discarded as a result of SDU Discards. SDUs are discarded because there is no room in the transmit SAR buffer, or the SDU was larger than the transmit frame buffer. For each SDU discarded, the number of cells within that SDU are counted and then added to this statistic.

Tx Cell Errors. The total number of cells within SDUs that were received from the switch back-plane in an invalid format.

Tx Cell No Buffers. The total number of cells within SDUs that were discarded because there was no room in the transmit frame buffer. Note that the cells counted in this statistic are not included in the **Tx Cell Discards** statistic.

ATM Layer Transmit Error Statistics Table For One ATM Access Module

To view the ATM Layer transmit error statistics table on a single ATM access module, you enter the **vlts** command along with the slot number for the ATM access module as follows:

```
vlts <slot>
```

where **<slot>** is the slot number where the ATM access module is installed. For example, if you wanted to obtain status information for the board in slot 5, you would enter:

```
vlts 5
```

This command displays a screen similar to the following:

ATM Layer Tx Error Statistics							
Slot	Port	Tx SDU Discards	Tx SDU Errors	Tx SDU No Buffers	Tx Cell Discards	Tx Cell Errors	Tx Cell No Buffers
5	1	0	0	0	0	0	0
5	2	0	0	0	0	0	0

Descriptions of the columns included in this display are described earlier in *Viewing the ATM Layer Tx Error Statistics Table* on page 33-50.

ATM Layer Transmit Error Statistics Table For One ATM Access Port

To view ATM Layer transmit error statistics on a single ATM access port, you enter the **vlts** command along with the slot number for the ATM access module and the port number for which you want to receive information, as follows:

```
vlts <slot>/<port>
```

where **<slot>** is the slot number where the ATM access module is installed and **<port>** is the port number on the ATM access board. For example, if you wanted to view status information for port 2 on the ATM access module in slot 5, you would enter:

```
vlts 5/2
```

This command displays a screen similar to the following:

ATM Layer Tx Error Statistics							
Slot	Port	Tx SDU Discards	Tx SDU Errors	Tx SDU No Buffers	Tx Cell Discards	Tx Cell Errors	Tx Cell No Buffers
5	2	0	0	0	0	0	0

Descriptions of the columns included in this display are described earlier in *Viewing the ATM Layer Tx Error Statistics Table* on page 33-50.

Viewing the ATM Connection Statistics Table

The **vcs** command displays the ATM Connection Statistics Table for each virtual channel. This table includes information at the ATM Service Data Unit (SDU), ATM cell, and octet level. Information for SDUs, which are composed of cells, are directly related to statistics for cells. When an SDU is counted, the cells in that SDU are counted and then added to the corresponding cell count.

◆ Note ◆

Information is displayed for a virtual channel only if that channel has been used for data transmission. If a virtual channel has been configured, but not used, then it will not be displayed by **vcs**.

The following is a sample **vcs** display:

ATM Connection Statistics									
Slot	Port	VPI	VCI	Rx SDUs	Tx SDUs	Rx Cells	Tx Cells	Rx Octets	Tx Octets
2	1	0	100	0	6769	0	15892	0	762816
2	2	0	1002	0	349	0	1047	0	50256
2	2	0	1004	0	2445	0	2445	0	117360
2	2	0	1005	0	350	0	1050	0	50400
2	2	0	1007	0	2445	0	2445	0	117360
2	2	0	1008	350	350	1050	1050	50400	50400
2	2	0	1010	679	679	679	679	32592	32592
2	2	0	101	375	353	1142	1056	54816	50688
2	2	0	1013	679	681	679	681	32592	32688
2	2	0	1014	350	352	1050	1055	50400	50640
2	2	0	1016	681	682	681	682	32688	32736
2	2	0	1017	354	367	1058	1112	50784	53376
2	2	0	1019	679	679	679	679	32592	32592
2	2	0	1021	0	1052	0	2104	0	100992
2	2	0	1022	0	2452	0	2452	0	117696
7	1	0	5	6650	6671	6650	6921	319200	332208
7	1	0	16	462	472	924	944	44352	45312
7	2	0	1015	462	464	924	928	44352	44544
7	2	0	1016	6650	6651	6900	6651	331200	319248
7	2	0	1017	318	346	959	1027	46032	49296
7	2	0	1019	5212	5213	5212	5213	250176	250224
7	2	0	1022	6319	6321	6319	6321	303312	303408

Slot. The port's slot number.

Port. The port number.

VPI. The virtual path identifier (VPI).

VCI. The virtual channel identifier (VCI).

Rx SDUs. The number of Service Data Units received on this virtual channel.

Tx SDUs. The number of Service Data Units transmitted on this virtual channel.

Rx Cells. The number of cells received on this virtual channel. The value is derived from the **Rx SDUs** statistic. Once an SDU is received on the virtual channel, the cells in the SDU are counted and added to this statistic.

Tx Cells. The number of cells transmitted on this virtual channel. The value is derived from the **Tx SDUs** statistic. Once an SDU is transmitted on the virtual channel, the cells in the SDU are counted and added to this statistic.

Rx Octets. The number of octets, or bytes, received as SDUs on this virtual channel.

Tx Octets. The number of octets, or bytes, transmitted as SDUs on this virtual channel.

Information on the Ports for one ATM Access Module

To view status information on a single ATM access module, you enter the **vcs** command along with the slot number for the ATM access module, as follows:

```
vcs <slot>
```

where the **<slot>** is the slot number where the ATM access module is installed. For example, if you wanted to view status information for the ATM access module in slot 7, you would enter:

```
vcs 7
```

This command displays a screen similar to the following:

ATM Connection Statistics									
Slot	Port	VPI	VCI	Rx SDUs	Tx SDUs	Rx Cells	Tx Cells	Rx Octets	Tx Octets
7	1	0	5	6650	6671	6650	6921	319200	332208
7	1	0	16	462	472	924	944	44352	45312
7	2	0	1015	462	464	924	928	44352	44544
7	2	0	1016	6650	6651	6900	6651	331200	319248
7	2	0	1017	318	346	959	1027	46032	49296
7	2	0	1019	5212	5213	5212	5213	250176	250224
7	2	0	1022	6319	6321	6319	6321	303312	303408

Descriptions of the columns included in this display are described earlier in *Viewing the ATM Connection Statistics Table* on page 33-52.

Information on One Port

To view status information on a single ATM access port, you enter the **vcs** command along with the slot number for the ATM access module and the port number for which you want to receive information, as follows:

```
vcs <slot>/<port>
```

where **<slot>** is the slot number where the ATM access module is installed and **<port>** is the port number on the ATM access module. For example, if you want to view status information for port 2 on the ATM access module in slot 7, you would enter:

```
vcs 7/2
```

This command displays a screen similar to the following:

ATM Connection Statistics									
Slot	Port	VPI	VCI	Rx SDUs	Tx SDUs	Rx Cells	Tx Cells	Rx Octets	Tx Octets
7	2	0	1015	462	464	924	928	44352	44544
7	2	0	1016	6650	6651	6900	6651	331200	319248
7	2	0	1017	318	346	959	1027	46032	49296
7	2	0	1019	5212	5213	5212	5213	250176	250224
7	2	0	1022	6319	6321	6319	6321	303312	303408

Descriptions of the columns included in this display are described earlier in *Viewing the ATM Connection Statistics Table* on page 33-52.

Information on One Virtual Channel

To view status information on a single virtual channel, you enter the **vcs** command along with the slot number for the ATM access module, the port number, the VPI number, and the VCI number for the virtual channel on which you want information, as follows:

```
vcs <slot>/<port> <vpi>/<vci>
```

where **<slot>** is the slot number where the ATM access module is installed, **<port>** is the port number on the ATM access module, and **<vpi>** is the virtual path identifier, and **<vci>** is the virtual channel identifier. For example, if you wanted to obtain status information for the board in slot 7, port 2, VPI 0, and VCI 6650, you would enter:

```
vcs 7/2 0/1016
```

This command displays a screen similar to the following:

ATM Connection Statistics									
Slot	Port	VPI	VCI	Rx SDUs	Tx SDUs	Rx Cells	Tx Cells	Rx Octets	Tx Octets
7	2	0	1016	6650	6651	6900	6651	331200	319248

Descriptions of the columns included in this display are described earlier in *Viewing the ATM Connection Statistics Table* on page 33-52.

Viewing the ATM Connection Rx Error Statistics Table

The **vcrs** command displays the ATM Connection Rx (Receive) Error Statistics Table on a virtual channel-by-virtual channel basis. This table includes discard and error information at the ATM Service Data Unit (SDU), or frame, level and the ATM cell level for each virtual channel.

Note that statistics for SDUs, which are composed of cells, are directly related to statistics for cells. When an SDU error or discard is counted, the cells in that SDU are counted and then added to the corresponding cell discard or error statistic.

The following is a sample **vcrs** display:

ATM Connection Rx SDU Error Statistics									
Slot	Port	VPI	VCI	Discards	Errors	Invalid Sz	No Buffers	Trash	CRC Errors
2	1	0	100	0	0	0	0	0	0
5	1	0	100	0	0	0	0	0	0
5	2	0	100	0	0	0	0	0	0

ATM Connection Rx Cell Error Statistics								
Slot	Port	VPI	VCI	Discards	Errors	No Buffers	Trash	CRC Errors
2	1	0	100	0	0	0	0	0
5	1	0	100	0	0	0	0	0
5	2	0	100	0	0	0	0	0

Slot. The port's slot number.

Port. The port number.

VPI. The virtual path identifier (VPI).

VCI. The virtual channel identifier (VCI).

SDU Discards. The number of Service Data Units (SDU), or frames, that have been discarded due to one of the following reasons: an invalid size error or CRC error. Invalid size and CRC errors are also displayed in this table and described below. The receive SAR buffer size (**Rx SAR Buffer Size**) is configured through the **map** command. The maximum frame size allowed on this virtual connection is configured through the **cvc** or **mvc** command.

SDU Errors. The number of Service Data Units that had one or more of the following errors: an invalid size error or CRC error. This Error statistic will typically match the **SDU Discards** statistic.

SDU Invalid Size. The number of Service Data Units, or frames, received that are either larger than the receive frame buffer or had an AAL5 length mismatch. One cell in an SDU contains an AAL trailer that includes a length field; an AAL5 mismatch error occurs when that length field is incorrect. The receive frame buffer size (**Rx Frame Buffer Size**) is configured through the **map** command.

SDU No Buffers. This statistic is not supported and will display zeroes.

SDU Trash. This statistic is not supported and will display zeroes.

SDU CRC Errors. The number of SDUs received with errors in the CRC (cyclical redundancy check) header. This error is counted in the **Rx SDU Discards** and **Errors** columns of the **vcrs** display.

Cell Discards. The total number of cells discarded as a result of SDU discards. SDUs are discarded due to CRC errors only. For each SDU discarded, the number of cells within that SDU are counted and then added to this statistic.

Viewing the ATM Connection Rx Error Statistics Table

Cell Errors. The total number of cells within SDUs that had one or more CRC errors. For each errored SDU, the number of cells within that SDU are counted and then added to this statistic.

Cell No Buffers. This statistic is not supported and will display zeroes.

Cell Trash. This statistic is not supported and will display zeroes.

Cell CRC Errors. The number of cells received with errors in the CRC (cyclical redundancy check) header. This error is counted in the **Rx Cell Discards** and **Errors** columns of the **vcrs** display.

Viewing the ATM Connection Tx Error Statistics Table

The **vcts** command displays the ATM Connection Tx (Transmit) Error Statistics Table on a virtual channel-by-virtual channel basis. This table includes discard and error information at the ATM Service Data Unit (SDU), or frame, level and the ATM cell level.

Note that statistics for SDUs, which are composed of cells, are directly related to statistics for cells. When an SDU error or discard is counted, the cells in that SDU are counted and then added to the corresponding cell discard or error statistic.

The following is a sample **vcts** display.

ATM Connection Tx Error Statistics									
Slot	Port	VPI	VCI	Tx SDU Discards	Tx SDU Errors	Tx SDU No Buffers	Tx Cell Discards	Tx Cell Errors	Tx Cell No Buffers
2	1	0	100	0	0	0	0	0	0
2	2	0	1002	0	0	0	0	0	0
2	2	0	1004	0	0	0	0	0	0
2	2	0	1005	0	0	0	0	0	0
2	2	0	1007	0	0	0	0	0	0
2	2	0	1008	0	0	0	0	0	0
2	2	0	1010	0	0	0	0	0	0
2	2	0	1011	0	0	0	0	0	0
2	2	0	1013	0	0	0	0	0	0
2	2	0	1014	0	0	0	0	0	0
2	2	0	1016	0	0	0	0	0	0
2	2	0	1017	0	0	0	0	0	0
2	2	0	1019	0	0	0	0	0	0
2	2	0	1021	0	0	0	0	0	0
2	2	0	1022	0	0	0	0	0	0
5	1	0	100	0	0	0	0	0	0
5	2	0	100	0	0	0	0	0	0

Slot. The port's slot number.

Port. The port number.

VPI. The virtual path identifier (VPI).

VCI. The virtual channel identifier (VCI).

Tx SDU Discards. The number of Service Data Units discarded because there was no room in the transmit SAR buffer or the SDU was larger than the transmit frame buffer. Transmit SAR buffer size (**Tx SAR Buffer Size**) and transmit frame buffer size (**Tx Frame Buffer Size**) are configured through the **map** command.

Tx SDU Errors. The number of Service Data Units that were received from the switch backplane in an invalid format.

Tx SDU No Buffers. The number of SDUs that were discarded because there was no room in the transmit frame buffer to dequeue and attempt to transmit frames. Note that the SDUs counted in this statistic are not included in the **Tx SDU Discards** statistic. The transmit frame buffer size (**Tx Frame Buffer Size**) is configured through the **map** command.

Viewing the ATM Connection Tx Error Statistics Table

Tx Cell Discards. The total number of cells discarded as a result of SDU Discards. SDUs are discarded because there is no room in the transmit SAR buffer, or the SDU was larger than the transmit frame buffer. For each SDU discarded, the number of cells within that SDU are counted and then added to this statistic.

Tx Cell Errors. The total number of cells within SDUs that were received from the switch back-plane in an invalid format.

Tx Cell No Buffers. The total number of cells within SDUs that were discarded because there was no room in the transmit frame buffer. Note that the cells counted in this statistic are not included in the **Tx Cell Discards** statistic.

Displaying the Number of ATM Connections on a Switch

You use the **vnac** command to display the total number of ATM connections on a switch. To use this command, enter

```
vnac
```

at the system prompt. A screen similar to the following will be displayed.

```
Current number of atm connections = 0
```

To display the total number of Point-to-Multipoint connections on a switch, use the **vnapc** command. To use this command, enter

```
vnapc
```

at the system prompt. A screen similar to the following will be displayed.

```
Current number of atm PTOMP connections = 0
```

Traffic Shaping (ASM2/ASX Modules)

Older ASM modules are capable of transmitting ATM cells on a “best effort” basis; that is, no specific traffic parameters can be set up for a given ASM port. Newer ASM2, FCSM II, and ASX module ports allow you to configure several traffic parameters. These parameters include the Peak Cell Rate (PCR), Sustaining Cell Rate (SCR), and Maximum Burst Size (MBS). Traffic shaping using these parameters takes place on data that is exiting (i.e., transmitted out) a switch port.

You can divide ASM2 and ASX ports into discrete “bandwidth groups” to which you can assign unique PCR, SCR, and MBS values. This feature, referred to as “traffic shaping,” can be configured on all Omni Switch/Router ATM access ports and on the following OmniSwitch ATM access modules:

- ASM2-155F
- ASM2-155RF
- ASM2-622F
- ASM2-622RF
- ASM2-DS3
- ASM2-E3
- FCSM II (ASM half)

◆ Note ◆

Traffic shaping is *not* supported on the FCSM I (FCSM-155).

On each ASM2 or ASX port you can configure up to eight (8) bandwidth groups. A bandwidth group is a reserved amount of bandwidth on the port. Bandwidth groups are ordered by priority, with bandwidth group 1 having the highest priority and bandwidth group 8 the lowest. Documentation for User Interface commands to configure and display traffic shaping parameters begin on page 33-68.

Bandwidth groups are associated with ATM services. When you configure any ATM service on an ASM2 or ASX port through the **cas** command, you are prompted for the bandwidth group to which the service will be associated. By default a service will be associated with bandwidth group 1. ATM services are described in Chapter 36, “Configuring ATM Services.”

◆ Important Note ◆

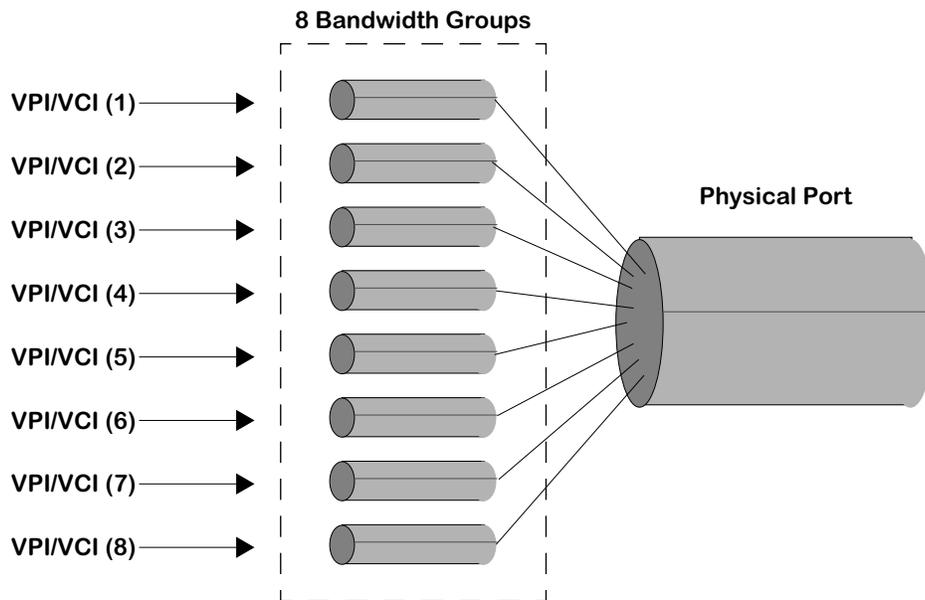
The ASX-M-622RF-1W uses VC-based traffic shaping and not bandwidth groups. See *Traffic Shaping Parameters for the ASX-M-622RF-1W Module* on page 33-19 for documentation on traffic shaping for this module.

Traffic Shaping Overview

The SAHI ASIC used on ASM2/ASX modules supports Traffic Shaping over PVCs and SVCs by using a dual Leaky Bucket Algorithm on Peak Cell Rate (PCR), Sustainable Cell Rate (SCR), and Maximum Burst Size (MBS) parameters. PCR defines the maximum cell rate, SCR defines the average cell rate, and MBS defines the number of cells transmitted at PCR.

The SAHI ASIC has 8 transmit descriptor rings that are hardwired to a VBR/UBR (Variable Bit Rate/Unspecified Bit Rate) service. Each of these 8 descriptor rings is associated with a Leaky Bucket Algorithm.

There are 8 Bandwidth Groups associated with the 8 Leaky Bucket Algorithms. You can configure values for PCR, SCR, and MBS for each bandwidth group and the leaky buckets are programmed based on the SAHI ASIC specification.



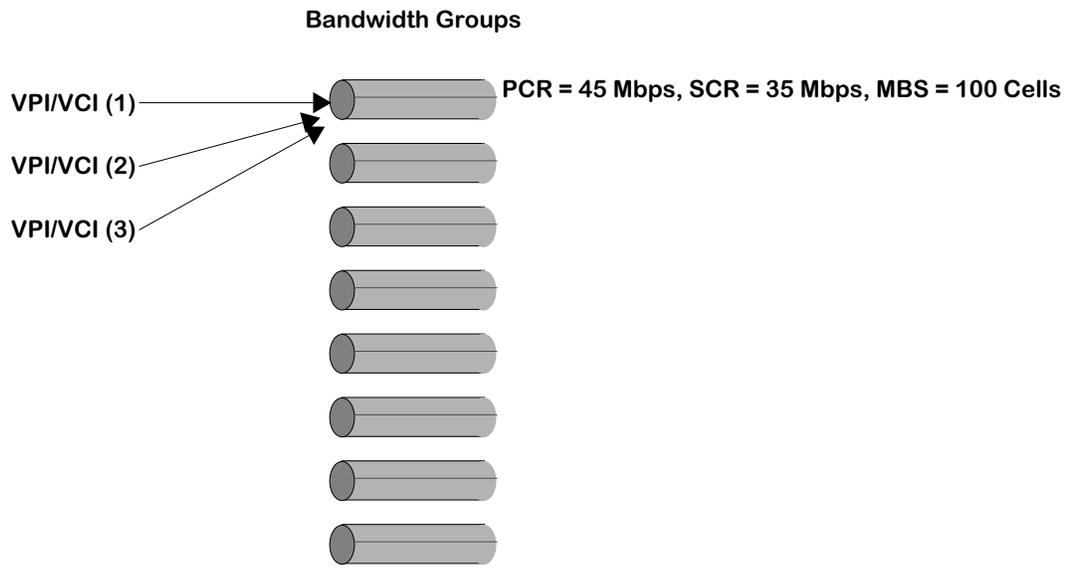
Eight Bandwidth Groups on ASM2/ASX Ports

The SAHI ASIC also prioritizes the Bandwidth Groups. The first 4 Bandwidth Groups are related to VBR channels and the next 4 to the UBR channels.

Within each type of channel (UBR or VBR), the lower Bandwidth Group number has higher priority than the higher number and VBR channels have higher priority than UBR channels. The SAHI ASIC transmits the packets from high to low priority. Hence Bandwidth Group 1 has higher priority than bandwidth group 2 and so on.

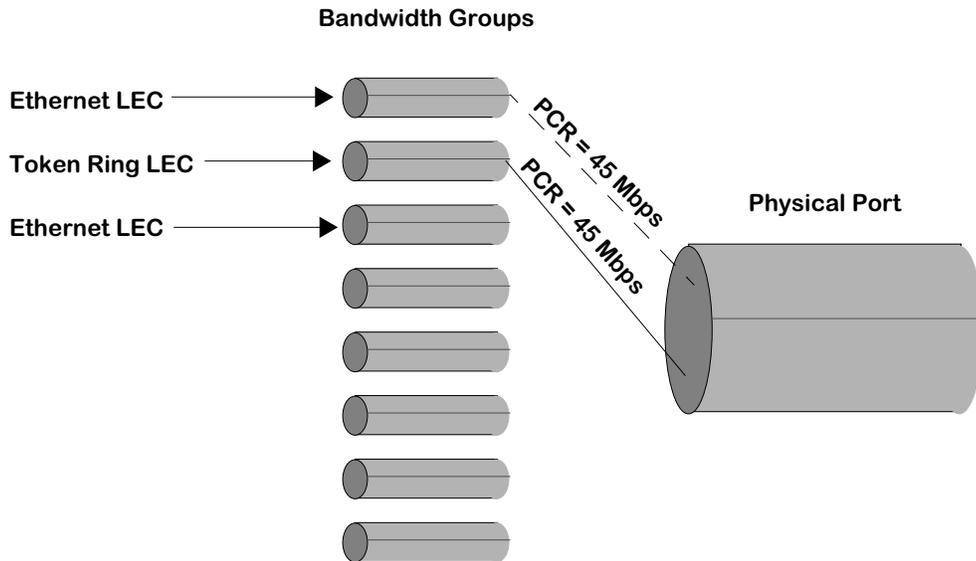
Each VC is associated with a particular bandwidth group. Both PVC and SVC services can be traffic shaped. You must assign the service to a particular bandwidth group when you create a PVC or SVC service. If multiple VCs are created (as a result of the service), all the VCs associated with the service are programmed to the single bandwidth group assigned during creation of the service.

If more than one service is assigned to a single bandwidth group, then all the services assigned to that bandwidth group share the configured bandwidth.



Multiple Services Sharing the Same Bandwidth Group

If traffic parameters are changed under data flow, all the services associated with that bandwidth group have to be restarted. This is done automatically by the traffic shaping software that keeps a tag of all the services associated with the bandwidth group.



Services Using Different Bandwidth Group

You can also modify the service to use a different bandwidth group and that particular service status is toggled to use the new traffic parameters.

Values for Traffic Shaping

With the SAHI ASIC, there are four internal parameters for Traffic Shaping: Prescaler Number, Peak Number, Sustainable Number, and Max_Burst_Number. Two (2) bits of prescaler, five (5) bits of Peak Number, four (4) bits of Sustainable Number, and five (5) bits of Max_Burst_Number are supported. These bits represent the levels of granularity for these values.

The SAHI ASIC can therefore be programmed in discrete levels of PCR, SCR, and MBS. Hence, based on the configured input, the software selects the closest discrete match and programs the SAHI ASIC for the best result.

In order to have the discrete values for the PCR, SCR, and MBS, you have to use the following formulas described below.

PCR Values

The peak cell rate of cell transmission is determined by the values for the prescaler field and the peak rate field. It is defined by the following equation where prescaler is equal to 16, 64, 256, or 1024, and the peak number is a decimal value between 1 and 31.

$$\text{Peak Leaky Bucket Rate} = (40 \text{ MHz} / \text{prescaler}) / \text{peak number}$$

Calculated PCR values (in kilobits per second) are shown in the table below.

PCR Values

Peak Number	PCR (kilobits/second)			
	Prescaler = 16	Prescaler = 64	Prescaler = 256	Prescaler = 1024
1	1060000.00	265000.00	66250.00	16562.50
2	530000.00	132500.00	33125.00	8281.25
3	353333.33	88333.33	22083.33	5520.83
4	265000.00	66250.00	16562.50	4140.63
5	212000.00	53000.00	13250.00	3312.50
6	176666.67	44166.67	11041.67	2760.42
7	151428.57	37857.14	9464.29	2366.07
8	132500.00	33125.00	8281.25	2070.31
9	117777.78	29444.44	7361.11	1840.28
10	106000.00	26500.00	6625.00	1656.25

continued on next page...

PCR Values (Cont.)

Peak Number	PCR (kilobits/second)			
	Prescaler = 16	Prescaler = 64	Prescaler = 256	Prescaler = 1024
11	96363.64	24090.91	6022.73	1505.68
12	88333.33	22083.33	5520.83	1380.21
13	81538.46	20384.62	5096.15	1274.04
14	75714.29	18928.57	4732.14	1183.04
15	70666.67	17666.67	4416.67	1104.17
16	66250.00	16562.50	4140.63	1035.16
17	62352.94	15588.24	3897.06	974.26
18	58888.89	14722.22	3680.56	920.14
19	55789.47	13947.37	3486.84	871.71
20	53000.00	1325000	3312.50	828.13
21	50476.19	12619.05	3154.76	788.69
22	48181.82	12045.45	3011.36	752.84
23	46086.96	11521.74	2880.43	720.11
24	44166.67	11041.67	2760.42	690.10
25	42400.00	10600.00	2650.00	662.50
26	40769.23	10192.31	2548.08	637.02
27	39259.26	9814.81	2453.70	613.43
28	37857.14	9464.29	2366.07	591.52
29	36551.72	9137.93	2284.48	571.12
30	35333.33	8833.33	2208.33	552.08
31	34193.55	8548.39	2137.10	534.27

Calculated PCR values (in cells per second) are shown in the table below.

PCR Values

Peak Number	PCR (cells/second)			
	Prescaler = 16	Prescaler = 64	Prescaler = 256	Prescaler = 1024
1	2500000	625000	156250	39062
2	1250000	312500	78125	19531
3	833333	208333	52083	13020
4	625000	156250	39062	9765
5	500000	125000	31250	7812
6	416666	104166	26041	6510
7	357142	89285	22321	5580
8	312500	78125	19531	4882
9	277777	69444	17361	4340
10	250000	62500	15625	3906
11	227272	56818	14204	3551
12	208333	52083	13020	3255
13	192307	48076	12019	3004
14	178571	44642	11160	2790
15	166666	41666	10416	2604

continued on next page...

PCR Values (Cont.)

Peak Number	PCR (cells/second)			
	Prescaler = 16	Prescaler = 64	Prescaler = 256	Prescaler = 1024
16	156250	39062	9765	2441
17	147058	36764	9191	2297
18	138888	34722	8680	2170
19	131578	32894	8223	2055
20	125000	31250	7812	1953
21	119047	29761	7440	1860
22	113636	28409	7102	1775
23	108695	27173	6793	1698
24	104166	26041	6510	1627
25	100000	25000	6250	1562
26	96153	24038	6009	1502
27	92592	23148	5787	1446
28	89285	22321	5580	1395
29	86206	21551	5387	1346
30	83333	20833	5208	1302
31	80645	20161	5040	1260

SCR Values

The sustain rate of cell transmission is determined by the peak rate and the value of the sustain field. It is defined by the following equation where the sustain number is a decimal value between 1 and 15.

$$\text{Sustain Leaky Bucket Rate} = \text{peak rate} / \text{sustain number}$$

MBS Values

The Maximum Burst Size (MBS) is the maximum number of cells that may be transmitted in a row at peak rate. The MBS is defined as follows where max_burst number is equal to a decimal value between 1 and 31.

$$MBS = 4 * max_burst\ number$$

The table below lists calculated MBS values.

MBS Values

4	8	12	16	20	24	28	32	36	40
48	52	56	60	64	68	72	76	80	84
88	92	96	100	104	108	112	116	120	124

Configuration Guidelines

By default, all connections are “best effort” and at full rate (353208 cells/second). Therefore, you need to modify the traffic descriptor and choose the best effort parameter to be **false**. To do this, use the **mbwg** command, which is described in *Configuring ASM2/ASX Traffic Shaping* on page 33-68. You can then specify the Traffic Shaping parameters documented in the sections above.

While creating a new service via the **cas** command, you will be asked for a bandwidth group for that service. Be careful not to exceed the line speed with the sum of all your SCR when you configure several Bandwidth Groups as it is not possible. Nevertheless, it is possible for the sum of the PCR to exceed the line speed as it is bursts and they will be possible only if there is sufficient bandwidth.

Configuring ASM2/ASX Traffic Shaping

The **mbwg** command allows you to configure the transmit traffic parameters on an ASM2 or ASX port. The syntax for this command is as follows:

```
mbwg <slot>/<port> <bandwidth group number>
```

For example if you wanted to set up bandwidth group 1 on Port 1 of the ASM2 or ASX module in slot 4 you would enter

```
mbwg 4/1 1
```

Follow these steps to set up traffic parameters on an ASM2 or ASX port:

1. Enter **mbwg** followed by the slot number, a slash (/), the ASM2 or ASX port number and then the bandwidth group for which you want to configure parameters. A screen similar to the following displays:

```
The following service numbers use the current Traffic Descriptors
Changing any of the traffic descriptor values would result in
toggling status of the following service numbers...
1
```

```
Bandwidth allocation: Slot 4, Port 1, Bwgid=1
```

```
          Tx Traffic parameters
1) Best Effort {False (1), True (2) }      : TRUE
```

```
Enter (option=value/save/cancel):
```

2. Enter **1=1** at the **Enter (option=value/save/cancel):** prompt to configure traffic parameters. If you enter **1=2**, then traffic will be transmitted on this bandwidth group on a “best effort” basis and you will not be able to configure traffic parameters. A screen similar to the following displays:

```
Bandwidth allocation: Slot 4, Port 1, Bwgid=1
```

```
          Tx Traffic parameters
1) Best Effort {False (1), True (2) }      : FALSE
11) Peak Cell Rate (PCR kbps)             : 540
12) Sustained Cell rate (SCR kbps)        : 50
13) Maximum Burst Size (MBS cells)        : 5
```

```
Enter (option=value/save/cancel):
```

You change a value in a field by entering the line number for the value, an equal sign (=), and then the new value for the variable. For example, to change the **Peak Cell Rate** field to **2000** you would enter an **11** (the line number for **Peak Cell Rate**), an equal sign, and then the new value as follows:

```
11=2000
```

This specification would provide 2 Megabits of bandwidth on this channel.

11) Peak Cell Rate (PCR kbps)

The maximum number of kilobits per second allowed on this bandwidth group. The PCR is specified for all types of ATM traffic. (The minimum value currently supported is 535.)

12) Sustained Cell Rate (SCR kbps)

The maximum *average* cell rate (in kilobits per second) allowed for traffic on this bandwidth group. The SCR is always less than or equal to the Peak Cell Rate. The SCR is not specified for Constant Bit Rate (CBR) traffic as this traffic requires a steady data flow at all times. For CBR traffic, the PCR is equal to the SCR. In the event that the PCR cannot be satisfied due to other configured channels, this channel should at least support the bandwidth you configure here for the SCR.

13) Maximum Burst Size (MBS cells)

The maximum number of cells that can be sent in a burst at the Peak Cell Rate. The MBS is not specified for CBR traffic. CBR traffic is constant and continuous, not bursty. (The valid range is 4 to 64.)

◆ Note ◆

If most of the traffic in a bandwidth group consists of very small packets (i.e., 64 bytes), then the actual speed achieved will be less than the values you configure for PCR, SCR, and MBS.

Viewing Traffic Shaping Parameters

The **vbwg** command allows you to view the traffic descriptor parameters for one or more ASM2 or ASX ports. When you enter

vbwg

a screen similar to the following displays:

Slot	Port	Bwg	Best Effort	PCR (kbps)	SCR (kbps)	MBS (cells)	Dependent Active Service Numbers
4	1	1	True	----	----	----	1
4	1	2	False	20000	20000	5	2
4	1	3	False	20000	20000	5	3
4	1	4	False	20000	20000	5	4
4	1	5	False	20000	20000	5	5
4	1	6	False	20000	20000	5	6
4	1	7	False	20000	20000	5	7
4	1	8	False	20000	20000	5	8
4	2	1	True	----	----	----	1
4	2	2	True	----	----	----	
4	2	3	True	----	----	----	
4	2	4	True	----	----	----	
4	2	5	True	----	----	----	
4	2	6	True	----	----	----	
4	2	7	True	----	----	----	
4	2	8	True	----	----	----	

Slot. The slot in the switch where this ASM2 or ASX module resides.

Port. The port on the ASM2 or ASX module for which information is supplied.

Bwg. The bandwidth group. You can configure up to eight bandwidth groups on each ASM2 or ASX port through the **mbwg** command. Bandwidth groups are ranked by priority with bandwidth group 1 having the highest priority and bandwidth group 8 having the lowest.

Best Effort. Indicates whether or not traffic will be transmitted from this port on a “best effort” basis. When set to **False**, data transmission will be based on the traffic descriptor parameters—PCR, SCR, and MBS—specified through the **mbwg** command. When set to **True**, traffic is transferred on a “Best Effort” basis.

PCR (kbps). The Peak Cell Rate, which is the maximum number of kilobits per second allowed on this bandwidth group.

SCR (kbps). The Sustained Cell Rate, which is the maximum average cell rate (in kilobits per second) allowed for traffic in this bandwidth group. The SCR is always less than or equal to the Peak Cell Rate.

MBS (cells). The Maximum Burst Size, which is the maximum number of cells that can be sent in a burst at the Peak Cell Rate.

Dependent Active Service Numbers. The number for the active ATM service to which this bandwidth group belongs. A bandwidth group is assigned to a service through the **cas** command. Only services that are currently active are displayed.

34 Managing Circuit Emulation Modules

Circuit emulation modules transport traditional T1 or E1 Time Division Multiplexing (TDM) and synchronous serial port traffic over ATM networks. Input data comes from traditional TDM or synchronous serial streams while output data goes out the ATM network in the form of a Constant Bit Rate (CBR) cell stream. Specifically, circuit emulation modules convert T1/E1 bits (or T1/E1 DS0 bundles) and serial data to ATM AAL1 cells.

Circuit Emulation modules (the ASM-CE and the CSM-CE) work best when connected to an ATM network using a single reference clock. This combination is best because circuit emulation is very timing sensitive, requiring the ATM Class of Service with the highest priority and lowest Cell Delay Transfer Variation (CDTV). Circuit Emulation modules process data segmentation and reassembly according to the ATM Forum Circuit Emulation Service Interoperability Specification (CES-IS), version 2.

T1 and E1 ports support structured or unstructured data transfer, which you can configure through software. Additional T1/E1 configuration options include frame format, line coding, and Facility Datalink Protocol. T1 and E1 ports also support synchronous, Synchronous Residual Time Stamp (SRTS), and adaptive clocking. Circuit Emulation modules can store up to 24 hours of performance statistics for local and remote ports.

◆ Note ◆

Additional overview and configuration information on T1/E1 ports can be found in Chapter 53, “Managing T1 and E1 Ports.”

This chapter is divided into two parts. The first part provides an overview of circuit emulation services and an application example. This first part runs from this page through page 34-10. The second part describes the configuration of the logical circuit emulation services supported on T1/E1 ports and the serial ports; this second part starts with the section, *The Circuit Emulation Menu* on page 34-11.

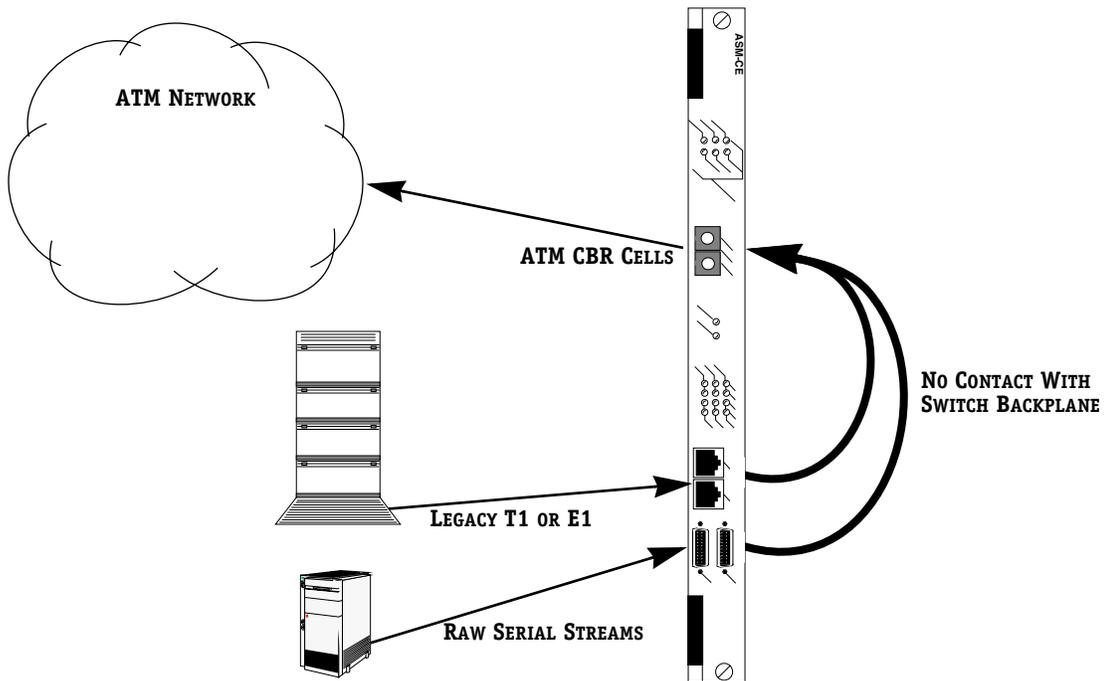
◆ Important Note ◆

Circuit emulation and standard ATM services (e.g., CIP, PTOp, 1483 routed) are *not* supported on the same Virtual Circuit (VC).

The ASM-CE

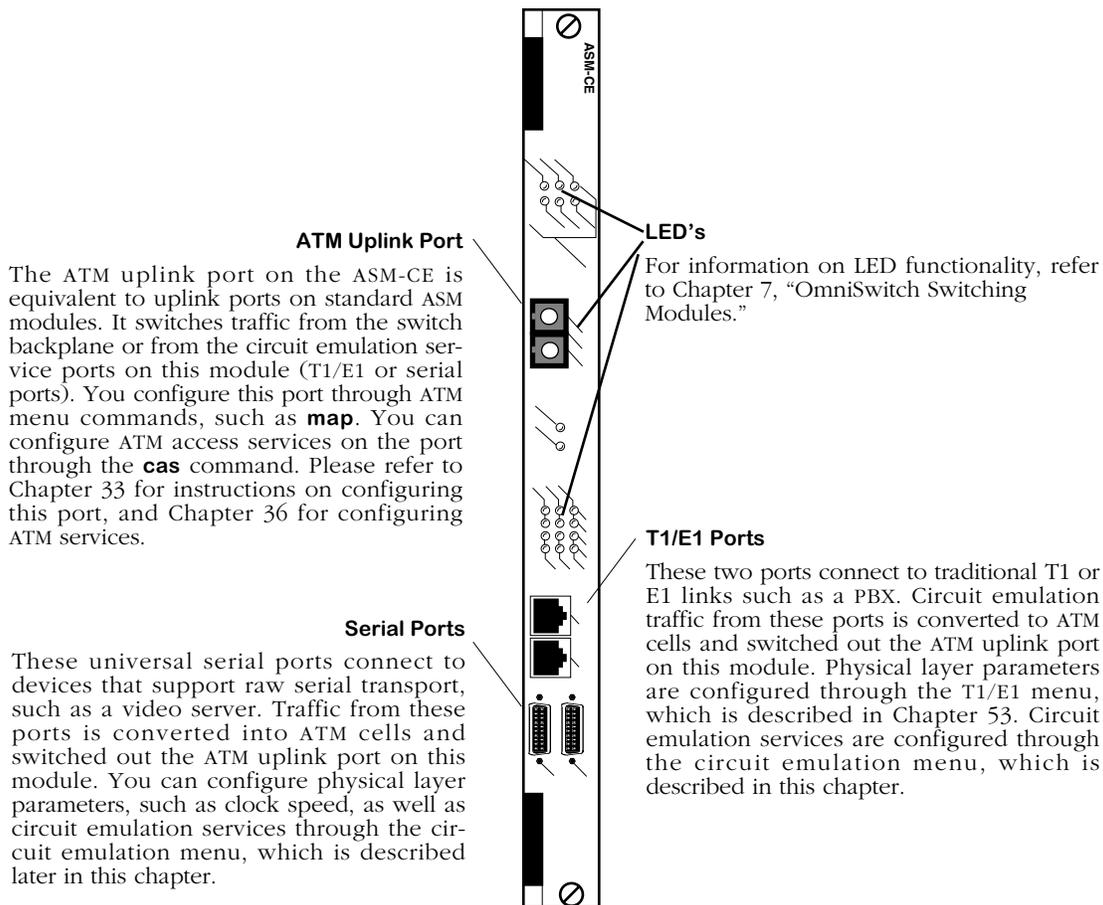
In addition to T1/E1 ports, all ASM-CE modules contain two synchronous serial ports. Serial ports support speeds from 56 KBPS to 2048 KBPS. Cable types used with serial ports can be V.35, X.21, RS-232, RS-449, or RS-530. Serial ports automatically detect cable type and initialize line drivers dynamically. Serial ports support unstructured data transfer only; they also support synchronous and Synchronous Residual Time Stamp (SRTS) clocking, but not adaptive clocking.

Unlike other switch modules, incoming circuit emulation traffic on an ASM-CE has no interaction with the switch backplane. Data from T1/E1 ports and serial ports comes into the ASM-CE and goes back out the ATM uplink port on the same ASM-CE module. The ATM uplink port may be factory configured as OC-3 (single mode or multimode), DS-3, or E3.



Data Flow Through a Circuit Emulation ATM Access Module

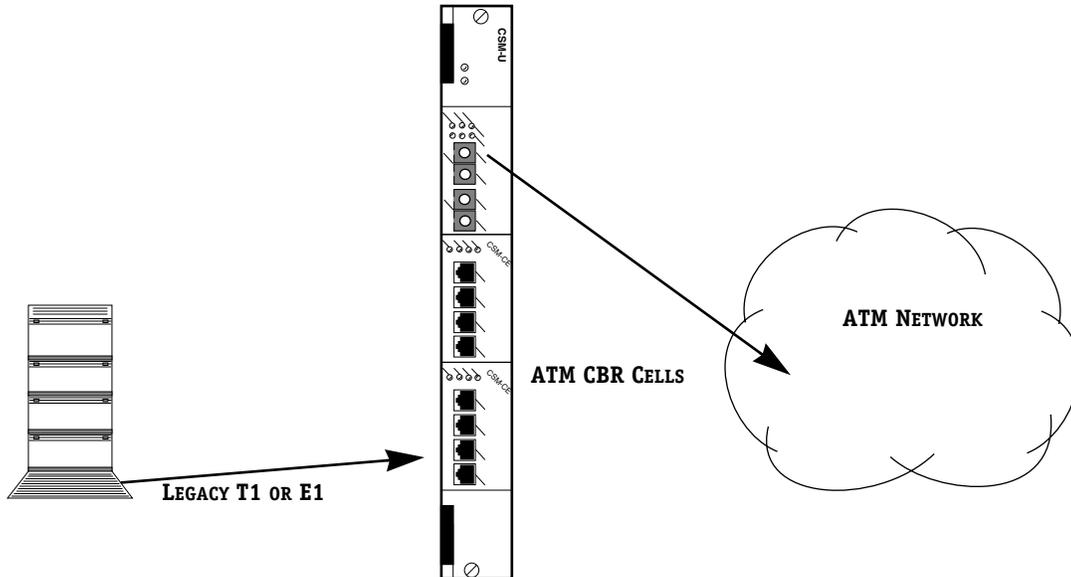
The ASM-CE Ports: An Overview



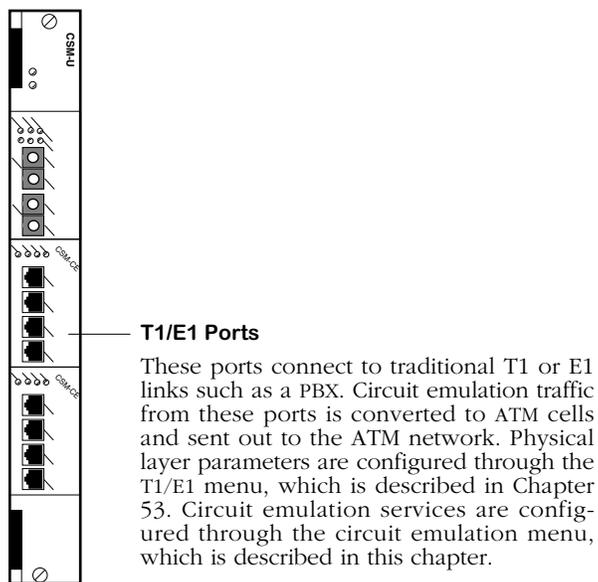
The CSM-CE

CSM-CE ports are part of an adapter board that connects to a CSM-U. Each CSM-U module can contain three adapter boards. This CSM-CE adapter board contains four T1 or E1 ports. Traditional T1/E1 traffic from a device such as a PBX comes in on a T1 or E1 port and is converted into ATM cells. These cells are forwarded directly onto the cell switching matrix. The CSM-CE ports are true ATM switch ports rather than uplink, or access, ports.

The bottom two adapter boards on the CSM-U module in this illustration are CSM-CE boards. Incoming traffic goes directly on the ATM cell switching matrix.



Data Flow Through a CSM Circuit Emulation Module



CSM-CE Ports

Circuit Emulation T1/E1 Ports

Circuit emulation T1/E1 ports are *not* generic ATM ports like the ones on other ASM and CSM modules (e.g., CSM-AB-T1-4W, CSM-AB-IMA-DS1-8W). Internally, a CSM-CE or ASM-CE module is connected to the switch fabric as a single ATM port. The AAL1 SAR receives multiple cell streams from the same internal ATM port, converts them to a traditional TDM T1/E1 stream, and sends them out to appropriate T1/E1 ports based on the VCI of incoming cell streams.

For example, a CSM-AB-CE module is installed in adapter slot No. 1 in a CSM-U in slot 5. If you use the **slot** command, circuit emulation ports 5/1, 5/2, 5/3, and 5/4 will be displayed. (See Chapter 13, “Switch-Wide Parameters,” for more information on the **slot** command.) However, if you execute the **vcs** or **vcv** command, a single CSM port, 5/1, will be displayed. (The **vcv** and **vcs** commands are described in Chapter 41, “Managing Cell Switching Modules (CSMs),” for CSMs and in Chapter 33, “Managing ATM Access Modules,” for ASMs.)

If, for example, you create the following four (4) circuit emulation circuits with the **ceadd** command (which is described in *Creating a Virtual Channel Connection on a T1/E1 Port* on page 34-12):

```
ceadd 5/1 256
ceadd 5/2 288
ceadd 5/3 320
ceadd 5/4 352
```

The **vcv** and **vcs** commands will display these virtual circuits as 5/1 0/256, 5/1 0/288, 5/1 0/320, and 5/1 0/352. In this example, the AAL1 SAR receives and transmits cells *only* from and to port 5/1.

Changes in Release 4.1.4 and Later

In software prior to Release 4.1.4, the **vap** command displayed all four ATM addresses for four CSM-AB-CE ports though logically there is only one ATM port (one ATM address) for all four CSM-AB-CE ports. In a Switched Permanent Virtual Circuit (SPVC) configuration, each CSM-AB-CE port had one corresponding local ATM address.

In Release 4.1.4 and later, the **vap** command only displays one (1) ATM address and also masks out all the other fields that are not applicable for this port. ATM addresses for all ports other than the first port are displayed as **N/A**; all the other non-applicable fields are displayed as dashes (--).

With this change, you need to keep in mind that there is only one (1) ATM address associated with four (4) CSM-AB-CE ports. Different VCs will have a different ATM selector (the least significant byte of the 20-byte ATM address); this selector is still configurable as before. To establish an SPVC connection, both calling and called CSM-AB-CE functions need to be created. The remote ATM address field is the ATM address of the remote port (*one* ATM address for the module) appended by the unique selector byte of the remote CSM-AB-CE connection.

◆ Note ◆

See *Creating a Soft Permanent Virtual Circuit (SPVC) on T1/E1 Ports* on page 34-17 for more information on configuring SPVCs on CSM-AB-CE submodules.

Configuring a Circuit Emulation Module

The steps to configuring a circuit emulation module depend on whether you have an ASM-CE or a CSM-CE. Due to the different port types on the ASM-CE, configuration of the module requires several general steps. There are differences in the configuration for logical-level circuit emulation parameters, T1/E1 physical parameters, and ATM uplink parameters. These general steps are as follows:

Step 1. Configure T1/E1 Ports

Configure framing, line encoding, signaling and other options through the **temod** command. This command sets up physical level parameters for the T1 or E1 port. This step is required for ASM-CE and CSM-CE modules. See Chapter 53, “Managing T1 and E1 Ports,” for directions on configuring a T1 or E1 port.

◆ **Note** ◆

Serial ports are configured while configuring circuit emulation parameters (in Step 3).

Step 2. Configure ATM Access Port (ASM-CE only)

The ATM port on the ASM-CE is the same port used with standard ASM ATM access modules. You use ATM menu commands to configure the ATM ports on the ASM-CE. This step is required for ASM-CE modules only. See Chapter 33, “Managing ATM Access Modules,” for information on those commands.

Step 3. Configure Circuit Emulation

You configure the circuit emulation service parameters on T1, E1, and serial ports through the **ceadd** and **cemodify** commands. You create circuit emulation virtual circuits through the **ceadd** command. These parameters include VPI, VCI, and Cell Delay Transfer Variation (CDTV). See *Creating a Virtual Channel Connection on a T1/E1 Port* on page 34-12 for T1 and E1 ports, or see *Creating a Virtual Channel Connection on a Serial Port* on page 34-21 for serial ports. This step is required for ASM-CE and CSM-CE modules.

You can also optionally configure port-level circuit emulation parameters, such as service modes and service clock modes, through the **cemodify** command. If you do not configure these port-level parameters, defaults will be assigned to ports.

Circuit Emulation Services

Once data comes into a circuit emulation module through a T1/E1 port or a serial port, it is passed onto the ATM network as ATM cells. There are two services available for segmenting data into ATM cells: structured and unstructured. In general, time slot information will be retained in a structured service and will not be interpreted in an unstructured service. Since serial port data does not use time slots, only an unstructured service is available for these ports.

◆ Note ◆

Circuit emulation and regular ATM services like PTOP are not supported on the same Virtual Circuit (VC).

Unstructured Service

An unstructured circuit emulation service assigns a single virtual circuit to an entire T1 or E1 bit stream. The data stream is segmented into AAL1 cells without regard to any structure in the user data or byte alignment between the user data and the ATM cell payload. Unstructured service is intended primarily for simple point-to-point applications. This service does not require the use of time slots associated with T1 and E1 data traffic. It is the required service for use with the serial ports on an ASM-CE.

The ATM cell format for unstructured service includes a 5-octet ATM cell header and a 1-octet AAL1 header. The 47 octets of data payload contain the T1 or E1 bit level data stream encapsulated in the same order they were received but without any structure. One ATM cell can hold 1.95 T1 frames (193 bit frames) or 1.47 E1 frames (256 bit frames).

Structured Service

In a structured circuit emulation service, time slots are considered before structuring data into ATM cells. Time slots allow a device such as a PBX to switch some data in one direction and other data in another direction. Time slots increase control over traffic and bandwidth.

A structured circuit emulation service preserves this extra control afforded by time slots when TDM traffic is converted to ATM cells. This service supports an $n \times 64$ KBPS data format and assigns any combination of time slots to a virtual connection. Structured service supports up to 24 virtual connections on a T1 port and up to 31 virtual connections on an E1 port. This service can also optionally carry Channel Associated Signaling (CAS) bits.

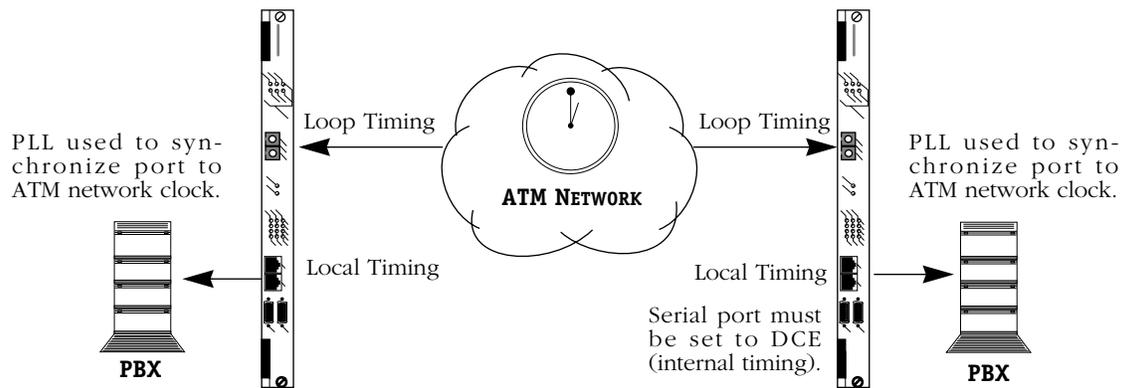
The ATM cell format for a structured service has a 5 octet ATM cell header and a 1- or 2-octet AAL1 header. The 46 or 47 octets of data payload contain the selected T1 or E1 channel and can optionally carry CAS bits. When CAS is included in the cell, it is collected from the appropriate time slots in the appropriate frame and placed at the end of the cell. A 2-octet AAL1 header has a 1-octet pointer (once every 8 cells) to point to the beginning of the multiframe.

Circuit Emulation Clocking Modes

The three service clock modes available for circuit emulation services are synchronous, Synchronous Residual Time Stamp (SRTS), and adaptive. The type of clocking that may be used depends on the circuit emulation service mode chosen. In structured service mode, synchronous and adaptive service clock modes are supported. In unstructured service mode, synchronous, adaptive, and SRTS clocking are supported.

Synchronous Clocking

Synchronous clocking can be used in an ATM network using a single master clock. Synchronous clocking is the most accurate form of clocking for circuit emulation services. The port uses a Phase Lock Loop (PLL) to synchronize to the ATM clock. This allows the port to derive and provide timing from the ATM network to attached devices.

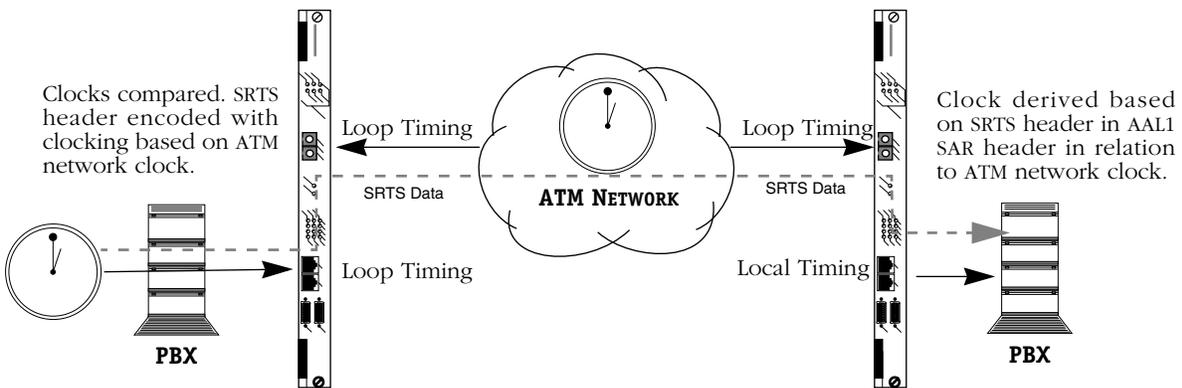


Synchronous Clocking

In a synchronous clocking mode, both sides of the connection (i.e., both circuit emulation ports) will use a local clock source. Therefore, the Transmit Clock Source setting should be set to *local timing*. The timing configuration for the port is shown in the above diagram.

Synchronous Residual Time Stamp (SRTS) Clocking

In SRTS clocking, the ATM network must provide a single master clock. The port receives the clock from the attached device, such as a PBX. The SRTS information is encoded within the AAL1 SAR header. The clock is derived and adjusted as needed on the remote port based on the SRTS information from the AAL1 SAR header.



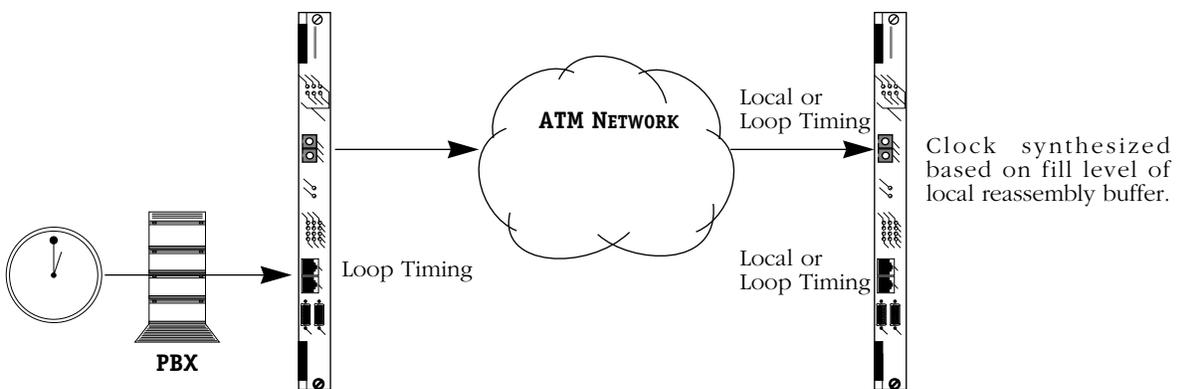
SRTS Clocking

In SRTS clocking, the port receives the clock on one end and regenerates the clock locally on the other end. In such a case, the Transmit Clock Source parameter for the port receiving the clock from the network should be configured to *loop timing* and the other end of the link should be configured to *local timing*.

SRTS clocking is supported on T1, E1, and serial ports. It can only be used with an unstructured circuit emulation service mode. In addition, when used on serial ports, the clocking speed must be set to 1.544 Mbits or 2.048 Mbits.

Adaptive Clocking

In adaptive clocking, the ATM network does not need to be running on a single master clock. The port receives the clock from the attached device, such as a PBX. No information on clocking is passed across the ATM network. The clock is synthesized and adjusted on the remote port based on the fill level of the local ATM reassembly buffer. If the buffer fills too much, the clock frequency is increased; if the buffer fills too little, the clock frequency is decreased. Adaptive clocking is the least accurate form of clocking and the most prone to bit errors.



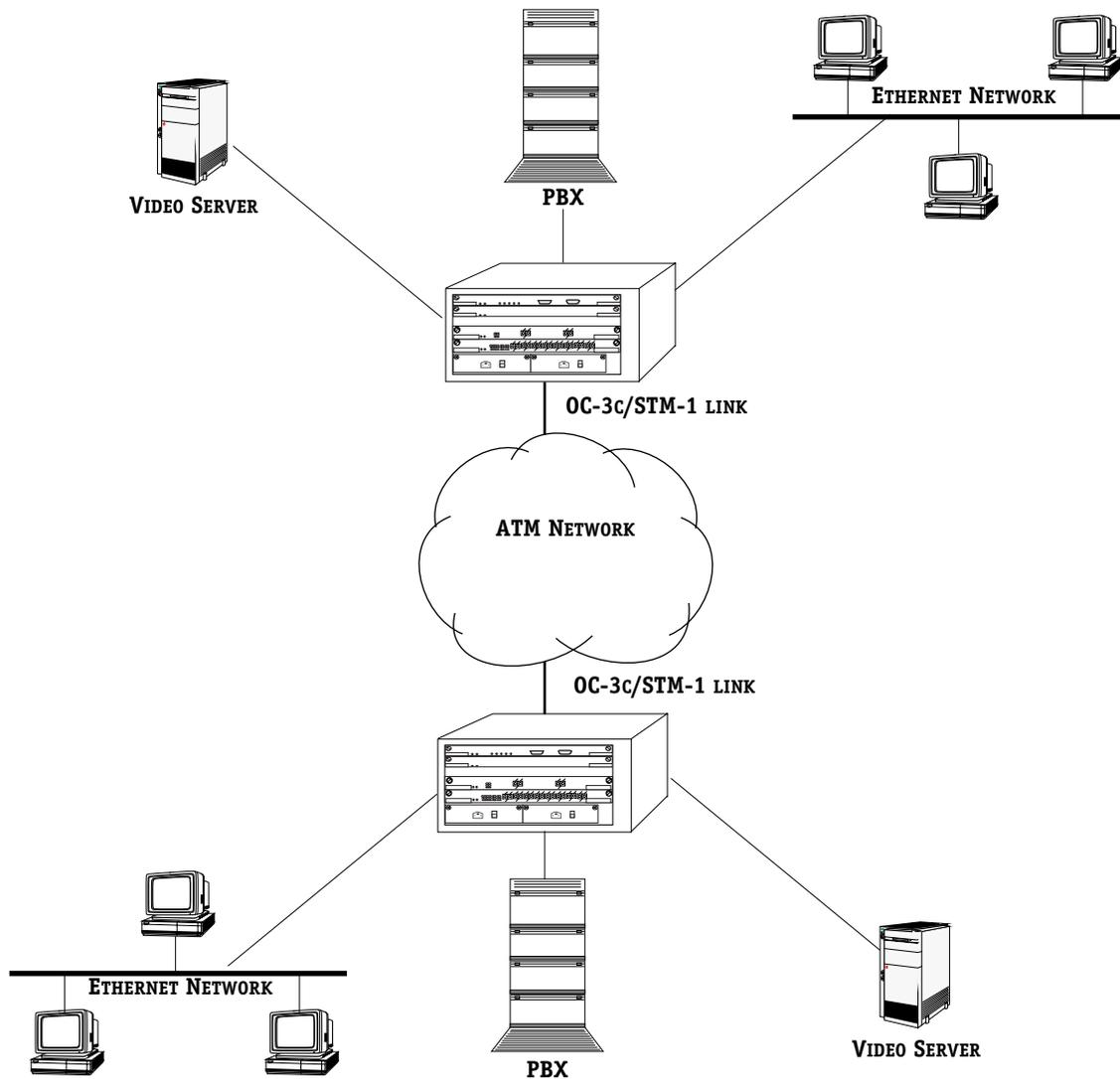
Adaptive Clocking

In adaptive clocking, the module receives the clock on one end and regenerates the clock locally on the other end. In such a case, the Transmit Clock Source parameter for the port receiving the clock from the network should be configured to *loop timing* and the other end of the link should be configured to *local timing*.

Adaptive clocking is supported for T1 and E1 ports only; it is not supported on serial ports.

Application Example - ASM-CE

Circuit emulation modules are typically used in networks in which legacy T1/E1 or synchronous serial traffic needs to be transmitted over an ATM network. The module can accept input from T1/E1 sources, such as a private branch exchange (PBX), or from pure serial traffic sources, such as a video server. The diagram below illustrates a circuit emulation application using an ASM-CE.



Typical Circuit Emulation Configuration

In this example, the PBX connects to one of the T1 ports on the circuit emulation module. The video server on each end of the network connects to one of the serial ports on an ASM-CE. The traffic from both of these sources is muxed and sent out as ATM cells through the ATM port on the ASM-CE. This ATM port in turn connects into the wider ATM network of cell switches. Other traffic, such as 10/100 Ethernet LAN traffic, that connects to the same switch can also be switched out the ATM port on an ASM-CE.

The Circuit Emulation Menu

The commands for configuring and monitoring circuit emulation virtual channel connections are contained in the ATM circuit emulation submenu. These commands control the circuit emulation services on both T1/E1 ports (ASM-CE and CSM-CE) and serial ports (ASM-CE only); they do not affect the ATM uplink port. This submenu displays as shown below and may be accessed (when in verbose mode) by entering **atmce** at a command line.

Command	ATM Circuit Emulation Management Menu
cemodify	Modify a port or a virtual channel configuration
cestatus	View status of a port or a virtual channel connection
ceadd	Create a virtual channel connection
cedelete	Delete a virtual channel connection
cecls	Clear statistics of a virtual channel connection

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

You create virtual channel connections through the **ceadd** command and modify those virtual channels later through the **cemodify** command. You can view the status of virtual channel connections through the **cestatus** command. Additionally, you can configure port-level circuit emulation parameters on T1/E1 ports and serial ports through the **cemodify** command.

Creating a Virtual Channel Connection on a T1/E1 Port

The **ceadd** command allows you to

set up circuit emulation virtual channels for T1 or E1 ports on ASM-CE and CSM-CE submodules.

The configuration parameters in this command are different for T1/E1 ports and serial ports. This section describes options for T1 and E1 ports.

To configure a virtual channel connection on a T1 or E1 port, enter the following command

```
ceadd <slot>/<port> <vci>
```

where **<slot>** is the slot number where the board is located, **<port>** is the T1 or E1 port number on the board (Port 2 or Port 3), and **<vci>** is the virtual channel identifier for the virtual channel that you want to add.

When selecting a VCI, you need to be aware of the ranges available for each circuit emulation port. The following VCI ranges are available for each port:

CSM-CE Port Number *	ASM-CE Port Number	Valid VCI Range
1	2	256–287
2	3	288–319
3	4	320–351
4	5	352–383

* The actual port number is based upon which slot position the board occupies, and whether other modules are installed. Port numbers increment from left to right.

For example, to create a virtual channel with a VCI of 257 on port 2 on an ASM-CE board in switch slot 5, you would enter

```
ceadd 5/2 257
```

A screen similar to the one on the following page displays.

◆ **Note** ◆

If the port is configured for unstructured service, time slot information will not be displayed.

Slot 5 Port 2 Connection 257 Configuration

Available Time Slot:

{1,2,3 }

- 1) Description (30 chars max) : Connection 257
- 2) Administration Status { UP (1), DOWN (2) } : UP
- 4) Partial Cell Fill Count (0-47) : 0
- 5) Cell Loss Integration Period in second (1-64) : 2
- 6) Cell Delay Variation Tolerance in frame (1-255) : 20
- 7) Idle Code (0-FF) : FF
- 8) Reassembly Buffer Size in frame (1-512) : 100
- 9) Time slots used : {4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24}
 (Usage: "+/-<ts|all>" add/remove a time slot. For example, "9=+10+12-9" to add time slot 10 & 12 and remove time slot 9. "9=+all" add all time slots. "9=-all" remove all time slots)
- 10) Connection type { PVC (1), SPVC (2) } : PVC
- 11) ATM uplink slot (1-5) : 3
- 12) ATM uplink port (1-1) : 1
- 13) ATM uplink VPI : 2
- 14) ATM uplink VCI : 2
- 17) Signalling Code (0-F) : 0
- 18) Multicast { Enable (1), Disable (2) } : Disable

Enter (option=value/save/cancel) :

1) Description

Enter a description for this virtual channel connection of up to 30 characters. This description will be used in screen displays to identify this connection.

2) Administration Status

This option enables and disables the virtual circuit you are modifying. Setting this option to **Up** enables the circuit and allows data to be sent or received as long as the Operational Status is also Up. Setting this option to **Down** disables the circuit; no data can be sent on the circuit. The **Down** option is a good option to use when preconfiguring a virtual circuit in advance of live network operation.

4) Partial Cell Fill Count

Enables the partial cell fill count feature, which is used to decrease cell fill delay. In this field, indicate the minimum number of octets of user data allowed per ATM cell. No data cell will be transmitted out the ATM uplink port until it contains the number of bytes you specify here. If you set this parameter to zero (0), the partial cell fill count feature is disabled and all cells will be filled completely before they are sent.

5) Cell Loss Integration Period

The time, in seconds, after which lost cells will be declared lost. When cells are lost, this integration period begins. If cells are not recovered within this period, an internal variable will be set indicating that cells have been lost on this virtual circuit. This may affect statistics counters.

6) Cell Delay Variation Tolerance

The maximum cell delay variation of this virtual circuit in frame increments. One frame is defined as the size of the buffer that can store incoming data for up to time T . In structured mode, T equals 125 ms. In unstructured mode, a frame equals to 32 octets and the corresponding values for T are as follows:

- Unstructured T1 $T = 166$ ms
- Unstructured E1 $T = 125$ ms
- Unstructured serial port $T = 32 * 8 / \text{speed}$

7) Idle Code

The idle character sent to the circuit emulation interface or to the ATM uplink port. This idle character is sent to T1/E1 time slots or to a serial port if the reassembly buffer for this virtual circuit is underrun or overrun. If an alarm is present on the T1/E1 port or if there is a cable drop on the serial port, this idle character will be sent upstream through the ATM network.

8) Reassembly Buffer Size

The maximum size of the ATM reassembly buffer, in frames. This buffer is used by the AAL1 SAR to buffer incoming data on the ATM uplink port. Data in the buffer is later passed on to the appropriate T1/E1 or serial port. This buffer allows some flexibility in the transmission of data to legacy T1/E1 and serial ports due to cell delay variation on the ATM network.

In unstructured mode, a frame equals 32 octets (256 bits). In structured mode, a frame is the number of time slots assigned to this virtual circuit. So, if 5 time slots are assigned to this virtual circuit and this parameter is set to 50, the total buffer size for all time slots in the virtual circuit is 250 bytes (each of the 5 time slots uses 50 bytes).

◆ Note ◆

The Reassembly Buffer Size must be greater than the Cell Delay Variation Tolerance.

9) Time Slots Used

Indicates which time slots this virtual circuit will use. You add time slots by entering **9=** followed by a plus sign (+) and the number of each time slot you want to add. For example to add time slots 14 and 15, you would specify:

9=+14+15

You can also enter a minus sign (-) followed by the number of the time slot you want to delete. For example, to delete time slot 14 from this virtual circuit, enter:

9=-14

◆ Note ◆

This field only appears if the T1/E1 port has been configured for Structured Service Mode. For more information on configuring the T1/E1 port, see *Configuring a Circuit Emulation T1/E1 Port* on page 34-23.

10) Connection Type

The type of VC you want to create, either a Permanent Virtual Circuit (PVC), or a Soft Permanent Virtual Circuit (SPVC). If you enter 2 (SPVC), additional options are displayed. See *Creating a Soft Permanent Virtual Circuit (SPVC) on T1/E1 Ports* on page 34-17 for more information on configuring SPVCs on a CSM-CE port. For more information on PVCs and SPVCs, see Chapter 41, “Managing Cell Switching Modules (CSMs).”

◆ Note ◆

You can only create SPVCs on CSM-CE modules.

11) ATM uplink slot

The slot in this chassis where input circuit emulation traffic will be transmitted. When multicast transmission is disabled, this parameter is used to create point-to-point Virtual Channel Connections (VCCs). On an ASM-CE, this slot is the same slot as this ASM-CE, and may not be changed.

12) ATM uplink port

The port on the circuit emulation module where input circuit emulation traffic is transmitted. When multicast transmission is disabled, this parameter is used to create point-to-point Virtual Channel Connections (VCCs). On an ASM-CE, this port will be Port 1, because the first port will always be used as the uplink port.

13) ATM uplink VPI

This parameter represents the VPI for the permanent virtual circuit on which cell traffic will be sent on the ATM network. When multicast transmission is disabled, this parameter is used to create point-to-point Virtual Channel Connections (VCCs).

◆ Note ◆

This field only appears if the VCI is being added to a T1/E1 port on a CSM-CE submodule.

14) ATM uplink VCI

This parameter represents the VCI for the permanent virtual circuit on which cell traffic will be sent on the ATM network. When multicast transmission is disabled, this parameter is used to create point-to-point Virtual Channel Connections (VCCs).

◆ Note ◆

This field only appears if the VCI is being added to a T1/E1 port on a CSM-CE submodule.

17) Signalling Code

Signaling code is used to carry signaling state information (e.g., on-hook, off-hook, ringing). Signaling bits are composed of four (4) bits for T1 Extended Superframe (ESF) and E1 Multi-frame (MF) or two (2) bits for T1 Superframe (SF).

This field specifies the 4-bit signaling code to be sent to attached and far-end equipment (e.g., alarms, receive cell starvation overflow). To change this parameter, enter a hexadecimal value from **0** to **f**.

◆ Note ◆

This field only applies to T1/E1 ports.

18) Multicast

“Multicast” virtual circuits, also referred to as point-to-multipoint virtual circuits, may be configured on any virtual circuit. Within a multicast virtual circuit, one circuit is the primary, or “root,” circuit and the others are “leaf” circuits. Quality of Service (QoS) and other traffic parameters are set up for the root circuit and these same parameters are inherited by all leaf circuits.

◆ Important Note ◆

Multicast virtual circuits are not supported on circuit emulation SPVCs.

Functionally, a multicast virtual circuit operates by copying a cell for each output leaf circuit and sending that copied cell out each circuit. Data traffic flows from root to leaf, but not from leaf to root. Leaf virtual circuits do not communicate directly with each other on a multicast connection.

Enter **18=2** (the default) to disable multicast transmission or **18=1** (multicast enabled) to make this virtual circuit either a leaf or a root of a point-to-multipoint connection. If you enable multicast transmission, you will be able to configure the circuit as a leaf or root circuit as described below.

If you enable multicast transmission any settings made in options 13 (**ATM uplink VPI**) and 14 (**ATM uplink VCI**) will be ignored. In addition, you must use either use the **cvc** command (for PVCs) or the **scvc** command (for SPVCs) to create the proper multicast Virtual Channel Connection (VCC).

180) Multicast Role

If you have enabled multicast transmission in option 18 above, a new suboption to configure this virtual circuit as a leaf or root circuit will be displayed beneath option 18 (**Multicast**) as shown below.

18) Multicast { Enable (1), Disable (2) }	: Enable
180) Multicast Role { Root (1), Leaf (2) }	: Leaf

Enter **180=2** (the default) to make this virtual connection a leaf virtual circuit or **180=1** to make this the root virtual circuit.

Creating a Soft Permanent Virtual Circuit (SPVC) on T1/E1 Ports

When creating a virtual channel connection for a T1 or E1 port on a CSM-CE module, the VCC can be either a Permanent Virtual Circuit (PVC) or a Soft Permanent Virtual Circuit (SPVC). A PVC is a point to point connection that is configured by the user and remains consistent despite switch restarts. Like PVCs, SPVCs require some user configuration, and are not affected by switch restarts, but use PNNI signaling to establish connections.

It is possible to create a SPVC on a T1 or E1 port, rather than a PVC. The procedure is nearly identical to configuring a PVC on a T1 or E1 port.

To configure a SPVC on a T1 or E1 port:

1. Enter the **ceadd** command as follows:

```
ceadd <slot>/<port> <vci>
```

where **<slot>** is the slot number where the board is located, **<port>** is the T1 or E1 port number on the board, and **<vci>** is the virtual channel identifier for the SPVC that you want to add.

When selecting a VCI, you need to be aware of the ranges available for each Circuit Emulation port. See *Creating a Virtual Channel Connection on a T1/E1 Port* on page 34-12 for the valid VCI ranges for each port.

For example, to create a virtual channel with a VCI of 289 on port 2 in switch slot 5, you would enter

```
ceadd 5/2 289
```

The screen for creating a virtual channel connection appears, as shown:

Slot 5 Port 2 Connection 289 Configuration

Available Time Slot:

```
{1,2,3 }
```

```
1) Description (30 chars max)      : Connection 289
2) Administration Status { UP (1), DOWN (2) }      : UP
4) Partial Cell Fill Count (0-47)      : 0
5) Cell Loss Integration Period in second (1-64)    : 2
6) Cell Delay Variation Tolerance in frame (1-255)  : 20
7) Idle Code (0-FF)                  : FF
8) Reassembly Buffer Size in frame (1-512)          : 100
9) Time slots used : {4, 5, 6, 7, 8, 9, 10, 11, 12,
                    13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24}
   (Usage: "+/-<ts|all>" add/remove a time slot. For example,
   "9=+10+12-9" to add time slot 10 & 12 and remove time slot 9.
   "9=+all" add all time slots. "9=-all" remove all time slots)
10) Connection type { PVC (1), SPVC (2) }          : PVC
11) ATM uplink slot (1-5)                      : 3
12) ATM uplink port (1-1)                      : 1
13) ATM uplink VPI                             : 2
14) ATM uplink VCI                             : 2
17) Signalling Code (0-F)                      : 0
18) Multicast { Enable (1), Disable (2) }        : Disable
```

Enter (option=value/save/cancel) :

◆ Note ◆

If the port is configured for unstructured service, time slot information is not displayed.

2. Configure options 1-9 as you would for a PVC. This procedure is described in *Creating a Virtual Channel Connection on a T1/E1 Port* on page 34-12.
3. Change the **Connection type** from **PVC** to **SPVC** by entering the line number (**10**), an equals sign (=), and then **2** (the value for **SPVC**), as shown:

10=2

The Virtual Channel Connection menu changes. Fields 11 through 14 are removed, and new fields that apply to SPVCs appear, as shown:

Slot 5 Port 1 Connection 256 Configuration

Available Time Slot:

{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16,
17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31}

1) Description (30 chars max) : Connection 256
2) Administration Status { UP (1), DOWN (2) } : UP
4) Partial Cell Fill Count (0-47) : 0
5) Cell Loss Integration Period in second (1-64) : 2
6) Cell Delay Variation Tolerance in frame (1-255) : 10
7) Idle Code (0-FF) : FF
8) Reassembly Buffer Size in frame (1-512) : 20
9) Time slots used : { none }
(Usage: "+/-<ts|all>" add/remove a time slot. For example,
"9=+10+12-9" to add time slot 10 & 12 and remove time slot 9.
"9=+all" add all time slots. "9=-all" remove all time slots)
10) Connection Type { PVC (1), SPVC (2) } : SPVC
100) SVC Mode { Active (1), Passive (2) } : Active
101) Selector for Local ATM Address (1..FF) : 1
11) Remote ATM Address : 00000000000000000000000000000000
12) Remote VPI : 0
13) Remote VCI : 256
14) SVC Retry Interval (0-36000 1/10ths sec) : 10
15) SVC Retry Limit (0-65535) : 0
16) Restart { True (1), False (2) } : False
17) Signalling Code (0-F) : 0
18) Multicast { Enable (1), Disable (2) } : Disable

Enter (option=value/save/cancel) :

◆ Note ◆

This menu can also be accessed through the **scvc** command in the ATM menu. See *Using the SPVC Configuration Command to Configure a CE-SPVC* on page 34-20 for more information.

Descriptions for option 1 (**Description**) through option 10 (**Connection Type**), and option 18 (**Multicast**) are described in *Creating a Virtual Channel Connection on a T1/E1 Port* on page 34-12. Options 3 (**Virtual Path Identifier**) and 100 (**SVC Mode**) through 16 (**Restart**) are described below.

100) SVC Mode

Selects the mode the virtual circuit uses. The options are **Active (1)** and **Passive (2)**. In **Active** mode the SPVC can both initiate and receive calls, whereas in **Passive** mode the SPVC can only receive calls.

◆ Note ◆

When in passive mode, the **svc** command does not function. For more information on this command, see Chapter 41, “Managing Cell Switching Modules (CSMs).”

101) Selector for the ATM Address

Determines a hexadecimal number to be appended to the ATM address. Since a port can have multiple SPVCs, the **Selector** allows for each SPVC to have a unique local ATM address.

11) Remote ATM Address

The ATM address of the remote end user for this SPVC. If this address is not supplied then the switch virtual circuit between this CES user and the remote CES user is not established.

12) Remote VPI

The Virtual Path Identifier (VPI) used for this circuit on the ATM switch at the other end of this soft PVC connection. The VPI specified in the **scvc** command line is the input VPI used on this OmniSwitch. The **Remote VPI** is the VPI used at the destination end of this soft PVC.

13) Remote VCI

The Virtual Channel Identifier (VCI) used for this circuit on the ATM switch at the other end of this soft PVC connection. This VCI is not the same one you specified in the **ceadd** command line. The VCI specified in the **scvc** command line is the input VCI used on this OmniSwitch. The **Remote VCI** is the VCI used at the destination end of this soft PVC.

14) SVC Retry Interval

The amount of time (in intervals of one-tenth seconds) between call attempts after an attempt has failed. If this value is set to **0**, no retry is attempted.

15) SVC Retry Limit

The maximum number of unsuccessful call attempts allowed before the attempt to establish a connection is abandoned. If this number is set to **0**, then setup attempts continue until the connection is set up successfully.

16) Restart

If an attempt of an SPVC fails for any reason (for example, it exceeds the **SVC Retry Limit**) the **Restart** option resets the statistics governing retries so that a second attempt can be made. If this value is set to **True**, when a connection fails a new attempt is made based on the information set in the SVC Retry Interval and SVC Retry Limit as if the failed attempt had not occurred. If this value is set to **False**, then the values set in the SVC Retry Interval and SVC Retry Limit are followed and there are no further attempts to make this connection.

Using the SPVC Configuration Command to Configure a CE-SPVC

You can also create an SPVC on a CSM-AB-CE T1/E1 Circuit Emulation port with the **scvc** command. However, you *must* use the first physical port when you use this command. For example, if a two-port OC-3 submodule is installed in the first slot of a CSM-U and a CSM-AB-CE submodule is installed in the middle slot of a CSM-U and this CSM-U is installed in chassis slot 4, the CSM-AB-CE ports will be numbered by software as 4/3, 4/4, 4/5, and 4/6.

To configure SPVC 0/288 on the second physical port (port 4/4) with the **scvc** command, you would enter

```
scvc 4/3 0/288
```

at the system prompt. The menu options are the same as the ones shown for the **ceadd** command in *Creating a Soft Permanent Virtual Circuit (SPVC) on T1/E1 Ports* on page 34-17.

◆ Note ◆

For more information on the **scvc** command and the ATM menu, see Chapter 42, “Advanced CSM Management.”

Creating a Virtual Channel Connection on a Serial Port

The **ceadd** command allows you to set up a circuit emulation virtual channel connection. The configuration parameters in this command are different for T1/E1 ports and serial ports. This section describes options for serial ports.

◆ Note ◆

This section applies only to the serial ports found on ASM-CE modules.

To configure a virtual channel connection on a serial port, enter the following command

```
ceadd <slot>/<port> <vci>
```

where **<slot>** is the slot number where the Circuit Emulation board is located, **<port>** is the serial port number on the Circuit Emulation board (Port 4 or Port 5), and **<vci>** is the virtual channel identifier for the virtual channel that you want to add.

When selecting a VCI, you need to be aware of the ranges available for each Circuit Emulation serial port. The following VCI ranges are available for each port:

ASM-CE Port Number	Valid VCI Range
2 (T1 or E1)	256–287
3 (T1 or E1)	288–319
4 (Serial)	320–351
5 (Serial)	352–383

◆ Important Note ◆

You can configure only one (1) connection on a serial port.

Creating a Virtual Channel Connection on a Serial Port

If you wanted to configure a virtual channel with a VCI of 320 on port 4 of the ASM-CE board in switch slot 5, you would enter

```
ceadd 5/4 320
```

A screen similar to the following is displayed:

Slot 5 Port 4 Connection 320 Configuration

Available Time Slot:
{ none }

1) Description (30 chars max)	: Connection 320
2) Administration Status { UP (1), DOWN (2) }	: UP
4) Partial Cell Fill Count (0-47)	: 0
5) Cell Loss Integration Period in second (1-64)	: 2
6) Cell Delay Variation Tolerance in frame (1-255)	: 20
7) Idle Code (0-FF)	: FF
8) Reassembly Buffer Size in frame (1-512)	: 20
10) Connection type { PVC (1), SPVC (2) }	: PVC
11) ATM uplink slot (1-5)	: 5
12) ATM uplink port (1-1)	: 1
13) ATM uplink VPI	: 2
14) ATM uplink VCI	: 2
17) Signalling Code (0-F)	: 0
18) Multicast { Enable (1), Disable (2) }	: Disable

Enter (option=value/save/cancel) :

The **ceadd** parameters for serial ports are the same as those used for T1/E1 ports. The difference between the two configurations is that the serial ports do not require time slot information. Descriptions for all of these configuration options are provided in the section, *Creating a Virtual Channel Connection on a T1/E1 Port* on page 34-12.

Configuring a Circuit Emulation T1/E1 Port

The **cemodify** command allows you to configure port-level circuit emulation parameters, such as service and clock modes. Use of this command is not required, but if you do not specify parameters, default parameters will be used to set up circuit emulation services on this port.

To configure circuit emulation parameters on a T1 or E1 port, enter the following command

```
cemodify <slot>/<port>
```

where **<slot>** is the slot number where the circuit emulation board is located, and **<port>** is the T1 or E1 port number on the board (Port 2 or Port 3) that you want to modify. For example, to modify Port 2 on the board in switch slot 5, enter

```
cemodify 5/2
```

A screen similar to the following displays (the values shown are the default values):

Circuit Emulation Port Configuration for slot 5, port 2

```

1) Description (30 chars max)                : Circuit Emulation T1 Port
2) Administration Status { UP (1), DOWN (2) } : UP
3) Service Mode { unstructured (1), structured (2) } : structured
4) Service Clock Mode { synchronous (1), srts (2),
    adaptive (3) }                             : synchronous

```

```
Enter (option=value/save/cancel) :
```

1) Description

Enter a textual description of this circuit emulation service port, up to 30 characters. This text will be used in other screen displays to identify this service port.

2) Administration Status

This option enables or disables the port. If set to **UP**, the port has been enabled and can transmit data as long as its Operational Status is also UP. If set to **DOWN**, the port will not pass data even if its physical connection is good.

3) Service Mode

The mode used to service data passing through this port. In **unstructured** mode, this circuit emulation service port passes all bits, including framing bits, through to the ATM network; an entire T1 or E1 bit stream is assigned to a single virtual circuit. The input data stream is segmented into AAL1 cells without regard to any structure in the data stream or byte alignment between the data and the ATM cell payload. In **structured** mode, time slots are assigned to each virtual channel connection. See *Circuit Emulation Services* on page 34-7 for further information on service modes.

4) Service Clock Mode

Specifies the clock mode used for this logical circuit emulation port. When using a synchronous clock, the ATM network must be running on and provide a single master clock. Synchronous clocking is the most accurate form of clocking used with circuit emulation; it is the least prone to bit errors. Synchronous clocking can be used with either structured or unstructured service modes.

Synchronous Residual Time Stamp (SRTS) clocking also requires a clock from the ATM network. However, the circuit emulation end system receives the clock provided from the device being serviced. SRTS clocking requires the use of unstructured service. Both sides of the connection must be configured to use SRTS clocking.

Adaptive clocking does not require the ATM network to run on a single master clock. The end system receives the clock provided from the device being serviced. No information on clocking is passed across the ATM network. Adaptive clocking is the least accurate form of clocking; it is the most prone to bit errors. If using adaptive clocking with structured mode, time slot information must be set correctly; you configure time slots through the **cemodify** command. Both sides of the connection must support adaptive clocking.

For more information on clock modes see *Circuit Emulation Clocking Modes* on page 34-8.

Configuring a Circuit Emulation Serial Port

The **cemodify** command allows you to configure port-level circuit emulation parameters, such as service and clock modes. Use of this command is not required, but if you do not specify parameters, default parameters will be used to set up the circuit emulation service on this port.

◆ Note ◆

This section applies only to the serial ports found on ASM-CE modules.

To configure circuit emulation parameters on a serial port, enter the following command

```
cemodify <slot>/<port>
```

where **<slot>** is the slot number where the board is located, and **<port>** is the serial port number on the board (Port 4 or Port 5) that you want to modify. For example, to modify Port 4 on the board in switch slot 4, enter

```
cemodify 4/4
```

A screen similar to the following displays:

Circuit Emulation Port Configuration for slot 4, port 4

```

1) Description (30 chars max)           : Circuit Emulation Serial Port
2) Administration Status { UP (1), DOWN (2) } : UP
3) DCE Clock Speed { 56000, 64000, 128000, 256000,
    384000, 512000, 768000, 1024000,
    1536000, 1544000, 2048000 } : 2048000
4) DCE Clock Source { internal (1), split (3) } : internal
5) Receive Clock { non-inverted (1), inverted (2) } : non-inverted
6) Transmit Clock { non-inverted (1), inverted (2) } : non-inverted
7) Service Clock Mode { synchronous (1), srts (2),
    adaptive (3) } : synchronous

```

1) Description

Enter a textual description of this circuit emulation service port, up to 30 characters. This text will be used in other screen displays to identify this service port.

2) Administration Status

This option enables or disables the port. If set to **UP**, the port has been enabled and can transmit data as long as its Operational Status is also UP. If set to **DOWN**, the port will not pass data even if its physical connection is good.

3) DCE Clock Speed

Indicates the data rate for this serial port if the port is a DCE device. Possible clock speeds for serial ports, in bps, are 56000, 64000, 128000, 256000, 384000, 512000, 768000, 1024000, 1536000, 1544000, and 2048000.

4) DCE Clock Source

Sets the type of clocking used to clock transmit and receive data in and out of the serial port. This value is only relevant if this serial port operates in DCE mode. If clocking is not controlled by this serial port (i.e., it is controlled by an external DCE device, such as a DSU), the external device will control clocking and the data rate on this port.

If you set this value to **Internal**, transmit and receive data are based on the local clock.

Split clocking uses additional control signals (TXCE) to keep the ASM-CE and external DTE device in sync. In split clocking, the DTE takes the incoming clock signals (TX clock) and loops them back out to the Circuit Emulation port. Split clocking should be used if the Circuit Emulation port is a physical DCE device and you are using a non-RS-232 cable, such as V.35.

◆ Important Note ◆

Split clocking is recommended if the access rate of the serial connection is greater than 256 Kbps. If split clocking is not used at these data rates, data out-of-phase errors, aborts, or CRC errors may occur. In cases where split clocking cannot be used because the clock is not returned, inverted clocking may be required.

5) Receive Clock

This parameter defines whether the serial port samples data on the falling or rising edge of the receive clock. If you select **non-inverted**, data is sampled on the falling edge of the receive clock. If you select **inverted**, data is sampled on the rising edge of the receive clock. Sampling data on the falling edge (non-inverted) is the appropriate option for most configurations. However, if the far-end is experiencing data errors due to a long cable, and therefore, propagation delay, you may need to invert the clock edge.

6) Transmit Clock

This parameter defines whether the serial port samples data on the falling or rising edge of the transmit clock. If you select **non-inverted**, data is sampled on the falling edge of the transmit clock. If you select **inverted**, data is sampled on the rising edge of the transmit clock. Sampling data on the falling edge (non-inverted) is the appropriate option for most configurations. However, if the far-end is experiencing data errors due to a long cable—and therefore, propagation delay—you may need to invert the clock edge.

7) Service Clock Mode

Specifies the clock mode used for this logical circuit emulation port. When using a synchronous clock, the ATM network must be running on and provide a single master clock. Synchronous clocking is the most accurate form of clocking used with circuit emulation; it is the least prone to bit errors. Synchronous clocking is supported for all serial port clock speeds.

Synchronous Residual Time Stamp (SRTS) clocking also requires a clock from the ATM network. However, the circuit emulation end system receives the clock provided from the device being serviced. SRTS clocking only operates at a clock speed of 1544000 or 2048000 bps.

Adaptive clocking is not supported on serial ports.

For more information on clock modes see *Circuit Emulation Clocking Modes* on page 34-8.

Modifying a Virtual Channel Connection

The **cemodify** command allows you to change circuit emulation virtual channel connection parameters that you previously set up through the **ceadd** command. The configuration parameters in this command are the same as those used in **ceadd**.

To modify a virtual channel connection, enter the following command

```
cemodify <slot>/<port> <vci>
```

where **<slot>** is the slot number where the circuit emulation board is located, **<port>** is the port number on the board, and **<vci>** is the virtual channel identifier for the virtual channel that you want to modify. For example, to modify a virtual channel with a VCI of 257 on Port 2 of the board in switch slot 5, enter

```
cemodify 5/2 257
```

A screen similar to the following displays:

```

Slot 5 Port 2 Connection 257 Configuration
Available Time Slot:
  { none }

1) Description (30 chars max)           : Connection 257
2) Administration Status { UP (1), DOWN (2) } : UP
3) Virtual Path Identifier (0-128)       : 0
4) Partial Cell Fill Count (0-47)       : 0
5) Cell Loss Integration Period in second (1-64) : 2
6) Cell Delay Variation Tolerance in frame (1-255) : 20
7) Idle Code (0-FF)                     : FF
8) Reassembly Buffer Size in frame (1-384) : 384
9) Time slots used : {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,
                    13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24}
   (Usage: "+/-<ts|all>" add/remove a time slot. For example,
   "9=+10+12-9" to add time slot 10 & 12 and remove time slot 9.
   "9=+all" add all time slots. "9=-all" remove all time slots)
10) ATM uplink slot (1-5)                : 5
11) ATM uplink port (1-1)                : 1
12) ATM Uplink VPI/VCI                   : 2
13) ATM Uplink VCI                       : 2
17) Signalling Code (0-F)                : 0
18) Multicast { Enable (1), Disable (2) } : Disable

Enter (option=value/save/cancel) :
```

The **cemodify** parameters for virtual channel connections are the same as those used in the **ceadd** command. For definitions of these parameters, please refer to *Creating a Virtual Channel Connection on a T1/E1 Port* on page 34-12 for T1 and E1 ports, and *Creating a Virtual Channel Connection on a Serial Port* on page 34-21 for serial ports.

◆ Note ◆

You can also modify SPVC connection parameters with the **mvc** command, which is described in Chapter 41, “Managing Cell Switching Modules (CSMs).”

Deleting a Virtual Circuit

You can delete a circuit emulation virtual circuit as long as you know its VCI and the port where it exists. To delete a virtual circuit, enter the following command

```
cedele <slot>/<port> {<VCI> | all}
```

where **<slot>** is the slot number for the board, **<port>** is the port where the virtual circuit is located, **<VCI>** is the identification number for the virtual circuit, and **all** specifies all connections. For example, to delete virtual circuit 300 on Port 4 of the board in slot 5, enter:

```
cedele 5/4 300
```

The system returns the following prompt to confirm the deletion:

```
This will delete Slot 5, Port 4, VCI 300. Continue? {(Y)es, (N)o} (N)
```

Enter a **Y** to confirm the deletion or press **<Enter>** to cancel the deletion.

◆ Note ◆

You can also delete SPVC connections with the **dvc** command, which is described in Chapter 41, “Managing Cell Switching Modules (CSMs).”

Viewing Circuit Emulation Information

The **cestatus** command provides circuit emulation information, including configuration parameters, time slot information, status, and statistics. You can obtain circuit emulation information on all circuit emulation boards in the switch, a single board, individual ports, and individual virtual circuits. You receive different displays depending upon which level you choose. The sections below describe all ways to use the **cestatus** command.

Viewing Information on All Circuit Emulation Boards in a Switch

To obtain circuit emulation service information on all circuit emulation boards in a switch, enter the **cestatus** command without any parameters as follows:

```
cestatus
```

This command displays a screen similar to the following:

Circuit Emulation Chassis Status

Slot/Port	Port Description	Admin/ Oper Status	Interface Type	Clock Speed	Setup VCCs
4/2	Circuit Emulation E1 Port	UP/UP	E1	2048000	2
4/3	Circuit Emulation E1 Port	UP/UP	E1	2048000	1
4/4	Circuit Emulation Serial Port	UP/DN	*NONE*	0	1
4/5	Circuit Emulation Serial Port	UP/DN	*NONE*	0	1
5/2	Circuit Emulation T1 Port	UP/UP	T1	1544000	1
5/3	Circuit Emulation T1 Port	UP/UP	T1	1544000	1
5/4	Circuit Emulation Serial Port	UP/UP	V35DCE	1544608	1
5/5	Circuit Emulation Serial Port	UP/UP	V35DTE	1544608	1

Each row in the table corresponds to a physical port on an board in the switch. The following sections describe the columns shown in this table:

Slot/Port. The first number in this column is the slot in the switch where this module is installed. The second number is the port number on the module.

Port Description. The textual description of this port as entered through the **cemodify** command.

Admin/Oper Status. This column shows the Administrative and Operational Status of this port. The status indicator before the slash refers to the Administrative Status. If **UP**, the port has been enabled and can transmit data as long as its Operational Status is also **UP**. If the Administrative Status is **DN**, the port will not pass data even if its physical connection is good.

The status indicator after the slash refers to the Operational Status. If **UP**, the port is capable of passing data as long as it has been logically enabled at the Administrative level. If **DN**, the port cannot pass data because of a problem in the physical connection (e.g., cable disconnected, hardware could not detect cable type) or because the port is Administratively Down.

Interface Type. This column indicates the physical cable type connected to this port. This cable type is automatically sensed by hardware.

For serial ports, this column indicates the cable type and whether it is DCE or DTE. The following values may display in this column

- **V35DTE** (V.35 DTE cable)
- **V35DCE** (V.35 DCE cable)
- **232DTE** (RS-232 DTE cable)
- **232DCE** (RS-232 DCE cable)
- **X21DTE** (X.21 DTE cable)
- **X21DCE** (X.21 DCE cable)
- **530DTE** (RS-530 or RS-449 EIA DTE cable)
- **530DCE** (RS-530 or RS-449 EIA DCE cable)
- **T1** (T1 CES port)
- **E1** (E1 CES port)

The ASM-CE sees RS-530 and RS-449 cables the same because they are electrically identical. However, this does not affect the operation of either cable type. Both RS-530 and RS-449 cables are supported.

If no serial port cable is connected to a port, this column will display

NONE

T1 and E1 ports will display their interface type whether or not a cable is attached. If an error has been detected on the port (e.g., cable type could not be detected), the following value displays:

ERROR!

Clock Speed. Indicates the data rate of the interface. T1 and E1 ports (ports 2 and 3) will always be set to 1544000 or 2048000, respectively. The clock speed of serial ports (ports 4 and 5) is dynamically derived from the cell rate. Possible clock speeds for serial ports, in bps, are 56000, 64000, 128000, 256000, 384000, 512000, 768000, 1024000, 1536000, 1544000, and 2048000.

Setup VCCs. The number of virtual channel connections (VCCs) that have been set up for the corresponding port in the table. Virtual channel connections are configured through the **ceadd** command, which is described in *Creating a Virtual Channel Connection on a T1/E1 Port* on page 34-12.

Viewing Information on One Module

To obtain circuit emulation service information on an board in the switch, enter the following command

```
cestatus <slot>
```

where <slot> is the slot number where the board is located. For example, to display information on the board in switch slot 4, enter

```
cestatus 4
```

This command displays a screen similar to the following:

Circuit Emulation Status for slot 4

Port	Port Description	Admin/ Oper Status	Interface Type	Clock Speed	Setup VCCs
2	Circuit Emulation E1 Port	UP/UP	E1	2048000	2
3	Circuit Emulation E1 Port	UP/UP	E1	2048000	1
4	Circuit Emulation Serial Port	UP/DN	*NONE*	0	1
5	Circuit Emulation Serial Port	UP/DN	*NONE*	0	1

Descriptions of the columns in this table are given under the description of the **cestatus** command for all boards in a switch. Please refer to *Viewing Information on All Circuit Emulation Boards in a Switch* on page 34-29.

Viewing Information for a T1 or E1 Port

To obtain circuit emulation service information on one T1 or E1 port, enter the following command

```
cestatus <slot>/<port>
```

where **<slot>** is the slot number where the board is located and **<port>** is the port number on the board for which you want to view information. For example, to view information on Port 2 of the board in switch slot 4, enter

```
cestatus 4/2
```

This command displays a screen similar to the following:

Circuit Emulation Status for slot 4, port 2

```
Description           : Circuit Emulation E1 Port
Admin/Oper Status     : UP/UP
Service Mode          : structured
Service Clock Mode    : synchronous
Available Time Slots  : { none }
```

Virtual Circuit Information

VPI/VCI	Channel Description	Admin/Oper Status	No. of Time Slots
0/256	Connection 256	UP/UP	4
0/257	Connection 257	UP/UP	27

Description. A textual description for this port entered when the port was configured through the **cemodify** command.

Admin/Oper Status. This field is described in *Viewing Information on All Circuit Emulation Boards in a Switch* on page 34-29.

Service Mode, Service Clock Mode. Descriptions of these two fields are given in the section, *Configuring a Circuit Emulation T1/E1 Port* on page 34-23.

Available Time Slots. The time slots that are available for virtual circuits on this port. Time slots are assigned to virtual circuits through the **ceadd** command, which is described in *Creating a Virtual Channel Connection on a T1/E1 Port* on page 34-12.

The following table columns also display for each virtual circuit on this port.

VPI/VCI. The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) for virtual channels on which information is provided. You configure the VPI and VCI for virtual channel connections through the **ceadd** command, which is described in *Creating a Virtual Channel Connection on a T1/E1 Port* on page 34-12.

Channel Description. A textual description of this virtual channel of up to 30 characters. This channel description is configured through the **ceadd** command.

Admin/Oper Status. This field is described in *Creating a Virtual Channel Connection on a T1/E1 Port* on page 34-12.

No. of Time Slots. The number of time slots for the given virtual circuit. You assign time slots to each virtual circuit through the **ceadd** command. Only circuit emulation services using a structured service mode require the use of time slots.

Viewing Information for a Serial Port

To obtain circuit emulation service information on one Circuit Emulation serial port, enter the following command

```
cestatus <slot>/<port>
```

where <slot> is the slot number where the ASM-CE board is located and <port> is the port number on the ASM-CE board for which you want information. For example, to view information on Port 4 for the ASM-CE board in switch slot 4, enter

```
cestatus 4/4
```

This command displays a screen similar to the following:

```

Circuit Emulation Status for slot 4, port 4

Description           : Circuit Emulation Serial Port
Admin/Oper Status     : UP/DOWN
Service Mode          : unstructured
Service Clock Mode    : synchronous
Clock Speed           : 0
Interface Type        : *NONE*      DCE Clock Source      : internal
Transmit Clock        : non-inverted  Receive Clock         : non-inverted

Virtual Circuit Information

VPI/VCI      Channel Description      Admin/Oper  No. of
=====      =====
0/320        Connection 320                UP/UP      N/A

```

Descriptions for the fields in the top section of this display can be found in *Configuring a Circuit Emulation Serial Port* on page 34-25.

Descriptions for the fields in the bottom section of the display can be found in *Viewing Information for a T1 or E1 Port* on page 34-32.

Viewing Information for a T1/E1 Virtual Circuit

To obtain circuit emulation service information on a virtual circuit (either a PVC or an SPVC) configured on a T1 or E1 port, enter the following command

```
cestatus <slot>/<port> <VCI>
```

where **<slot>** is the slot number where the board is located, **<port>** is the port number on the board, and **<VCI>** is the virtual channel identifier for the virtual channel for which you want to view information. For example, to view information on a virtual channel with a VCI of 257 on Port 2 of the board in switch slot 5, enter

```
cestatus 5/2 257
```

This command displays a screen similar to the following:

```

Circuit Emulation Status for slot 5, port 2, vci = 289

Description           : Connection 289
SVC MODE              : Active
VPI/VCI               : 0/289
ATM Uplink slot/port  : 5/1
Time Slot Used        : {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,
                       13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24}
Admin/Oper Status    : UP/UP
Idle Code             : FF
Elapsed Time          : 0 days, 00:36:18.68
Receive Buffer Size    : 384
CDVT                  : 20

                        Total      Rate
Transmit Data Cells   : 4280757    4097
Transmit Conditioned Cells : 65543      0
Transmit Cells Suppressed : 0          0
Receive Data Cells    : 4310044    4097
Receive Bad Sequence Number Cells : 0          0
Receive Cells Dropped Pointer Search : 183        0
Receive Cells Dropped Queue Underrun : 183        0
Receive Cells Dropped Queue Overrun : 0          0
    
```

Descriptions for fields in the top portion of this screen display (except for **SVC MODE** and **Elapsed Time**) are described in the section, *Configuring a Circuit Emulation Serial Port* on page 34-25.

Descriptions for fields in the bottom half of the display are provided below. Values in the **Total** column indicate the total number of cells transmitted or received on this virtual channel connection. Values in the **Rate** column indicate the number of cells transmitted or received in the last second.

SVC Mode. This field displays the mode the virtual circuit uses, which can be **Active** or **Passive**. In **Active** mode, the SPVC can both initiate and receive calls, whereas in **Passive** mode the SPVC can only receive calls.

Elapsed Time. This field identifies the length of time since the last time the virtual circuit statistics were cleared via the **cecls** command (see *Clearing ATM Circuit Emulation Statistics* on page 34-37 for more information). Elapsed Time is displayed in the format “xxx days, hh:dd:ss.tt.”

Transmit Data Cells. The number of cells on this virtual circuit containing user data that has been transmitted upstream.

Transmit Conditioned Cells. The number of cells transmitted upstream on this virtual circuit when there are one or more active alarms on the port where this virtual circuit is configured.

Transmit Cells Suppressed. The number of cells that were dropped on this virtual circuit due to line resynchronization.

Receive Data Cells. The total number of data cells received on this virtual circuit.

Receive Bad Sequence Number Cells. The number of times that cells received had a bad sequence number in the AAL1 SAR header. This value indicates the number of times hardware *detected* bad sequence numbers, but the actual number of cells lost may be higher.

Receive Cells Dropped Pointer Search. The number of times the ATM-CE module dropped incoming cells during the pointer searching process. This value indicates the number of times hardware *detected* dropped cells due to this condition, but the actual number of cells lost may be higher.

Receive Cells Dropped Queue Underrun. The number of times the ATM-CE module dropped incoming cells because the reassembly buffer underran. This value indicates the number of times hardware *detected* dropped cells due to this condition, but the actual number of cells lost may be higher.

Receive Cells Dropped Queue Overrun. The number of times the ATM-CE module dropped incoming cells because the reassembly buffer overran. This value indicates the number of times hardware *detected* dropped cells due to this condition, but the actual number of cells lost may be higher.

Viewing Information for a Serial Port Virtual Circuit

To obtain circuit emulation service information on a virtual circuit configured on a serial port, enter the following command

```
cestatus <slot>/<port> <VCI>
```

where **<slot>** is the slot number where the circuit emulation board is located, **<port>** is the port number on the board, and **<VCI>** is the virtual channel identifier for the virtual channel for which you want to view information. For example, to view information on a virtual channel with a VCI of 320 on port 4 on the circuit emulation board in switch slot 5, enter

```
cestatus 5/3 320
```

This command displays a screen similar to the following:

Circuit Emulation Status for slot 5, port 3, vci = 320

Description	: Connection 320		
VPI/VCI	: 0/320		
ATM Uplink slot/port	: 4/1		
Admin/Oper Status	: UP/UP		
Idle Code	: FF		
Receive Buffer Size	: 100	CDVT	: 20
		Total	Rate
Transmit Data Cells	: 438420442		5448
Transmit Conditioned Cells	: 0		0
Transmit Cells Suppressed	: 0		0
Receive Data Cells	: 438420442		5448
Receive Bad Sequence Number Cells	: 0		0
Receive Cells Dropped Pointer Search	: 0		0
Receive Cells Dropped Queue Underrun	: 1		0
Receive Cells Dropped Queue Overrun	: 0		0

Descriptions for fields in the top portion of this screen display are described in the section, *Configuring a Circuit Emulation Serial Port* on page 34-25. Descriptions for fields in the bottom half of the display are described above in the section, *Viewing Information for a T1/E1 Virtual Circuit* on page 34-34.

Clearing ATM Circuit Emulation Statistics

To clear the accumulated statistics for an ATM CE circuit, use the **cecls** command, as follows:

```
cecls <slot>/<port> {<VCI> | all}
```

where **<slot>** is the slot number where the circuit emulation board is located, **<port>** is the port number on the board, **all** specifies all VCIs, and **<VCI>** is the virtual channel identifier for the virtual channel whose statistics you want to clear. For example, to clear the statistics on a virtual channel with a VCI of 256 on port 5 on the circuit emulation board in switch slot 1, enter

```
cecls 5/1 256
```

Once the statistics have been cleared, the following message will be displayed:

```
Statistics of Virtual Circuit 256 on 5/1 have been cleared.
```


35 LANE Server Configuration

Introduction

The integration of LES/BUS and LECS services into the OmniSwitch architecture provides a complete, “on-board” solution for supporting ATM LAN Emulation (LANE). The software that supports these services inserts several commands into the switch’s User Interface (UI) to provide you with a means of configuring LES/BUS and LECS services and monitoring their operational status and configuration parameters.

To be able to configure LES/BUS and LECS services properly, you will need to have at least some basic knowledge of the design and operation of ATM LANE itself. The information which follows below provides an overview of LAN Emulation and its component services, including LES/BUS and LECS. Chapter 36, “Configuring ATM Services,” provides more information on configuring your switch to perform ATM LAN Emulation.

LAN Emulation Components

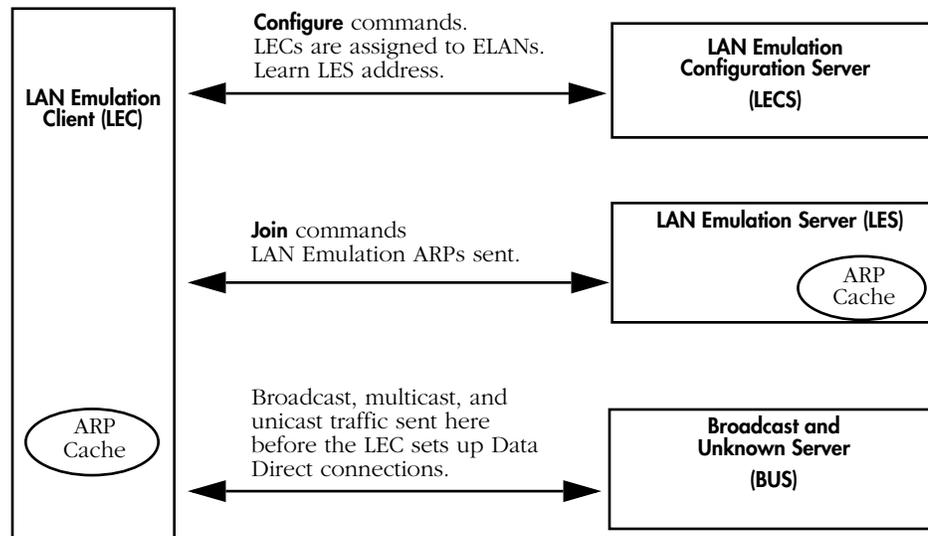
ATM LAN Emulation is made up of a group of both physical and “logical” ATM devices which collectively are called an ELAN (Emulated LAN). The counterpart to an ELAN in the traditional LAN world is a group of workstations attached to a LAN segment (either Ethernet or Token-Ring). But, because an ELAN is a *logical* grouping of devices, it does not limit membership to only those devices that are attached to the same physical network segment. However, a single ELAN “entity” can be comprised of only one media type: either Ethernet (IEEE 802.3) or Token-Ring (IEEE 802.5). In other words, if you need to support more than one media type in LANE, you will need to configure multiple ELANs (one for each type).

The software running in your OmniSwitch provides your ATM networks with the logical devices required by LANE to support interoperability between ATM and Ethernet and/or Token-Ring LANs. There are four logical ATM devices created “within” the switch which comprise an ELAN:

- The LAN Emulation Client (LEC): an entity which performs data forwarding, address resolution, and other control functions for a single broadcast domain (that is, a single ELAN). The software in your switch which supports the ATM access module provides LEC services.
- LAN Emulation Server (LES): an entity which implements the control functions for an single ELAN. There is only one LES per ELAN. When we say that a LEC “belongs to” a particular ELAN, we means that it has a control relationship with that ELAN’s LES. Additional software in your switch provides LES services as well as the following two services.
- Broadcast and Unknown Server (BUS): an entity which floods unknown destination address traffic as well as forwarding multicast and broadcast traffic to the LECs that belong to an individual ELAN. There is only one BUS per ELAN. And, because the LES and the BUS within an ELAN must operate together, they are typically called a “LES/BUS pair.” Within the switch’s UI, the term “ELAN” is often used to refer to a single LES/BUS pair.
- LAN Emulation Configuration Server (LECS): an entity which assigns individual LECs to a particular ELAN by “directing” them to the LES that corresponds to that ELAN. There is only one LECS within a broadcast domain which serves all the ELANs within that domain. By using the switch’s UI commands, you can set policies for the LECS to use to control which LECs (and consequently which Groups and VLANs) are allowed to join a specified ELAN.

LANE Component Interactions

The figure below shows the four logical ATM entities that comprise LANE (LEC, LES, BUS, and LECS) and the different types of communications that take place between them.



The LAN Emulation Client/Services Model

Initializing the ELAN. The LEC starts the ELAN initialization process by sending a Configure request to the LAN Emulation Configuration Server (LECS). The LECS verifies the configuration settings for the LEC, assigns it to an ELAN, and informs it of the LES's address.

After configuration, the LEC sends a Join request to the LES so that it can participate in address resolution and the creation of virtual circuit connections (VCCs). The LES assigns the LEC an identification number, and, in some configurations, begins to register the MAC addresses in the broadcast domain of the LEC. The OmniSwitch's LEC, however, acts as a "proxy" and only provides registration information when specifically requested by the LES.

Next, the LEC sets up a connection with the BUS by sending ARPs to the broadcast MAC address. The BUS can handle all broadcast, unicast, and multicast traffic from the LEC. While the LES tries to resolve the MAC-to-ATM address request from the LEC, the BUS will try to reach the same ATM destination by forwarding LEC broadcasts to the ATM address.

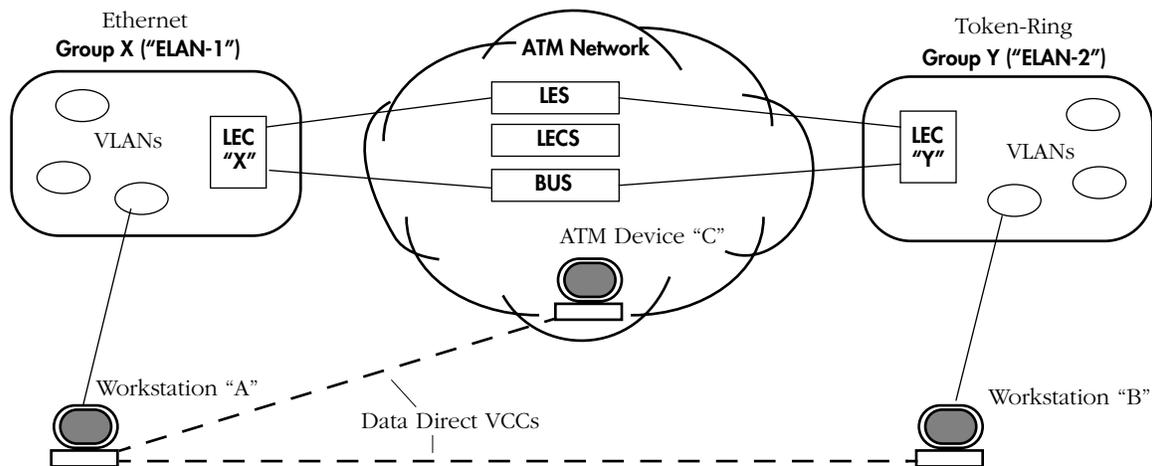
The LAN Emulation ARP Cache. The LAN Emulation ARP cache is a table of entries that maps MAC-to-ATM addresses for unicast and broadcast addresses (but not multicast addresses). Each table entry establishes a relationship between a LAN destination and the ATM address where data frames for that LAN destination are to be sent. The ARP cache binds a MAC address to an ATM address. The LEC contains an ARP cache for those addresses that are in its broadcast domain, while the LES contains a master ARP cache.

◆ Note ◆

Auto-activated LAN Emulation Clients (LECs) will not re-initialize after hot swapping an OmniSwitch ASM or ASM2 module or after hot swapping an Omni Switch/Router ASX module. Reboot the switch to re-initialize the auto-activated LECs.

LAN-to-ATM Communication

After a LEC has established a connection to a LES/BUS pair, it can begin responding to LES's requests for MAC addresses from the ATM side and to Ethernet's requests for ATM address destinations from the LAN side. The following diagram shows a simple LAN Emulation setup.



Traditional LANs and an ATM Network Connected Through LAN Emulation

The LES, BUS, and LECS all "reside" in a single OmniSwitch that contains at least one ATM access module which is connected to an ATM network. After you have configured the LANE services, including "creating" the two ELANs as shown in the above diagram, interaction between the devices on the ATM network and those on the Ethernet and Token-Ring networks can begin. Here is an example of a LAN-to-ATM communication interaction:

Whenever Workstation "A" wants to communicate with either ATM device "C" or Workstation "B" on another ELAN it must use the LANE services because it cannot directly communicate with either of these devices. The LEC in Workstation A's Group "X" picks up A's request to connect with ATM device. This LEC does not "know" the whereabouts of the ATM device, so it sends out an ARP to the LES. In the meantime, it may also send one or more unicast packets to the BUS to locate the ATM device, thereby setting up a virtual circuit with the BUS which allows the BUS to forward packets to the ATM device.

When the LES does locate the ATM device, LEC X can then set up a "Data Direct" VCC between Workstation A and the ATM device C. However, it must first stop sending unicast packets to the BUS. Otherwise, the ATM device would receive data from both the BUS and the Data Direct VCC at the same time, resulting in frame-out-of-order errors. Therefore, the LEC first flushes the connection to the BUS, then sets up a Data Direct VCC with the ATM device. Once the Data Direct VCC has been established, data may begin passing directly between the devices on the traditional LAN and the ATM network.

Overview of LES/BUS and LECS Configuration

You will need to perform the following steps, using parameters that are relevant to your ATM network, to enable the operation of LES/BUS and LECS services on your OmniSwitch:

1. Create at least one LES/BUS pair (synonymous with creating a single ELAN). See *Creating a LES/BUS Pair* on page 35-8 for information on this procedure.
2. Creating the LECS (LAN Emulation Configuration Server) entity and its database. See *Creating the LECS* on page 35-13 for information on this procedure.
3. Adding at least one LES/BUS pair (or ELAN) to the LECS database. See *Adding ELANs to the LECS* on page 35-17 for information on this procedure.
4. Adding “policy values” to the LES/BUS pairs (ELANs) added to the LECS database to control which LAN Emulation Clients (LECs) are allowed to join the ELAN(s). See *Adding Policies to ELANs in the LECS* on page 35-20 for information on this procedure.

The LANE Service Menu (LSM)

The software which provides LES/BUS and LECS services inserts a submenu under the Interface menu. This submenu is abbreviated LSM for “LANE Service Menu.” The first command (**ismcfg**) in the LSM menu is used to access a submenu where you can configure the LES/BUS and LECS services. The other commands in the LSM menu are used to display screens showing the LES/BUS and LECS operational status, statistics, and configuration.

To switch to the **LSM** submenu, enter the following command:

ism

A screen similar to the following displays (if you have enabled verbose mode):

Command	LANE Service Menu
autolesbus	Automatic Configuration of LES/BUS, LECS and/or LECS database
ismcfg	Configuration of LES/BUS, LECS and/or LECS database
lslb	List all LES-BUS pairs configured on this port
vlb	Show status of a LES/BUS pair
vlbs	Show statistics of a LES/BUS pair
vlbc	Show configuration of a LES/BUS pair
vlec	List all LE clients per LES/BUS pair
vmac	List registered MAC address of a given LES/BUS pair
vrld	List registered route descriptor of a given LES/BUS pair
vlecd	List detail LE client information by LEC id
vlecs	Show status of a LECS
vlecss	Show statistics of a LECS
vlecsc	Show configuration of a LECS
velan	List elan(s) configured in the LECS database
vpolicy	List policy value assigned to an elan in the LECS database

Main File Summary VLAN Networking
Interface Security System Services Help

All of the commands in the LSM menu, as well as all of the commands in all of its submenus, require the specification in the command line of both the switch slot that contains the ATM access or FCSM board and the ATM port to which the command is to be applied.

In other words, the command line syntax is: **command <slot>/<port>**.

Configuring LES/BUS and LECS

The **autolesbus** command on the LANE Service Menu is used to quickly set up your switch to support one ELAN (named “default”) and to initialize LECS services.

To run this automated procedure, enter the following command (in this example command line, the ATM access board is in switch slot 2, and the port being addressed is port 1):

```
autolesbus 2/1
```

A screen similar to the following displays:

```
One LECS is already configured on this physical interface.
Creating LES/BUS pair for elan 'default' on slot 2, port 1, please wait...
LES/BUS pair for elan 'default' on slot 2, port 1 created
Creating default ELAN 'default' for LES/BUS pair on slot 2, port 1, please wait...
default elan default added to the LECS database
default policy (ELAN_NAME) added to LECS database for elan 'default'
```

You can use the **ismcfg** command on the LANE Service Menu to modify the “default” LES/BUS pair. Entering the **ismcfg** command displays a submenu which contains all the commands used to configure LES/BUS and LECS services.

To display the LES/BUS and LECS configuration submenu, enter the following command (in this example, the ATM access board is in switch slot 2, and the port being addressed is port 1):

```
ismcfg 2/1
```

A screen similar to the following displays:

```
1) Global elan name (currently none specified)
2) Create LES/BUS
3) Modify LES/BUS
4) Delete LES/BUS
5) Create LECS
6) Modify LECS
7) Delete LECS
8) Add elan to LECS database
9) Delete elan from LECS database
10) Add policy to elan in LECS database
11) Delete policy from elan in LECS database
12) Exit configuration menu
```

Enter option :

The **ismcfg** submenu contains individual options for:

- Specifying a “global” ELAN name (to be used with the other commands to save time);
- Creating, modifying, and deleting LES/BUS pairs (which are related to individual ELANs);
- Creating, modifying and deleting a LECS database;
- Adding and deleting a LES/BUS pair (i.e., an ELAN) to and from the LECS database;
- Adding and deleting policy values to the LES/BUS pairs (i.e., ELANS) in the LECS database.
- Exiting the submenu and returning to the LSM menu.

Each of these options is described in the subsections that follow immediately below.

Making SubMenu Option Selections

To make changes to the individual options at the **lsmcfg** submenu simply enter the option's index number. The program will respond with a prompt indicating any more information needed by the option. For example, the first option ("Global elan name") will respond with a prompt asking for the name of the ELAN.

Important Note

Before you can configure LES/BUS and LECS services, you must first change the ATM access port's type from "PVC" to "SVC" (Switched Virtual Port) using the **map** command. See Chapter 33, "Managing ATM Access Modules," for a complete description of the procedure.

If you have not yet made this change, do so *now before* continuing with the instructions below.

Specifying a Global ELAN Name

Option 1 on the **lsmcfg** submenu (“Global elan name”) is used to specify the ELAN to which you want the other options to be applied. This “shortcut” will save you the trouble of having to specify the name of the desired ELAN when you access the other options (to modify or delete configurations). In other words, if you decide not to set a “global ELAN name,” you will have to specify the ELAN with which you want to work by entering its name whenever you access the other options on the **lsmcfg** submenu. You must have *already* created an ELAN (i.e., a LES/BUS pair) to be able to use this option.

Here is what the screen looks like before you enter any command:

- 1) **Global elan name (currently none specified)**
- 2) **Create LES/BUS**
- 3) **Modify LES/BUS**
- 4) **Delete LES/BUS**
- 5) **Create LECS**
- 6) **Modify LECS**
- 7) **Delete LECS**
- 8) **Add elan to LECS database**
- 9) **Delete elan from LECS database**
- 10) **Add policy to elan in LECS database**
- 11) **Delete policy from elan in LECS database**
- 12) **Exit configuration menu**

Enter option :

1. To specify that you want to work with “elan1”, enter the following command:

1

A screen similar to the following displays:

Enter (elan name) :

2. Enter the name of the ELAN with which you wish to work. For example, you could enter:

elan1

A screen similar to the following displays:

- 1) **Global elan name** **elan1**
- 2) **Create LES/BUS**
- 3) **Modify LES/BUS**
- 4) **Delete LES/BUS**
- 5) **Create LECS**
- 6) **Modify LECS**
- 7) **Delete LECS**
- 8) **Add elan to LECS database**
- 9) **Delete elan from LECS database**
- 10) **Add policy to elan in LECS database**
- 11) **Delete policy from elan in LECS database**
- 12) **Exit configuration menu**

Enter option :

The screen has changed to indicate that the LES/BUS pair named “elan1” will be used as the default when the other commands on this submenu are used.

Creating a LES/BUS Pair

Option 2 on the **lsmcfg** submenu (“Create LES/BUS”) is used to create a LES/BUS “pair.” These two entities work together to provide services for a single ELAN (emulated LAN). The hosts and other devices which make up a single ELAN can be connected by only one media type, either Ethernet (IEEE 802.3) or Token Ring (IEEE 802.5). Therefore, you’ll need to create a separate ELAN for each media type.

Note

If the chosen LES/BUS is more than one hop away, you *must* change the CSM port from UNI to PNNI with the **map** command. See Chapter 41, “Managing Cell Switching Modules (CSMs),” for more information on the **map** command for CSMs.

Here is what the screen looks like before you enter any command:

- 1) Global elan name elan1
- 2) Create LES/BUS
- 3) Modify LES/BUS
- 4) Delete LES/BUS
- 5) Create LECS
- 6) Modify LECS
- 7) Delete LECS
- 8) Add elan to LECS database
- 9) Delete elan from LECS database
- 10) Add policy to elan in LECS database
- 11) Delete policy from elan in LECS database
- 12) Exit configuration menu

Enter option :

1. To begin to create a LES/BUS pair, enter the following command:

2

A screen similar to the following displays:

Enter (elan name) :

2. To create an ELAN named “elan1”, you would enter the following command:

elan1

A screen similar to the following displays:

LES/BUS for Slot 2 Port 1

- 1) ELAN name (32 chars max) : elan1
- 2) ELAN type { 802.3 (1), 802.5 (2) } : 802.3
- 3) Max Data Frame Size { 1516 (1), 4544 (2),
9234 (3), 86
- 4) Control time-out { 10 - 300 seconds } : 120
- 5) Max. Frame age { 1 - 4 seconds } : 1
- 6) Enable redundancy { No (1), Yes (2) } : NO
- 7) Admin Status { Disable (1), Enable (2) } : Enable
- 8) LES/BUS Security { Disable (1), Enable (2) } : Disable

Enter (option=value/save/cancel) :

The fields on this screen have the following meanings:

ELAN {32 characters max}

The name of the ELAN the LES/BUS is administering.

ELAN type {802.3 (1), 802.5 (2) }

The assigned type of ELAN. Ethernet ELANs are 802.3 while Token Ring ELANs are 802.5.

Max Data Frame Size {1516 (1), 4544 (2), 9234 (3), 18190 (4)}

The maximum size, in octets, for the data frames sent to/from this ELAN. The default for Ethernet is 1516; for Token Ring, 4544. Token Ring ELANs can also support sizes of 9234 and 18190. To avoid packet loss, you should select a setting for the LECS which matches, or is a higher rate than, the maximum size used by the LE Clients on the ELAN.

Control time-out {10-300 seconds}

The period, in seconds, used to time out most request/response control frames.

Max Frame age {1-4 seconds}

The number of seconds allowed for the BUS to transmit the frame. If the age is exceeded, the BUS will discard the frame.

Enable redundancy {No (1), Yes (2)}

Used to turn redundancy on or off (the default is off). If you decide to use redundancy, you will be asked to specify whether this ELAN is to take a “primary” or “secondary” role. If you set it to “secondary”, make sure that you add this secondary LES ATM address to the primary LES when you configure the primary LES.

Admin Status {Enable (1), Disable (2)}

Used to turn this ELAN on or off in regards to the LES.

LES/BUS Security {Enable (1), Disable (2)}

Used to turn the security option for this ELAN on or off (the default is off). When on, security will prevent LAN Emulation Clients (LECs) from directly accessing the LES/BUS and its ELAN without having to pass the policy review of the LECS (LAN Emulation Configuration Server).

3. The defaults settings for each of the fields on this screen are appropriate for an Ethernet ELAN. If you need to change any of them, do so now. Simply enter the desired option number first, followed by an “equals” (=) sign, then the desired value.
4. When you are finished setting the parameters for each option, you must save the changes you have made. To save changes, enter the following command:

save

But, if you wish to abort and discard changes, simply enter the **cancel** command.

After entering the **save** command, a message similar to the following displays, then the previous configuration menu reappears:

Creating LES/BUS pair for elan 'elan1' on slot 2, port 1, please wait...

LES/BUS pair for elan 'elan1' created on slot 2, port 1

Modifying a LES/BUS Pair

Option 3 on the **lsmcfg** submenu (“Modify LES/BUS”) is used to modify the configuration of an existing LES/BUS “pair” (emulated LAN or ELAN).

Here is what the menu looks like before you enter any command:

- ```

1) Global elan name elan1
2) Create LES/BUS
3) Modify LES/BUS
4) Delete LES/BUS
5) Create LECS
6) Modify LECS
7) Delete LECS
8) Add elan to LECS database
9) Delete elan from LECS database
10) Add policy to elan in LECS database
11) Delete policy from elan in LECS database
12) Exit configuration menu

```

Enter option :

1. First, you must specify that you want to modify an ELAN. If you did not use Option 1 to set a “global” ELAN name, you would enter the following command:

```
3
```

A screen similar to the following displays:

Enter (elan name) :

2. To proceed to modify the configuration of “elan1”, enter the following command:

```
elan1
```

A screen similar to the following displays:

LES/BUS for Slot 2 Port 1

- ```

1) ELAN name (32 chars max)          : elan1
2) ELAN type { 802.3 (1), 802.5 (2) } : 802.3
3) Max Data Frame Size { 1516 (1), 4544 (2),
   9234 (3), 86
4) Control time-out { 10 - 300 seconds } : 120
5) Max. Frame age { 1 - 4 seconds }      : 1
6) Enable redundancy { No (1), Yes (2) } : NO
7) Admin Status { Disable (1), Enable (2) } : Enable
8) LES/BUS Security { Disable (1), Enable (2) } : Disable

```

Enter (option=value/save/cancel) :

This screen shows the parameters that were originally entered for this ELAN. The meaning of the options at this screen is given earlier under the heading “*Creating a LES/BUS Pair* on page 35-8.

3. If you want to make changes to any of these parameters, enter the desired option number first, followed by an “equals” (=) sign, then the desired value.
4. When you are finished changing the parameters for each option, you must save the changes you have made. To save changes, enter the following command:

```
save
```

But, if you wish to abort and discard changes, simply enter the **cancel** command.

Deleting a LES/BUS Pair

Option 4 on the **lsmcfg** submenu (“Delete LES/BUS”) is used to delete the configuration of an existing LES/BUS “pair” (emulated LAN or ELAN).

Here is what the menu looks like before you enter any command:

- 1) Global elan name elan1
- 2) Create LES/BUS
- 3) Modify LES/BUS
- 4) Delete LES/BUS
- 5) Create LECS
- 6) Modify LECS
- 7) Delete LECS
- 8) Add elan to LECS database
- 9) Delete elan from LECS database
- 10) Add policy to elan in LECS database
- 11) Delete policy from elan in LECS database
- 12) Exit configuration menu

Enter option :

1. First, you must specify that you want to delete an ELAN. If you did not use Option 1 to set a “global” ELAN name, you would enter the following command:

4

A screen similar to the following displays:

Enter (elan name) :

2. To proceed to delete “elan1”, enter the following command:

elan1

A screen similar to the following displays:

ELAN typ st	ELAN Name	LES ATM Addr
Eth UP	elan1	0000000000000000000000000020da8055fdd2

Delete this LES/BUS pair ([N]/Y):

3. To answer “yes”, enter the following command (the default response is **N** for “no”):

Y

A message will appear informing you of the deletion.

Creating the LECS

Option 5 on the **lsmcfg** submenu (“Create LECS”) is used to create a LECS (LAN Emulation Configuration Server). A LECS assigns individual LAN Emulation Clients (LECs) to a particular ELAN by directing them to the LES that corresponds to the ELAN. The LECS maintains a database of ELANs, which are related to the LES/BUS pairs you create. When you create the LECS, you also create its database. There are no other steps required to create this database. However, you must manually add the ELANs you have created to the LECS database. This procedure is described below

Here is what the menu looks like before you enter any command:

- ```

1) Global elan name elan1
2) Create LES/BUS
3) Modify LES/BUS
4) Delete LES/BUS
5) Create LECS
6) Modify LECS
7) Delete LECS
8) Add elan to LECS database
9) Delete elan from LECS database
10) Add policy to elan in LECS database
11) Delete policy from elan in LECS database
12) Exit configuration menu

```

Enter option :

- To create the LECS, enter the following command:

5

A screen similar to the following displays:

### Configuration for LECS at Slot 2 Port 1

- ```

1) Max Config Direct VCCs to LECS      {1 - 65535}      : 128
2) Seconds before VCC declare idle     {1 - 43200}      : 60
3) Priority for ELAN name policies      {0 - 65535}      : 1
4) Priority for ELAN type policies      {0 - 65535}      : 0 - not used
5) Priority for ATM addr prefix policies {0 - 65535}      : 0 - not used
6) Priority for MAC address policies    {0 - 65535}      : 0 - not used
7) Priority for Max. Frame Size policies {0 - 65535}      : 0 - not used
8) Priority for Route Descriptor policies {0 - 65535}      : 0 - not used
9) Admin Status                        { Disable (1), Enable (2) } : Enable
10) Disable WKA registration { No (1), Yes (2) } : No
    
```

Enter (option=value/save/cancel) :

The fields on this screen have the following meanings:

Max Config Direct VCCs to LECS {1-512}

The maximum number of simultaneous VCCs (Virtual Channel Connections) that the LECS can support at one time. A higher number requires more RAM and processing time.

Seconds before VCC declare idle {1-43200}

The number of seconds before the LECS releases an idle VCC. Releases will only occur after the maximum number of Direct VCCs (as configured above) has been reached.

Priority for ELAN name policies {1-65535}

The priority of ELAN name policies in regards to the LECS. The lower the number, the higher the priority. The LECS uses this, and the other priority settings, to determine which ELANs are allowed to establish a connection when multiple requests are received at once.

Priority for ELAN type policies {1-65535}

The priority of ELAN type policies in regards to the LECS.

Priority for ATM addr prefix policies {1-65535}

The priority of ATM address prefix policies in regards to the LECS.

Priority for MAC address policies {1-65535}

The priority of MAC address policies in regards to the LECS.

Priority for Max. frame size policies {1-65535}

The priority of maximum frame size policies in regards to the LECS.

Priority for Route Descriptor policies {1-65535}

The priority of route descriptor policies in regards to the LECS.

Admin Status {Enable (1), Disable (2)}

Used to enable or disable the LECS. If the LECS is disabled, no LANE clients (LECs) will be able to join secured ELANs (because the ELAN's LES/BUS address must be supplied by the LECS in order for the LECs to make a connection).

Disable WKA Registration {No (1), Yes (2)}

Used to enable or disable Well-Known Address (WKA) registration. If WKA registration is enabled (i.e., not disabled, which is the default), then the LECS's WKA will be registered in the cell switch's Integrated Local Management Interface (ILMI) service registry table.

2. You do not need to change any of the defaults settings for the options on this screen. If you do wish to change any of them. Enter the option number first, followed by an "equals" (=) sign, then the desired value.
3. When you are finished setting the options, you must save the configuration to create the LECS. To do so, enter the following command:

save

If you wish to abort, simply enter the **cancel** command.

After entering the **save** command, a message similar to the following displays:

Creating LECS on slot 2, port 1, please wait...

Modifying the LECS

Option 6 on the **lsmcfg** submenu (“Modify LECS”) is used to modify the configuration of an existing LECS.

Here is what the menu looks like before you enter any command:

- ```

1) Global elan name elan1
2) Create LES/BUS
3) Modify LES/BUS
4) Delete LES/BUS
5) Create LECS
6) Modify LECS
7) Delete LECS
8) Add elan to LECS database
9) Delete elan from LECS database
10) Add policy to elan in LECS database
11) Delete policy from elan in LECS database
12) Exit configuration menu

```

Enter option :

- To display the existing configuration of the LECS, enter the following command:

6

A screen similar to the following displays:

### Configuration for LECS at Slot 2 Port 1

- ```

1) Max Config Direct VCCs to LECS      {1 - 512}      : 128
2) Seconds before VCC declare idle     {1 - 43200}    : 60
3) Priority for ELAN name policies      {0 - 65535}    : 1
4) Priority for ELAN type policies      {0 - 65535}    : 0 - not used
5) Priority for ATM addr prefix policies {0 - 65535}    : 0 - not used
6) Priority for MAC address policies     {0 - 65535}    : 0 - not used
7) Priority for Max. Frame Size policies {0 - 65535}    : 0 - not used
8) Priority for Route Descriptor policies {0 - 65535}    : 0 - not used
9) Admin Status                        { Disable (1), Enable (2) } : Enable

```

Enter (option=value/save/cancel) :

This screen shows the parameters that were originally entered for this LECS. The meaning of the options at this screen is given earlier under the heading *Creating the LECS* on page 35-13.

- If you want to make changes to any of these parameters, enter the desired option number first, followed by an “equals” (=) sign, then the desired value.
- When you are finished changing the parameters for each option, you must save the changes you have made. To save changes, enter the following command:

save

But, if you wish to abort and discard changes, simply enter the **cancel** command.

Deleting the LECS

Option 7 on the **lsmcfg** submenu (“Delete LECS”) is used to delete the existing LECS.

Here is what the menu looks like before you enter any command:

- 1) Global elan name elan1
- 2) Create LES/BUS
- 3) Modify LES/BUS
- 4) Delete LES/BUS
- 5) Create LECS
- 6) Modify LECS
- 7) Delete LECS
- 8) Add elan to LECS database
- 9) Delete elan from LECS database
- 10) Add policy to elan in LECS database
- 11) Delete policy from elan in LECS database
- 12) Exit configuration menu

Enter option :

1. To delete the LECS, enter the following command:

7

A screen similar to the following displays:

```
Status of LECS at slot 2 port 1:
State                               : Operational
  Time of last state change         : 12.34.56.55
  Elapsed time since last change    : 00.00.04.44
Error Log                           : no errors
Well-known address                   : Registered with ATM switch
```

Delete this LECS ([N]/Y):

2. To answer “yes”, enter the following command (the default response is **N** for “no”):

Y

A message will appear informing you of the deletion.

Adding ELANs to the LECS

Option 8 on the **lsmcfg** submenu (“Add elan to LECS database”) is used to add existing ELANs (LES/BUS pairs) to the LECS database.

Here is what the menu looks like before you enter any command:

- 1) Global elan name elan1
- 2) Create LES/BUS
- 3) Modify LES/BUS
- 4) Delete LES/BUS
- 5) Create LECS
- 6) Modify LECS
- 7) Delete LECS
- 8) Add elan to LECS database
- 9) Delete elan from LECS database
- 10) Add policy to elan in LECS database
- 11) Delete policy from elan in LECS database
- 12) Exit configuration menu

Enter option :

1. First, you must specify that you want to add an existing ELAN to the LECS database. To do so, enter the following command:

8

A screen similar to the following displays:

- 1) ELAN name (32 chars max) :
 - 2) Elan type {802.3 (1), 802.5 (2)} : 802.3
 - 3) Max Frame Size { 1516 (1), 4544 (2)
9234 (3), 18190 (4) } : 1516
 - 4) Primary LES's ATM address :
index ATM address

 - 5) Backup LES { No (1), Yes (2) } : No
- Enter (option=value/save/cancel) :

2. Enter the name of an existing ELAN. For example, if the name is “elan1”, you would enter the following command:

1=elan1

A screen similar to the following displays:

- 1) ELAN name (32 chars max) : elan1
 - 2) Elan type {802.3 (1), 802.5 (2)} : 802.3
 - 3) Max Frame Size { 1516 (1), 4544 (2)
9234 (3), 18190 (4) } : 1516
 - 4) Primary LES's ATM address :
index ATM address

local 0000000000000000000000000000000020da8055fdd2
 - 5) Backup LES { No (1), Yes (2) } : No
- Enter (option=value/save/cancel) :

The fields on this screen have the following meanings:

ELAN name {32 chars max}

The name (a text string) given to this ELAN to identify it.

Elan type {802.3 (1), 802.5 (2) }

The assigned type of ELAN. Ethernet ELANs are 802.3 while Token Ring ELANs are 802.5.

Max Frame Size {1516 (1), 4544 (2), 9234 (3), 18190 (4)}

The maximum size, in octets, for the data frames sent to/from this ELAN. The default for Ethernet is 1516; for Token Ring, 9234. Token Ring ELANs can also support sizes of 4544 and 18190. To avoid packet loss, you should select a setting for the LECS which matches, or is a higher rate than, the maximum size used by the LE Clients on the ELAN.

Primary LES's ATM address

The ATM address of the Primary LES. This field is automatically filled by the program.

Backup LES {No (1), Yes (2)}

Used to specify whether a backup LES is in service for this ELAN. If you set this option to "yes", you will be prompted to enter the ATM address for the backup LES.

3. The ATM address of the ELAN has been automatically entered in Option 4 by the program. If you wish to change any of the values of any of the *other* options on this screen, do so now. To make a change, enter the option number first, followed by an "equals" (=) sign, then the desired value.
4. When you are finished setting all the options, you must save the configuration to record the changes you have made. To do so, enter the following command:

save

But, if you wish to abort out of the procedure, simply enter the **cancel** command.

After entering the **save** command, a message similar to the following displays:

elan elan1 added to the LECS database

Deleting an ELAN from the LECS

Option 9 on the **lsmcfg** submenu (“Delete elan from LECS database”) is used to delete one or more ELANs that have been added to the LECS database.

Here is what the menu looks like before you enter any command:

```

1) Global elan name                elan1
2) Create LES/BUS
3) Modify LES/BUS
4) Delete LES/BUS
5) Create LECS
6) Modify LECS
7) Delete LECS
8) Add elan to LECS database
9) Delete elan from LECS database
10) Add policy to elan in LECS database
11) Delete policy from elan in LECS database
12) Exit configuration menu

```

Enter option :

1. First, you must specify that you want to delete an ELAN from the LECS. If you did not use Option 1 to set a “global” ELAN name, you would enter the following command:

9

A screen similar to the following displays:

Enter (elan name) :

2. To proceed to delete “elan1” from the LECS, enter the following command:

elan1

A screen similar to the following displays:

Remove elan elan2 from LECS database (n)? :

3. To answer “yes”, enter the following command (the default response is **N** for “no”):

Y

A message will appear to tell you if there was any problem with the deletion.

If the deletion was successful, you will simply be returned to the **lsmcfg** menu:

LSM configuration for slot 2, port 1

```

1) Global elan name                elan1
2) Create LES/BUS
3) Modify LES/BUS
4) Delete LES/BUS
5) Create LECS
6) Modify LECS
7) Delete LECS
8) Add elan to LECS database
9) Delete elan from LECS database
10) Add policy to elan in LECS database
11) Delete policy from elan in LECS database
12) Exit configuration menu

```

Enter option :

Adding Policies to ELANs in the LECS

Option 10 on the **lsmcfg** submenu (“Add policy to elan in LECS database”) is used to add policies to the ELANs you have added to the LECS database. The available policies are: ELAN name, ELAN type, ATM address prefix, MAC address, maximum frame size, and route descriptor. By setting any one of these policies, you can control which LAN Emulation Clients (LECs), and consequently which Groups and VLANs, are allowed by the LECS to join the identified ELAN. You can use any or all of the policy options to set up multiple criteria for a LEC’s acceptance into an ELAN.

Here is what the menu looks like before you enter any command:

- 1) Global elan name elan1
- 2) Create LES/BUS
- 3) Modify LES/BUS
- 4) Delete LES/BUS
- 5) Create LECS
- 6) Modify LECS
- 7) Delete LECS
- 8) Add elan to LECS database
- 9) Delete elan from LECS database
- 10) Add policy to elan in LECS database
- 11) Delete policy from elan in LECS database
- 12) Exit configuration menu

Enter option :

1. First, you must specify that you want to add a policy to an ELAN in the LECS. If you did not use Option 1 to set a “global” ELAN name, you would enter the following command:

10

A screen similar to the following displays:

Enter (elan name) :

2. Enter the name of an existing ELAN. For example, if the name is “elan1”, you would enter the following command:

elan1

A screen similar to the following displays:

Add policy value to elan ‘elan1’

- 1) By Elan name { No (1), Yes (2) } : No
- 2) By Elan type { No (1), Yes (2) } : No
- 3) By ATM address prefix { No (1), Yes (2) } : No
- 4) By MAC address { No (1), Yes (2) } : No
- 5) By Max. Frame size { No (1), Yes (2) } : No
- 6) By Route Descriptor { No (1), Yes (2) } : No

Enter (option=value/exit) :

The fields on this screen have the following meanings:

By Elan name {No (1), Yes (2)}

If set to “yes”, enters a policy value of “by ELAN name.” Only those LAN Emulation Clients (LECs) which match this policy will be allowed to join the specified ELAN.

By Elan type {No (1), Yes (2)}

If set to “yes”, enters a policy value of “by ELAN type.” Only those LAN Emulation Clients (LECs) which match this policy will be allowed to join the specified ELAN.

By ATM address prefix {No (1), Yes (2)}

If set to “yes”, enters a policy value of “by ATM address prefix.” Only those LAN Emulation Clients (LECs) which match this policy will be allowed to join the specified ELAN.

By MAC address {No (1), Yes (2)}

If set to “yes”, enters a policy value of “by MAC address.” Only those LAN Emulation Clients (LECs) which match this policy will be allowed to join the specified ELAN.

By Max. Frame size {No (1), Yes (2)}

If set to “yes”, enters a policy value of “by Maximum frame size.” Only those LAN Emulation Clients (LECs) which match this policy will be allowed to join the specified ELAN.

By Route Descriptor {No (1), Yes (2)}

If set to “yes”, enters a policy value of “by Route descriptor.” Only those LAN Emulation Clients (LECs) which match this policy will be allowed to join the specified ELAN.

- To add policies, for example “By Elan type”, to the criteria for the specified ELAN, you would enter the following command:

2=2

A screen similar to the following displays:

Enter elan type:

- To specify that Ethernet must be used, you would enter the following command:

802.3

A screen similar to the following displays:

policy added to LECS database for elan ‘elan1’

Add policy value to elan ‘elan1’

- | | |
|---|--------------|
| 1) By Elan name { No (1), Yes (2) } | : No |
| 2) By Elan type { No (1), Yes (2) } | : Yes |
| 3) By ATM address prefix { No (1), Yes (2) } | : No |
| 4) By MAC address { No (1), Yes (2) } | : No |
| 5) By Max. Frame size { No (1), Yes (2) } | : No |
| 6) By Route Descriptor { No (1), Yes (2) } | : No |

Enter (option=value/exit) :

- If you wish to change any of the values of any of the other options on this screen, you can do so now. Simply enter the option number first, followed by an “equals” (=) sign, then the desired value.

- To exit and save changes, enter the following command:

exit

Deleting Policies from ELANs in the LECS

Option 11 on the **ismcfg** submenu (“Delete policy from elan in LECS database”) is used to delete one or more policies already associated with the ELANs in the LECS database.

Here is what the menu looks like before you enter any command:

- 1) Global elan name elan1
- 2) Create LES/BUS
- 3) Modify LES/BUS
- 4) Delete LES/BUS
- 5) Create LECS
- 6) Modify LECS
- 7) Delete LECS
- 8) Add elan to LECS database
- 9) Delete elan from LECS database
- 10) Add policy to elan in LECS database
- 11) Delete policy from elan in LECS database
- 12) Exit configuration menu

Enter option :

1. First, you must specify that you want to delete a policy from an ELAN in the LECS. If you did not use Option 1 to set a “global” ELAN name, you would enter the following command:

11

A screen similar to the following displays:

Enter (elan name) :

2. To delete a policy from an ELAN named “elan1”, you’d enter the following command:

elan1

A screen similar to the following displays:

Delete policy value from elan ‘elan1’

- 1) By Elan name { No (1), Yes (2) } : No
- 2) By Elan type { No (1), Yes (2) } : Yes
- 3) By ATM address prefix { No (1), Yes (2) } : No
- 4) By MAC address { No (1), Yes (2) } : No
- 5) By Max. Frame size { No (1), Yes (2) } : No
- 6) By Route Descriptor { No (1), Yes (2) } : No

Enter (option=value/exit) :

3. To delete the policy of “By Elan type”, you would enter the following command:

2=1

A screen similar to the following displays:

Enter elan type:

4. To specify the type to be deleted is Ethernet, you would enter the following command:

802.3

5. To exit and save changes, enter the following command:

exit

Displaying LES/BUS Pair Status

The **vlb** command on the LANE Service Menu (see *The LANE Service Menu (LSM)* on page 35-4) is used to display information about the status and configuration of a given LES/BUS pair on a given physical interface.

To display information about a specific LES/BUS pair (for example, one named “elan1” configured on slot 2, port 1), you would enter the following command:

```
vlb 2/1 elan1
```

A screen similar to the following displays:

```
ELAN Name:          elan1
ELAN Type:          Ethernet
# of Proxy LEC's:   2
# of Non-Proxy LEC's: 0
LES ATM Address:    0000000000000000000000000020da8055fdd2

-Status-
LES-BUS State:      OPERATIONAL
Major Reason LES-BUS was last Down: none
Minor Reason LES-BUS was last Down: none
LES-BUS State last changed at: 00.48.57.23 (System Up Time)
LES-LEC Status Table changed at: 00.51.44.51 (System Up Time)
BUS-LEC Status Table changed at: 00.51.44.64 (System Up Time)

-Current Configuration-
LES-BUS Enabled/Disabled: Enabled
ELAN Type: (S2) Ethernet
Max Frame Size: (S3) 1516
Control Timeout: (S4) 120
Max Frame Age: (S5) 1
Redundancy: Disabled
```

The fields on this screen have the following meanings:

ELAN Name

Shows the text string you entered as the name for this ELAN.

ELAN Type

Indicates the type of this ELAN. The possible entries are “Ethernet” and “Token Ring.”

of Proxy LEC's

Indicates the number of “proxy” LEC's.

of Non-Proxy LEC's

Indicates the number of “non-proxy” LEC's.

LES ATM Address

Shows the ATM address of this ELAN in the LAN Emulation Server.

LES-BUS State

Indicates the operational status of this ELAN.

Major Reason LES-BUS was last Down

Indicates the reasons why LES/BUS services went down.

Minor Reason LES-BUS was last Down

Indicates any additional information about why the LES/BUS services went down.

LES-BUS State Last changed at

Indicates the system time when the LES-BUS state last changed.

LES-LEC Status Table changed at

Indicates the system time when the LES-LEC Status Table last changed.

BUS-LEC Status Table changed at

Indicates the system time when the BUS-LEC Status Table last changed.

LES-BUS Enabled/Disabled

Indicates whether this LES/BUS has been set to the “enabled” or the “disabled” state.

ELAN Type

Indicates the type of this ELAN. The possible entries are “Ethernet” and “Token Ring.”

MAX Frame Size

Indicates the maximum data frame size, in octets, for the data frames sent to/from this ELAN.

Control Timeout

Indicates the time period, in seconds, specified for the timing-out of most request/response control frames.

MAX Frame Age

Indicates the number of seconds allowed for the BUS to transmit the frame. If the age is exceeded, the BUS will discard the frame.

Redundancy

Indicates whether the redundancy options has been enabled or disabled for this LES/BUS.

Displaying LES/BUS Pair Statistics

The `vlbs` command on the LANE Service Menu (see *The LANE Service Menu (LSM)* on page 35-4) is used to display operational statistics for a LES/BUS pair.

To do so for an ELAN named “elan1”, you would enter the following command:

```
vlbs 2/1 elan1
```

A screen similar to the following displays:

```
Statistics for LES/BUS:
ATM Forum LES MIB Statistics:

joinOK:                                0
verNotSup:                              0
invalidReqParam:                         0
dupLanDest:                              0
dupAtmAddr:                              0
insRes:                                  0
accDenied:                               0
invalidReqId:                            0
invalidLanDest:                          0
invalidAtmAddr:                          0
badPkts:                                  0
outRegFails:                             0
leArpIn:                                  0
leArpFwd:                                 0
Other Statistics:
leArpAnswers:                            0
leArpRspFwd:                             0
topologyFwd:                             0
narpFwd:                                  0
flushRspFwd:                             0
outJoinFails:                            0
regOK:                                    0
unRegOK:                                  0
outUnRegFails:                           0
proxyLeacs:                              0
nonProxyLeacs:                           0
macAddrMappings:                         0
rdMappings:                              0
atmAddrMappings:                         0
joinRetransmits:                         0
joinParmChanges:                         0
joinTimeouts:                            0
reRegs:                                   0
ctlDirRefused:                           0
ctlDirReleased_err:                      0
ctlDistFailure:                          0
ctlDistReleased_err:                     0
ctlDistPartyReleased_err:                0
redundancyVccRefused:                    0
redundancyVccReleased:                   0
redundancyVccFailure:                    0
oam_droppedFrames:                       0
invalidSize_droppedFrames:               0
invalidMarker_droppedFrames:             0
invalidProtocol_droppedFrames:           0
verNotSup_droppedFrames:                 0
invalidLecid_droppedFrames:              0
unknownLecid_droppedFrames:              0
invalidOpcode_droppedFrames:             0
dupJoin_droppedFrames:                   0
incompleteSourceJoin_droppedFrames:      0
incompleteTargetJoin_droppedFrames:      0
noProxy_droppedFrames:                   0
```

The fields on this screen have the following meanings:

joinOK

Indicates the number successful Join responses sent out by the LAN Emulation Server.

verNotSup

Indicates the number of version not supported errors.

invalidReqParam

Indicates the number of invalid request parameters errors.

dupLanDest

Indicates the number of times that the LES has received the same LAN destination registration from another LEC.

dupAtmAddr

Indicates the number of duplicate ATM address errors.

insRes

Indicates the number of insufficient resources to grant errors.

accDenied

Indicates the number of access denied for security reasons errors.

invalidReqId

Indicates the number of invalid LEC ID errors.

invalidLanDest

Indicates the number of invalid LAN destination errors.

invalidAtmAddr

Indicates the number of invalid ATM address errors.

badPkts

Indicates the number of malformed ATM ARP requests.

outRegFails

Indicates the number of registration failures sent out by this LES.

leArpIn

Indicates the total number of LE_ARP_REQUEST frames the LES has accepted since its last initialization.

leArpFwd

Indicates the number of LE_ARP_REQUESTs that the LES forwarded onto the clients (either via the control distribute or individually over each control direct) rather than answering directly. This may be due to implementation decision (forward all requests) or because the resolution to the request did not reside in the LES's LE ARP cache.

leArpAnswers

Indicates the number of ARP requests answered by LES.

leArpRspFwd

Indicates the number of ARP responses forwarded by LES.

topologyFwd

Indicates the number of topology frames forwarded by LES.

narpFwd

Indicates the number of NARP frames forwarded by LES.

flushRspFwd

Indicates the number of flush response frames forwarded by LES.

outJoinFails

Indicates the number of Join responses transmitted with unsuccessful status values, including retransmissions.

regOK

Indicates the number of successful registration responses sent by LES, includes reregistrations.

unRegOK

Indicates the number of successful unregistration responses sent by LES.

outUnRegFails

Indicates the number of unregistration responses transmitted with unsuccessful status values.

proxyLecs

Indicates the number of Proxy LECs currently joined to LES.

nonProxyLeCs

Indicates the number of Non-Proxy LECs currently joined to LES.

regMacAddr

Indicates the number of MAC address mappings currently in the database.

regRd

Indicates the number of route descriptor mappings currently in the database.

regAtmAddr

Indicates the number of unique ATM addresses currently in mapping database.

joinRetransmits

Indicates the number of Join response retransmissions.

joinParmChanges

Indicates the number of LEC ELAN memberships terminated because parms changed on subsequent Join request.

joinTimeouts

Indicates the number of Join timeouts.

reRegs

Indicates the number of reregistrations.

ctlDirRefused

Indicates the number of Control Direct VCC call setup requests rejected by the LES for any reason.

ctlDirReleased_err

Indicates the number of Control Direct VCCs released by LEC/network with cause code indicating error.

ctlDistFailure

Indicates the number of Control Distribute VCC requests made by LES that failed for any reason (includes calls to first and subsequent parties).

ctlDistReleased_err

Indicates the number of Control Distribute VCCs released by LEC/network due to error (this is release of entire point-to-multipoint VCC, not just one party).

ctlDistPartyReleased_err

Indicates the number of times call to party on Control Distribute VCC was released by LEC/network with cause code indicating error.

redundancyVccRefused

Indicates the number of redundancy VCCs refused by the LES.

redundancyVccReleased

Indicates the number of redundancy VCCs released by the LES.

redundancyVccFailure

Indicates the number of redundancy VCC failures.

oam_droppedFrames

Indicates the number of OAM frames dropped by the LES.

invalidSize_droppedFrames

Indicates the number of frames dropped by LES due to frame size being invalid for a control frame.

invalidMarker_droppedFrames

Indicates the number of frames dropped by LES due to invalid marker.

invalidProtocol_droppedFrames

Indicates the number of frames dropped by LES due to invalid protocol.

verNotSup_droppedFrames

Indicates the number of frames dropped by LES due to incorrect version number.

invalidLecid_droppedFrames

Indicates the number of frames dropped by LES due to unknown LECID (these are NARP and topology requests).

unknownLecid_droppedFrames

Indicates the number of frames dropped by LES due to unknown LECID (these are ARP and FLUSH responses).

invalidOpcode_droppedFrames

Indicates the number of frames dropped by LES due to invalid opcode.

dupJoin_droppedFrames

Indicates the number of duplicate Join requests dropped by LES because processing of the original request had not been completed.

incompleteSourceJoin_droppedFrames

Indicates the number of frames dropped by LES because source LEC had not completed the JOIN phase.

incompleteTargetJoin_droppedFrames

Indicates the number of frames dropped by LES because target LEC had not completed the JOIN phase.

noProxy_droppedFrames

Indicates the number of “unknown” ARP requests dropped by LES because the ELAN had no proxy LEC members.

Displaying LES/BUS Configuration

The **vlbc** command on the LANE Service Menu (see *The LANE Service Menu (LSM)* on page 35-4) is used to display the configuration of a LES/BUS pair.

To do so for an ELAN named “elan1”, you would enter the following command:

```
vlbc 2/1 elan1
```

A screen similar to the following displays:

LES-BUS Enabled/Disabled:	Enabled
ELAN Type: (S2)	Ethernet
Max Frame Size: (S3)	1516
Control Timeout: (S4)	120
Max Frame Age: (S5)	1
Redundancy:	Disabled

This screen shows the same configuration information as is displayed by the **vlb** command:

LES-BUS Enabled/Disabled

Indicates whether this LES/BUS has been set to the “enabled” or the “disabled” state.

ELAN Type

Indicates the type of this ELAN. The possible entries are “Ethernet” and “Token Ring.”

MAX Frame Size

Indicates the maximum data frame size, in octets, for the data frames sent to/from this ELAN.

Control Timeout

Indicates the time period, in seconds, specified for the timing-out of most request/response control frames.

MAX Frame Age

Indicates the number of seconds allowed for the BUS to transmit the frame. If the age is exceeded, the BUS will discard the frame.

Redundancy

Indicates whether the redundancy options has been enabled or disabled for this LES/BUS.

Displaying LECs in a LES/BUS Pair

The `vlec` command on the LANE Service Menu (see *The LANE Service Menu (LSM)* on page 35-4) is used to display a list of LAN Emulation Clients (LECs) that are related to a given LES/BUS pair.

To display LEC information related to a specific LES/BUS pair (for example, one named "elan1" configured on slot 2, port 1), you would enter the following command:

```
vlec 2/1 elan1
```

A screen similar to the following displays:

```

Number of LEC's to display: 1
LEC-LES and LEC-BUS State (UP=Up, ID=Idle, --. --.
**=Other; Show specific LEC to see actual) v v

```

LEC Primary ATM Address	Proxy	LEC ID	State LES BUS	#ATM Adrs	#Reg MACs
0000000000000000000000000000000002da8055fdd2	Y	0001	UP UP	1	1

The fields on this screen have the following meanings:

LEC Primary ATM Address

Shows the Primary ATM address of this LEC.

Proxy

Indicates whether or not this LEC is a proxy.

LEC ID

Indicates the LEC ID of this LEC.

State LES

Indicates the operational state of the LES for this LEC.

State BUS

Indicates the operational state of the BUS for this LEC.

#ATM Adrs

Indicates the number of ATM addresses for this LEC.

#Reg MACs

Indicates the number of registered MACs for this LEC.

Displaying MAC Addresses for a LES/BUS Pair

The **vmac** command on the LANE Service Menu (see *The LANE Service Menu (LSM)* on page 35-4) is used to display a list of registered MAC addresses for a LES/BUS pair.

To display registered MAC information related to a specific LEC (for example, one named “elan1” configured on slot 2, port 1 with an ID of 0001), you would enter the following command:

```
vmac 2/1 elan1 0001
```

A screen similar to the following displays:

```
Number of Registered MAC's to display: 1
Registered
MAC Address   Registering ATM Address           Type   LEC
-----
0020da81f8d4  0000000000000000000000000020da8055fdd2  R     0001
```

The fields on this screen have the following meanings:

Registered MAC Address

Shows the Registered MAC address of this LEC.

Registering ATM Address

Indicates the ATM address of the LEC which registered the MAC.

Type

Indicates the database entry types. Possible values are “**R**” for Registered which means the entry was registered by the LEC. and “**S**” for Static Volatile which means the entry was created by the network manager.

LEC ID

Indicates the LE Client identifier for this entry in the table.

Displaying Registered Route Descriptor for a LES/BUS Pair

The **vrđ** command on the LANE Service Menu (see *The LANE Service Menu (LSM)* on page 35-4) is used to display the registered route descriptor for a LES/BUS pair.

To display registered route descriptor information related to a specific LES/BUS pair (for example, one named “elan1” configured on slot 2, port 1), you would enter the following command:

```
vrđ 2/1 elan1
```

A screen similar to the following displays:

```

Number of Route Descriptors to display: 1
Route Descriptors      Registering ATM Address      Type      LEC ID
-----
000000000000000000000000020da8055fdd2  R      0001
    
```

The fields on this screen have the following meanings:

Route Descriptors

Indicates the route descriptor associated with the corresponding ATM addresses.

Registering ATM Address

Indicates the ATM address of the LEC that registered the route descriptor.

Type

Indicates the database entry types. Possible values are “**R**” for Registered which means the entry was registered by the LEC. and “**S**” for Static Volatile which means the entry was created by the network manager.

LEC ID

Indicates the LEC ID for this entry in the table.

Displaying Detailed LEC Information

The `vlec` command on the LANE Service Menu (see *The LANE Service Menu (LSM)* on page 35-4) is used to display detailed LAN Emulation Client (LEC) information by LEC ID. To use this command, you will need to know the LEC ID you want to look at.

To display information for a specific LEC (for example, one that is part of “elan1” configured on slot 2, port 1 with an ID of 0001), you would enter the following command:

```
vlec 2/1 elan1 0001
```

A screen similar to the following displays:

```
LEC ID:                0x0001
LEC ATM Address:       0000000000000000000000000020da8055fdd2
Proxy:                 Yes
LEC State at LES:     OPERATIONAL
Entered LES State at: 00.12.17.44 (System Up Time)
LEC State at BUS:     OPERATIONAL
Entered BUS State at: 00.12.17.73 (System Up Time)
Control Direct Vcc:   OPERATIONAL 0/274
Control Distribute Vcc: OPERATIONAL 0/275
Multicast Send Vcc:   OPERATIONAL 0/276
Multicast Forward Vcc: OPERATIONAL 0/277
MAC Address in Join Req: 0020da:81f8d4
# ATM Address Mappings: 1
# MAC Address Mappings: 1
```

The fields on this screen have the following meanings:

LEC ID

Indicates the LEC ID for which the subsequent information is being displayed.

LEC ATM Address

Indicates the ATM address of the LEC.

Proxy

Indicates whether or not this LEC is a “proxy.”

LEC State at LES

Indicates the state of the LEC in regards to the LES.

Entered LES State at

Shows the system time when this LEC entered the LES state.

LEC State at BUS

Indicates the state of the LEC in regards to the BUS.

Entered BUS State at

Shows the system time when this LEC entered the BUS state.

Control Direct VCC

Indicates the bi-directional point-to-point virtual channel connection to the LES from the LEC for sending control traffic.

Control Distribute VCC

Indicates the uni-directional point-to-point or point-to-multipoint control virtual channel connection to the LEC from the LES for distributing control traffic.

Multicast Send VCC

Indicates the bi-directional point-to-point virtual channel connection to the BUS from the LEC to send multicast and initial unicast data.

Multicast Forward VCC

Indicates the uni-directional point-to-point or point-to-multipoint virtual channel connection from the BUS to the LEC for distributing data from the BUS.

MAC Address in Join Req

Indicates the MAC address in the Join request, if present.

#ATM Address Mappings

Indicates the number of ATM address mappings for this LEC.

#MAC Address Mappings

Indicates the number of MAC address mappings for this LEC.

Displaying LECS Status

The **vlecs** command on the LANE Service Menu (see *The LANE Service Menu (LSM)* on page 35-4) is used to display the status of the LECS.

To display the status of the LECS for a specific physical interface (for example, for slot 2, port 1), you would enter the following command:

```
vlecs 2/1
```

A screen similar to the following displays:

LECS status at slot 2, port 1

State:	Operating normally (88)
Time of last state change:	00.49.26.41
Elapsed time since last change:	00.02.50.83
Error Log:	No error (0)
Local ATM address:	3903488001bc900001000100010020da7e79cdc2
Well-known address:	470079000000000000000000000000a03e00000100

The fields on this screen have the following meanings:

State

Indicates the operating status of the LECS.

Time of last state change

Indicates the system time at which the last state change occurred.

Elapsed time since last change

Indicates the elapsed time since the last state change.

Error Log

Describes the error that caused the LECS to enter the “Down due to Error” state. This information is used for diagnostic purposes.

Local ATM address

Indicates the ATM address of the LECS.

Well-known address

Indicates the “Well-known” ATM address specified for the LECS.

Displaying LECS Statistics

The **vlecss** command on the LANE Service Menu (see *The LANE Service Menu (LSM)* on page 35-4) is used to display statistics related to the LECS.

To display statistics related to the LECS for a specific physical interface (for example, for slot 2, port 1), you would enter the following command:

```
vlecss 2/1
```

A screen similar to the following displays:

```
LECS status at slot 2, port 1

Num ELAN(s) configured in the LECS database: 2

Num configured VCCs           : 1
Num accepted VCC              : 46
Num Rejected VCC              : 0
Num VCCs dropped by LECS     : 0
Num VCCs dropped by caller    : 45
Times exceeded Max VCC       : 0
LECS discarded frames        : 0

LECS responses by status
  Success( 0) : 1
  No Configuration(20) : 89
```

The fields on this screen have the following meanings:

Num ELAN(s) configured in the LECS database

Indicates the number of ELANS currently in the LECS database.

Num configured VCCs

Indicates the number of configured Virtual Channel Connections.

Num accepted VCC

Indicates the number of accepted Virtual Channel Connections.

Num Rejected VCC

Indicates the number of rejected Virtual Channel Connections.

Num VCCs dropped by LECS

Indicates the number of Virtual Channel Connections dropped by the LECS.

Num VCCs dropped by caller

Indicates the number of Virtual Channel Connections dropped by the calling station.

Times exceeded Max VCC

Indicates the number of times the Maximum number of VCCs limit was exceeded.

LECS discarded frames

Indicates the number of frames discarded by the LECS.

LECS responses by status (Success)

Indicates the number of LECS responses in regards to the “Success” status condition.

LECS responses by status (No configuration)

Indicates the number of LECS responses in regards to the “No Configuration” status condition.

Displaying LECS Configuration

The **vlepsc** command on the LANE Service Menu (see *The LANE Service Menu (LSM)* on page 35-4) is used to display the configuration of the LECS.

To display the configuration of the LECS for a specific physical interface (for example, for slot 2, port 1), you would enter the following command:

```
vlepsc 2/1
```

A screen similar to the following displays:

Configuration parameters for LECS at slot 2, port 1

```
Maximum number of config direct VCCs to LECS : 128
Seconds before VCC declared idle             : 60
Number of policy type enabled                 : 1
```

The fields on this screen have the following meanings:

Maximum number of config direct VCCs to LECS

Indicates the maximum number of simultaneous VCCs (Virtual Channel Connections) that the LECS can support at one time.

Seconds before VCC declared idle

Indicates the number of seconds before the LECS releases an idle VCC. Releases will only occur after the maximum number of direct VCCs (as shown above) has been reached.

Number of policy type enabled

Indicates the number of different policy types that have been enabled for LECS.

Note that the above configuration parameters can be changed using the **lsmcfg** command.

Displaying ELANs in the LECS

The **velan** command on the LANE Service Menu (see *The LANE Service Menu (LSM)* on page 35-4) is used to display a list of the ELANs configured in the LECS database.

To display the number of ELANs currently in the LECS for a specific physical interface (for example, for slot 2, port 1), you would enter the following command:

```
velan 2/1
```

A screen similar to the following displays:

ELAN(s) in the LECS database:

Type	MFS	ELAN name
===== Ethernet	===== 1516	===== 'elan1'

The fields on this screen have the following meanings:

Type

Indicates the type of this ELAN. The possible entries are “Ethernet” and “Token Ring.”

MFS

Indicates the maximum data frame size, in octets, for the data frames sent to/from this ELAN.

ELAN name

Shows the text string you entered as the name for this ELAN.

Displaying ELAN Policies in the LECS

The **vpolicy** command on the LANE Service Menu (see *The LANE Service Menu (LSM)* on page 35-4) is used to display the policy values assigned to an ELAN in the LECS.

To display the policies assigned to a specific ELAN in the LECS (for example, for an ELAN named "elan1" in the LECS for slot 2, port 1), you would enter the following command:

```
vpolicy 2/1 elan1
```

A screen similar to the following displays:

```

ELAN name => LES
=====
'elan1'

=> 0000000000000000000000000020da8055fdd2

+++++++

ELAN type => LES
=====
* No ELAN types assigned to ELAN 'elan1'

+++++++

ATM address => LES
=====
* No ATM addresses assigned to ELAN 'elan1'

+++++++

      <MAC addresses displayed using Ethernet bit order>

MAC address => LES
=====
* No MAC addresses assigned to ELAN 'elan1'

+++++++

Frame size => LES
=====
* No max frame sizes assigned to ELAN 'elan1'

+++++++

Route descriptor => LES
=====
* No route descriptors assigned to ELAN 'elan1'

+++++++

```

This screen shows a listing of the policies that have been added for the specified ELAN. All of the possible categories of policies is shown even if they have not been used.

36 Configuring ATM Services

Introduction

Alcatel Omni Switch/Routers and OmniSwitches provide several powerful ATM services. ATM Services run over an ATM backbone and provide a variety of mechanisms to switch or route traffic (including Groups and VLANs) over a connection-oriented ATM network:

- Classical IP, ATM Trunking, and Point-to-Point (PTOP) Bridging provide solutions for inter-connecting IP-based networks via ATM backbones.
- LANE Client Services provide connectivity between ATM and non-ATM (legacy) networks by emulating the services of a LAN.
- VLAN Clusters provide a loop-free bridging topology over a meshed ATM backbone.

This chapter documents User Interface (UI) commands to manage ATM services on OmniSwitch and Omni Switch/Router ATM access modules. Except for the following, all software features documented in this chapter can also be configured and monitored with Command Line Interface (CLI) commands:

- Persistent data direct VCs on LANE client services.
- Using Integrated Local Management Interface (ILMI) for the LANE Client Server (LECS) address.
- Using the Well Known Address (WKA) for the LECS address.

For documentation on CLI commands to configure and monitor services on ATM access modules, see the *Text-Based Configuration Reference Manual*.

◆ Important Note ◆

In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory configured to boot up in CLI mode, rather than the UI mode. See Chapter 8, “The User Interface,” for documentation on changing from CLI mode to UI mode.

ATM Services

Alcatel ATM access modules (ASMs and FCSMs on the OmniSwitch and ASXs on the Omni Switch/Router) provide support for six (6) ATM services:

- LANE Client (Ethernet and Token Ring) - enables devices on legacy Ethernet- and Token Ring-based LANs to communicate over ATM networks. (See *LANE Client (LEC) Services* on page 36-4.) FDDI services can be supported over either topology by performing appropriate packet translations.
- ATM Trunking - enables Groups and VLANs to be extended across an ATM backbone network. (See *ATM Trunking* on page 36-9.)
- Classical IP Routing (RFC 1577) - provides connectivity between IP-based networks via an ATM backbone network. (See *Classical IP Routing* on page 36-12.)

- Point to Point Bridging - enables two groups to communicate across an ATM network using a single virtual circuit (VC). (See *Point-to-Point Bridging* on page 36-14.)
- VLAN Clusters - enables mesh-interconnection of point-to-point and point-to-multipoint virtual circuits. (See *VLAN Clusters* on page 36-15.)

◆ **Note** ◆

Only 64 neighbors are supported in a VLAN cluster service (i.e., X-LANE) per ATM access port on OmniSwitches with an MPM-II or MPM-1G.

- 1483 Routed Format - enables transport of IP over ATM. (See *1483 Routed Format Services* on page 36-19.)

On the FCSM II and Omni Switch/Router ASX modules, you can also create 1483 Scaling Services, which enable approximately 1000 permanent virtual circuits (PVCs) on a single port. Each virtual circuit (VC) maps to an OmniSwitch group ID. (See *1483 Scaling Services* on page 36-17.)

Except for 1483 scaling services, you can run multiple services of the same or different type on a single port. (If you configure one or more 1483 scaling services on a FCSM II, you will be able to configure one PTOP service on this module but no more additional ATM services of any kind.) Each ATM port (a single base MAC address) can support up to 16 bridging services.

With two ATM ports on an ATM access module (two base MAC addresses), up to 32 bridging services are supported. Bridging services include all ATM services except Classical IP. It is possible to add more base MAC addresses to an ATM module. (You can have up to 8 MAC address per switching module.) If locally-administered MAC support is enabled, the MAC space is doubled, allowing twice as many ATM services (32). For more information on adding MAC addresses, contact Alcatel Internetworking technical support.

All ATM access ports must be associated with at least one ATM service. When a switch containing an ATM access module is booted up without configuration information, or when an ATM access is hot-swapped into a chassis, a default service is automatically created. This default service will be an Ethernet (802.3) LANE Client. You can delete this default service only after you have created another one. If you delete all services and don't create a new one, a PTOP PVC service will automatically be created.

PVC/SVC Support

ATM services use either PVCs, Switched Virtual Circuits (SVCs), or both, depending upon the service. If you are setting up a service that supports both SVCs and PVCs, you will be prompted for different parameters, depending upon which virtual circuit type you chose.

◆ Note ◆

All newly-installed or unconfigured ATM access ports default to SVC mode, ready to support SSCOP and ILMI protocols.

The table below lists what services support which connection types (SVC or PVC):

Service	SVC	PVC
LANE Client	X	
ATM Trunking	X	X
Classical IP	X	X
PTOP Bridging	X	X
VLAN Clusters		X
1483 Scaling (FCSM II and Omni Switch/Router ASXs Only)		X
1483 Routed Format		X

◆ Note ◆

The current version of software supports ATM SVCs on up to 10 ATM access ports per switch.

LANE Client (LEC) Services

In a LANE configuration, ATM stations become LECs to allow non-ATM devices on legacy Ethernet- and Token Ring-based LANs to communicate over ATM networks and support existing applications. Such a configuration is called an Emulated LAN, or ELAN. This ability to work with existing networking infrastructure makes it possible to plan for a gradual transition from legacy networks to an ATM-based network.

Because ATM is a connection-oriented technology, and Token Ring and Ethernet LANs are connectionless (i.e., based upon MAC addresses), you need some way of correlating ATM addresses to MAC addresses. This is one of the functions that LANE services provides. The ATM access module supplies a LAN Emulation Client (LEC) function, not LANE Services (LES). The OmniMSS normally provides LES. For information on configuring LANE services, see Chapter 35, "LANE Server Configuration."

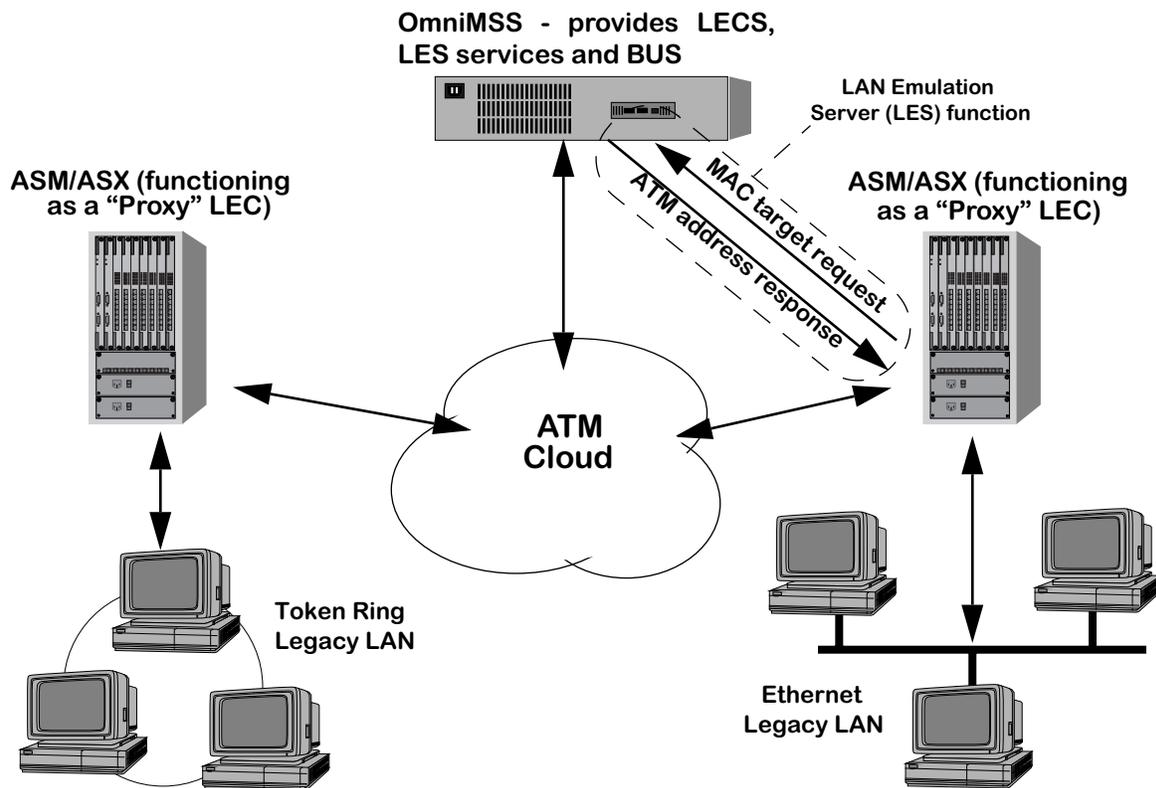
An ELAN consists of the following components:

- LANE Client (LEC): An LEC is responsible for forwarding data and address resolution. This function is provided by an end-station ATM access configured as a LANE Client.
- LAN Emulation Configuration Server (LECS): An LECS assigns clients to particular ELAN services. This function is usually provided by an MSS (Multiprotocol Switching Services)-type device.
- LAN Emulation Server (LES): The LES uses Address Resolution Protocol (ARP) to translate and map MAC addresses to ATM addresses. This service can be provided either by the LES functionality of the MPM/MPX, or an OmniMSS.
- Broadcast and Unknown Server (BUS): The BUS handles initial unicast, multicast and broadcast traffic sent to it by the LEC. This service can be provided either by the BUS functionality of the switch MSM, or an OmniMSS.

The figure on the following page shows the interrelationships of the major components in a typical LANE configuration.

◆ Note ◆

Up to 16 LANE LECs of global MAC address plus 16 LECs of local Administrative MAC address per port and a maximum of 64 LECs per switch has been tested.



LANE Services Architecture

Both the LES and BUS can use either a point-to-multipoint connection or a bidirectional point-to-point connection to communicate with a client (LEC). The LECS uses a point-to-point connection.

Token Ring vs. Ethernet Networks

Token Ring 802.5 LE clients and Ethernet 802.3 clients perform similar functions with the following differences:

- For Token Ring LECs, MAC data frames are transmitted within an 802.5 ELAN type frame using an 802.5 frame format. For Ethernet LECs, MAC data frames are transmitted within an 802.3 ELAN type frame using an 802.3 frame format.
- Token Ring LE_ARPs use a non-canonical MAC address format (i.e., the most significant bit of each address byte is transmitted first), whereas Ethernet LEC clients use a canonical format.
- Source-routed traffic is supported by Token Ring, but not by Ethernet LEC clients.

Source-Routed Traffic

Source-routed traffic is handled by assigning a ring number to the ELAN and adding intelligence to the forwarding decision of the Token Ring LEC. The LEC examines frames for the next hop after the ELAN of which it is a member. With this information, the LEC can forward the frame to the correct next hop LEC. Knowledge of the next hop allows a LEC to avoid forwarding frames to all LECs on the ring—an action that would typically occur in traditional Token Ring networks.

From the perspective of the source routing logic and AutoTracker, a Token Ring LEC is treated like another Token Ring interface. For this reason, source routing commands, such as **sts** (Spanning Tree Statistics) and **stc** (Spanning Tree Configuration), may be used with Token Ring LECs. For more information on using these commands, see Chapter 22, “Configuring Bridging Parameters.”

Ethernet and Token Ring LECs cannot be directly connected. However, ELANs to which dissimilar LECs belong can be connected through the switch via translational bridging or routing.

LANE Version 2.0

In Release 4.0 and higher, LANE Version 2.0 is supported on ATM access modules for the Omni Switch/Router and OmniSwitch. This enhanced version of LANE provides support for ATM Forum Multiprotocol Over ATM (MPOA).

LANE Client (LEC) Enable/Disable Traps

In releases prior to 4.3, Alcatel’s software polled the switch to determine if any LANE Client (LEC) state changes had taken place. In Release 4.3 and later, you can configure traps with the **snmpc** command that will display in real time if a LEC has been enabled or disabled. In addition, these traps contain the following information about the state change for the LEC:

- LEC ID number
- Emulated LAN (ELAN) name
- The 20-character ATM address
- The chassis slot number
- The chassis port number
- The LEC’s service number
- The current state of the LEC
- The state of the LEC prior to the change
- The reason for the LEC state change

◆ Note ◆

See Chapter 17, “SNMP (Simple Network Management Protocol),” for more information on the **snmpc** command.

LAN Emulated Client Start-Up and Back-Off Timers

Alcatel LECs provide the capability of backing-off if the LEC notices calls being released or when multiple LECs on the same switch are being enabled at the same time (e.g., a cable is disconnected/reconnected). The amount of time (in ticks) and nature (fixed/random) of the back-off period can be controlled using the variables described in the table below.

Timer Name	Description	Range	Default value
atmlec_randomize_throttle	This flag determines if the procedure uses random back off or fixed back off.	0 (fixed back off) or 1 (random back off)	1
atmlec_backoff	The back off percentage in both random and fixed procedures. For example, setting this flag will set the percentage to 500%.	>= 100	300
atmlec_lecs_throttle_ticks	All values for ticks should be a power of two (e.g., 8, 16, 32, 64, etc.). Each tick is 16.66 milliseconds long.	Power of 2 and >=2	32
atmlec_les_throttle_ticks	All values for ticks should be a power of two (e.g., 8, 16, 32, 64, etc.). Each tick is 16.66 milliseconds long.	Power of 2 and >=2	32
atmlec_bus_throttle_ticks	All values for ticks should be a power of two (e.g., 8, 16, 32, 64, etc.). Each tick is 16.66 milliseconds long.	Power of 2 and >=2	32
atmlec_lecs_retry	Number of LECS retries before restarting the LEC	>= 3	7
atmlec_les_retry	Number of LES retries before restarting the LEC	>= 3	7
atmlec_bus_retry	Number of BUS retries before restarting the LEC	>= 3	7

It should be noted that the adjustment of these values needs to be done only if the ATM network (which the LECs are connected) is not capable of processing the total number of calls that could be generated by all the LECs connected to the ATM network. This scenario is most likely to occur under the following two situations:

- During a global restart of all the LECs due to power on or power failure.
- During a global attempt to join an ELAN when a central LANE server resource such as LECs/LES/BUS is disconnected/reconnected or some failure.

Each LEC needs to setup a call to the LEC/LES and BUS before it stops retrying. If any fails, the LEC backs off and continues the process of attempting to join the ELAN. The default values are chosen so that calls to the LECs/LES/BUS are individually throttled by a time period of 16.66 — 266.56 milliseconds.

To modify these default timers, you must edit the **mpm.cmd** or **mpx.cmd** command files. (See Chapter 11, “Managing Files,” for more information on editing the command file.). For example, to change the **atmlec_lecs_throttle_ticks** timer on an OmniSwitch to 64, add:

```
atmlec_lecs_throttle_ticks=64
```

to the **mpm.cmd** file.

◆ **Note** ◆

You must add the timers after the **cmInit** line.

Debugging LANE Client Problems

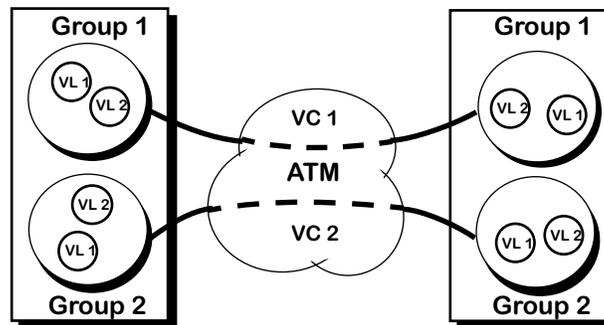
In Release 4.3.2 and higher, you can display LANE client debug messages with the **atmlsem** command. See *Debugging LANE Client Problems* on page 36-75 for more information.

ATM Trunking

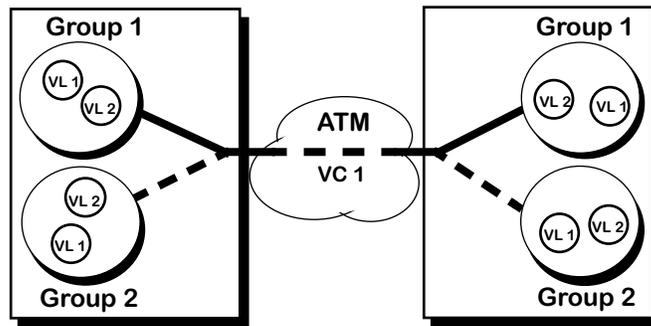
ATM Trunking is a proprietary service that allows Groups and VLANs to be extended across an ATM backbone network. This trunking service operates in a manner similar to Frame Relay Trunking (for more information on Frame Relay Trunking, see the “Trunking” section in Chapter 49, “Managing Frame Relay”).

Groups over ATM

An ATM trunk is actually a virtual connection, rather than a physical line. A common implementation is to connect to an external router to provide interconnectivity. This service enables a single ATM access port to send traffic to multiple destinations on the other side of the ATM cloud. A single ATM port can support several trunk port connections to other switches on an ATM network. The switch will bridge between the assigned trunk ports.



With straight group-to-group bridging (no trunking), different groups must use two separate virtual circuits across an ATM interface.



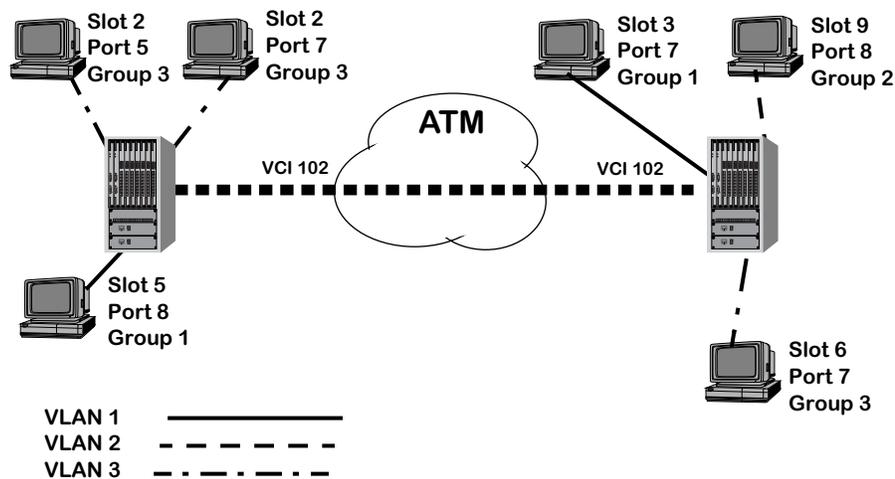
With Trunking, separate Groups can share the same ATM virtual circuit. Group 1 traffic will only be sent to Group 1 and Group 2 traffic will only be sent to Group 2.

VLANs over ATM

An ATM trunking service supports VLANs distributed across an ATM network. Trunk ports encapsulate the bridged frames within a proprietary frame, which includes information needed to reproduce the frame on the opposite end of the trunk and to maintain VLAN separation. Each switch will only participate in those VLANs to which it is assigned.

VLAN Groups can be carried within the encapsulation header. As long as the same VLAN policies are maintained at both ends of the trunk, VLAN segregation may be maintained (via AutoTracker rules; for more details, see Chapter 27, “Managing AutoTracker VLANs”). If a port is configured as a trunk port, it can support groups distributed across multiple switches connected by LANs or ATM networks.

In the example below, members of three different Groups on one side of the ATM cloud are able to communicate with members of their respective Groups on the far end of the ATM cloud (via VCI 102).



Typical VLAN Over ATM Configuration

Physical LAN interfaces are mapped one-to-one to virtual bridge ports. For ATM interfaces, a Trunking service and a Point-to-Point Bridging service could also be run simultaneously on the same VLAN.

Spanning Tree and Trunking

Via a Trunk port, each Group with its own spanning tree can be extended across an ATM network. As with normal Spanning Tree, BPDUs are processed and Spanning Tree dynamically controls the forwarding state.

In software releases prior to 4.3, spanning tree restarts for all existing groups when you add one or more groups to an ATM trunk. In Release 4.3 and later, spanning tree is only restarted on the new group (or groups) added to the ATM trunk; existing groups are unaffected.

Translations Across Trunks

The switch sends frames onto the trunk in the same format as the original LAN type. Any necessary translation is performed at the destination switch.

ATM Trunking and Older ATM Access Modules

If you have an older ATM access module (OmniSwitch ASM and FCSM I modules but not Omni Switch/Router ASX modules or OmniSwitch ASM2 and FCSM II modules) and you want to maintain compatibility with switches running Release 3.2 and earlier versions of ATM trunking, add the following to the **mpm.cmd** file:

```
atm_use_old_trunk=1
```

Make sure that it is added prior to the **cmInit** line. (See Chapter 11, “Managing Files,” for more information on editing the **mpm.cmd** file.)

Classical IP Routing

In classical IP (CIP) routing, ATM is used to interconnect ATM switches with IP-based ATM devices in a routed environment. ATM networks are configured as Logical IP Subnetworks (LISs). Communication between the LIS-configured ATM networks is accomplished through the routing of Groups. A Group is created for routing CIP only. Each Group consists of a router port and its associated ATM CIP service.

LLC Header Encapsulation

CIP is routed across ATM networks by the use of routed Protocol Data Units (PDUs) encapsulated in LLC Headers and distributed over ATM Adaptation Layer 5 (AAL 5). For a detailed description of LLC encapsulation, refer to RFC-1483, *"Multiprotocol Encapsulation Over ATM Adaptation Layer 5."*

IP to ATM Address Resolution

For SVC-based CIP services, the following sequence establishes a CIP connection over an ATM network:

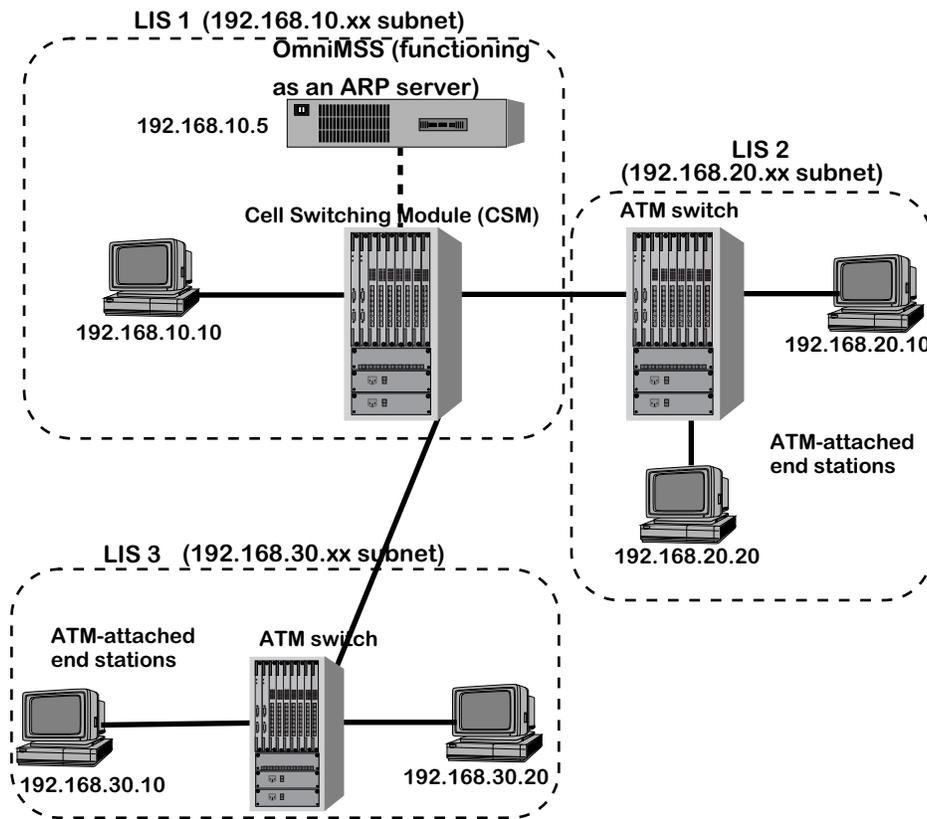
1. An IP Host sends a request to the ARP server. IP addresses are resolved to ATM addresses via the Inverse ARP function of the ARP server within the LIS. An MSS-type device usually provides the ARP server function. (For PVC-based CIP services, no ARP server is required; VCs are configured manually via VCI numbers.)
2. The ARP Server returns an ATM address to the requesting station. Once it has the ATM address, the IP Host will establish an SVC.
3. Once the setup is completed and confirmed a VCI now exists, and data can be sent.

IP Over ATM Signaling

CIP over ATM uses local ATM call control signaling to initiate and terminate ATM connections. For a complete description of the content and format of ATM signaling, refer to RFC-1577, *ATM Signaling Support for IP over ATM."*

Typical CIP over ATM Configuration

In the following illustration, three ATM networks are configured as Logical IP Subnetworks (LIS1, LIS2, and LIS3). The ATM switches in subnets 20.xx and 30.xx provide IP routing services for their respective endstations.



Classical IP Architecture

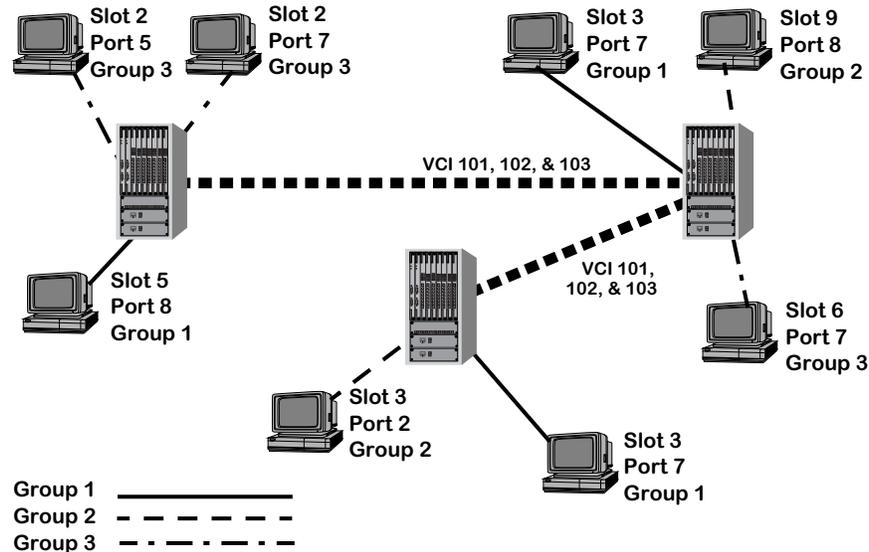
Point-to-Point Bridging

Point to point bridging is a service that enables two Groups to communicate across an ATM network using a single virtual circuit (VC). The VC can be configured to be a Switched Virtual Circuit (SVC) or a Permanent Virtual Circuit (PVC).

Point to point bridging can use either of two types of encapsulation.

- RFC 1483 — LLC encapsulation. RFC 1483 defines two methods for transmitting data over a VC: VC-Based Multiplexing and LLC encapsulation. The OmniSwitch and Omni Switch/Router support only LLC encapsulation. The main advantage of RFC 1483 is its interoperability with other vendors.
- OmniSwitch encapsulation. OmniSwitch encapsulation is a more efficient method, because it uses fewer bytes and word-aligns the frame for transmission.

The following illustration shows how multiple instances of Point-to-Point bridging can be supported over separate VCIs. Three Groups are linked over the ATM backbone in a one-to-one configuration, with Group 1 communicating over VCI 101, Group 2 communicating over VCI 102, and Group 3 communicating over VCI 103.



Point-to-Point Bridging

VLAN Clusters

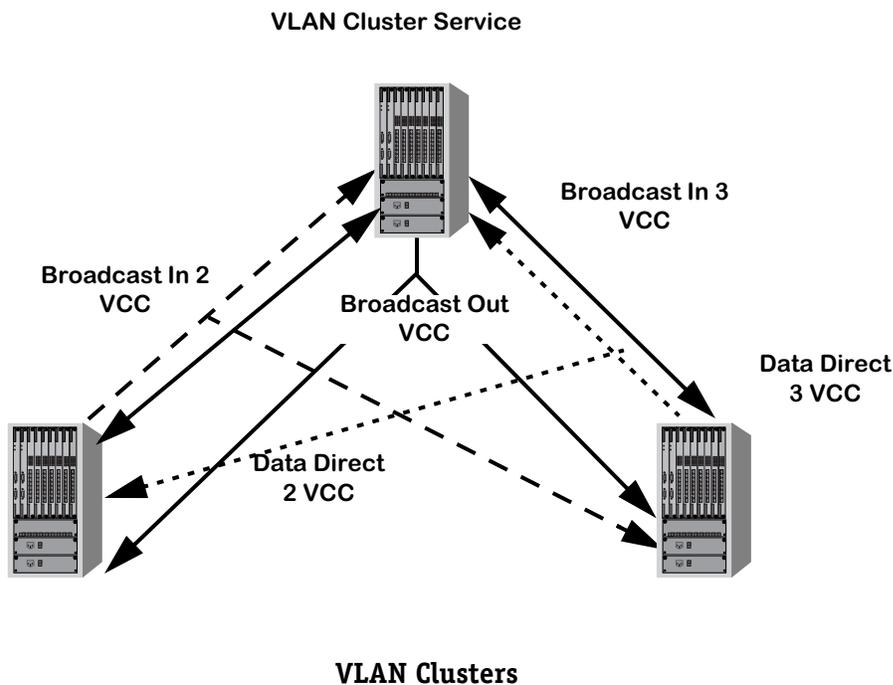
A VLAN cluster (X-LANE) consists of a collection of switches interconnected over an ATM-switched network, in which the switches are mesh-interconnected with point-to-point and (optionally) point-to-multipoint virtual circuits. Up to 33 switches (including the local switch) may be included in a VLAN cluster. The mesh of circuits acts as a single VLAN cloud, appearing as a loop-free bridge topology. This configuration is further optimized through the use of point-to-multipoint virtual circuits to provide a distributed broadcast/unknown capability.

◆ **Note** ◆

Only 64 neighbors are supported in a VLAN cluster service (i.e., X-LANE) per ATM access port on OmniSwitches with an MPM-II or MPM-1G.

A VLAN cluster implementation is similar to LANE, but has the following advantages:

- It is more scalable.
- It is static (no dynamic VCs)
- The need for PNNI is eliminated
- The packet format remains unchanged; no translations are made
- A number of VLAN Groups can be attached to the same VLAN Cluster
- It is not susceptible to a single point of failure or choke point, as is LANE, in which the LE servers must be distributed to avoid creating a single point of failure.



The VLAN Cluster service can interface to multiple VLAN Cluster services over a single ATM interface. You have the option of configuring one or more Groups to multiplex each set of mesh interconnections. (The number of Groups that can be multiplexed depends upon the encapsulation—Private (proprietary) Trunking or 1483—that you select.) The user also has the option to select one of two methods for forwarding of broadcast, multicast, or unknown unicast destination traffic. These two methods are either to allow all traffic to bi-directionally traverse point-to-point (Data Direct) circuits along with the known unicast traffic, or to allow broadcast, multicast and unknown unicast traffic to use a separate set of point-to-multipoint virtual circuits.

VLAN Clusters can use either of two types of ATM virtual circuits; point-to-point or point-to-multipoint. The following paragraphs describe how these circuits are configured for each method of operation.

Method 1

Method 1 provides both point-to-point virtual circuits (for VLAN forwarding) and point-to-multipoint (for flooding) virtual circuits.

- **Data Direct** circuits (Data Direct 2 and Data Direct 3, above) are point-to-point virtual circuits that forward frames that have known unicast destination addresses with a learned association with the circuit. These circuits are used for two-way frame forwarding between pairs of switches in a full mesh throughout the VLAN Cluster.
- **Broadcast** circuits (Broadcast Out, Broadcast In 2, and Broadcast In 3, above) are point-to-multipoint virtual circuits that are used to forward frames that have a broadcast, multicast, or unknown unicast destination address. These circuits are used for one-way traffic only. One circuit originates at each switch and terminates at all switches in the cluster. This configuration provides a distributed BUS function, in contrast to the centralized BUS server provided with LANE.

Method 2

In Method 2, Data Direct circuits provide the functionality of both types of circuits used in method 1. That is, Data Direct circuits provide point-to-point virtual circuits that handle both VLAN forwarding and flooding traffic.

These types of frames must be sent to each switch that is part of the Cluster. Therefore, a copy of a frame is sent on each Data Direct virtual circuit within the Cluster. This method minimizes the number of connections required to support full connectivity between Alcatel switches while providing a loop-free bridged topology.

VLAN Clusters can be configured to use the same encapsulation as that used by either Alcatel's proprietary ATM trunking service or RFC 1483 encapsulation. With VLAN Clusters, Alcatel switches learn the data associated with a remote switch by directly associating the MAC addresses with the circuit.

1483 Scaling Services

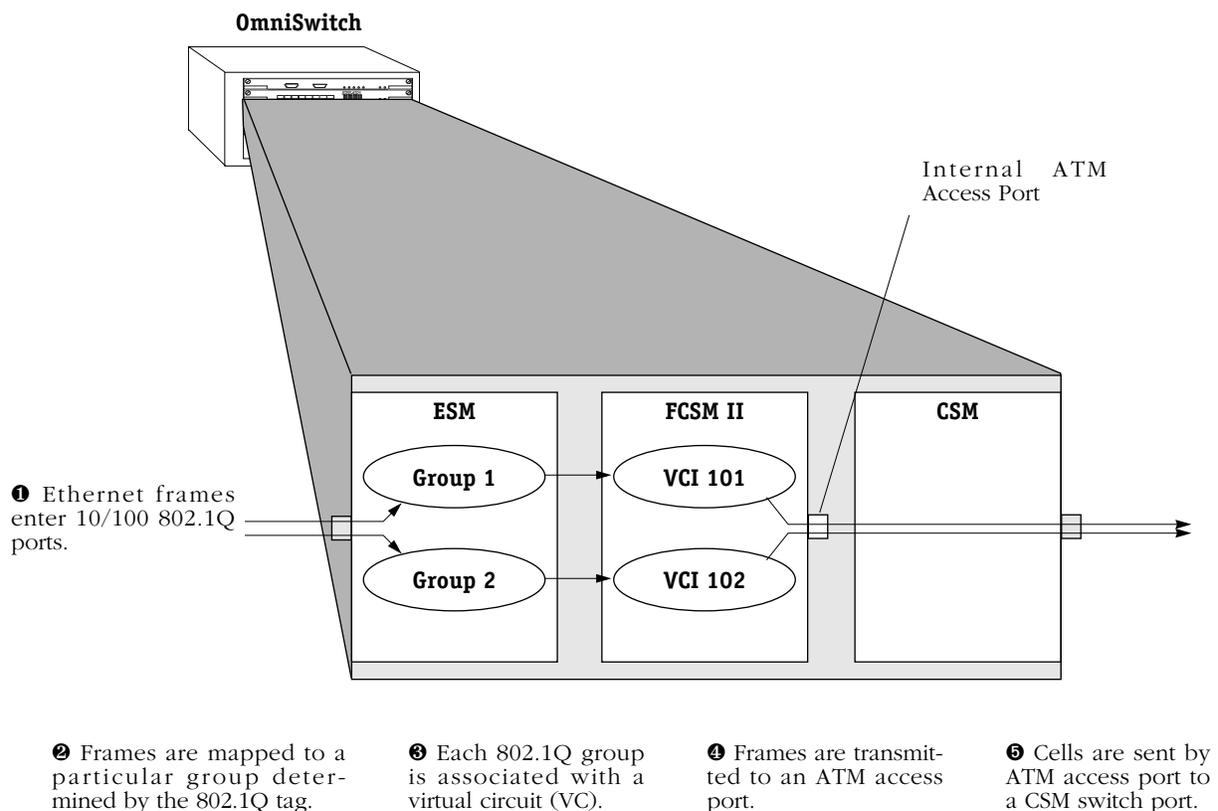
A 1483 scaling service maps OmniSwitch Ethernet groups (including standard IEEE 802.1Q groups) to ATM virtual circuits (VCs) on a one-to-one basis. This is accomplished by mapping the group ID to an ATM Virtual Circuit Identifier (VCI). The use of 1483 data encapsulation ensures interoperability with hardware from other vendors.

◆ Important Note ◆

In the current release, 1483 scaling services are only supported on the FCSM II module and Omni Switch/Router ASX modules.

You can create approximately 1000 permanent virtual circuits (PVCs) on a single port in a 1483 scaling service. (The actual number of services is dependent on the total amount of flash memory.) And a 1483 scaling service can coexist on the same port with other ATM services. However, only one (1) 1483 scaling service can be configured on a port. In addition, Switched Virtual Circuits (SVCs) are not supported.

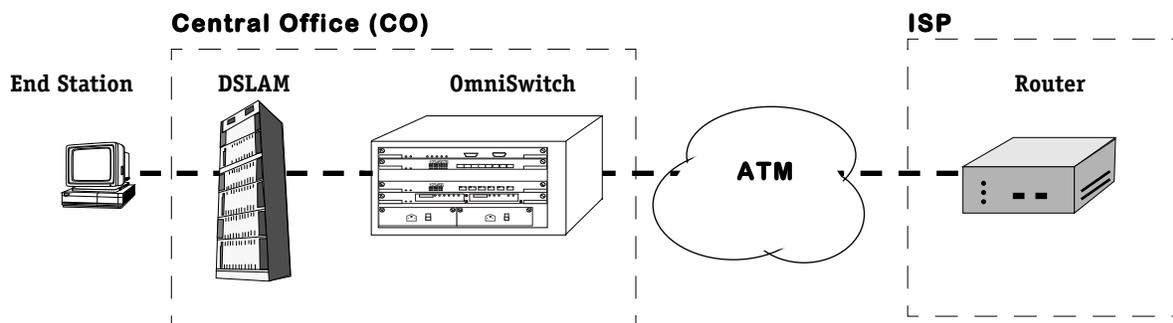
The figure below shows a diagram of a 1483 scaling service. The OmniSwitch is a hybrid LAN/ATM switch with an FCSM II, ESMs, and CSMs. VCI 101 is mapped to 802.1Q Group 1 and VCI 102 is mapped to 802.1Q Group 2. The ESMs map each frame to an 802.1Q group determined by the 802.1Q tag. A 1483 scaling service has been created on an FCSM II, which maps each 802.1Q group to a VC on a one-to-one basis.



1483 Scaling Service Diagram

The FCSM II uses its SAR functionality to convert the frames into cells and transmits them to the OmniSwitch's cell matrix. CSMs then transmit cells across an ATM network. The whole process is reversed for cells received by the CSMs.

The illustration below shows an application of 1483 scaling service. An end station transmits frames to a Digital Subscriber Line Access Multiplexer (DSLAM) device at a Central Office (CO). The DSLAM tags all frames via 802.1Q and transmits the frames across 10/100 Mbps Ethernet lines to an OmniSwitch. The OmniSwitch then transmits the frames across an ATM network to an Internet Service Provider (ISP). The ISP then transmits the frames to a Router.



1483 Scaling Service Application Example

A 1483 scaling service has been created on the OmniSwitch that maps the frames from 802.1Q groups to VCIs according to the 802.1Q group IDs. The OmniSwitch sends the frames across an ATM network to an Internet Service Provider (ISP). The whole process is reversed for cells transmitted back to an end station.

◆ Note ◆

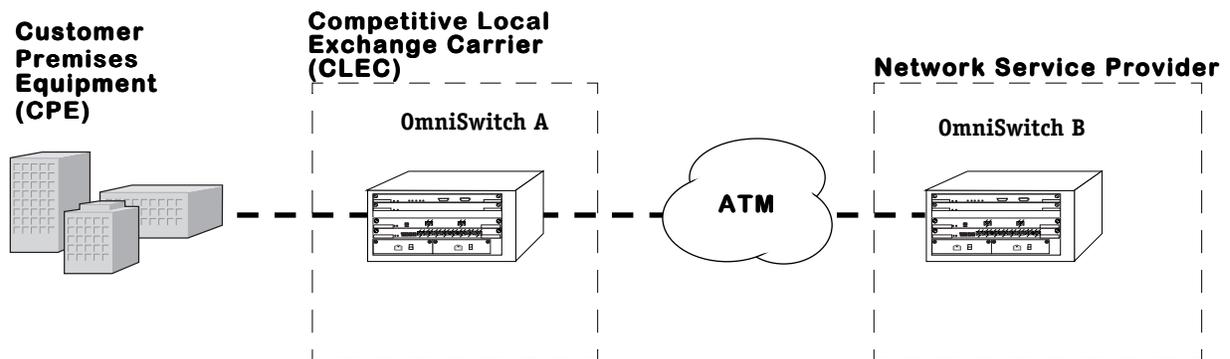
If you configure one or more 1483 scaling services on a FCSM II, you will be able to configure one (1) PTO service on this module but no more additional ATM services of any kind.

1483 Routed Format Services

Currently, most Internet Service Providers (ISPs), Competitive Local Exchange Carriers (CLECs), and other carriers use routers at the edge of their network that are configured to support 1483 routed format service by default. Therefore, 1483 routed format services enhance interoperability of Alcatel switches with switches and routers from other vendors. In addition, this format is the most efficient way to transport IP traffic since there is less overhead due to Layer 2 encapsulation.

The 1483 routed format service is similar to the Classical IP (CIP) service, which is described in *Classical IP Routing* on page 36-12. Like CIP, it uses Protocol Data Units (PDUs) encapsulated in LLC Headers and distributed over ATM Adaptation Layer 5 (AAL 5). However, the 1483 routed format does not run Address Resolution Protocol (ARP), thus saving CPU cycles on the switch. In addition, the 1483 routed format service only supports PVCs and not SVCs.

In the figure below, a 1483 routed format service has been configured on OmniSwitch A that routes frame traffic across an ATM network to a Network Service Provider (NSP).



1483 Routed Format Application Example

In Release 4.4 and later, you can configure, modify, and monitor statistics for routed 1483 services on all ATM access ports through User Interface (UI) commands. In addition, you can monitor statistics for 1483 routed services with Command Line Interface (CLI) commands. Descriptions of UI commands for 1483 routed format services begin on page 36-21. See the *Text-Based Configuration Reference Manual* for descriptions of CLI commands for 1483 routed format services.

◆ Important Note ◆

In the current release, you *cannot* configure or modify 1483 routed services with CLI commands. You must use UI commands to configure or modify 1483 routed format services instead.

Configuring ATM Services

The seven ATM Services (LANE Client, Trunking, Classical IP, Point-to-Point Bridging, VLAN Clusters, 1483 scaling, and 1483 routed) are created and configured primarily with the following commands:

- **cas** - Create a Service. Use this command to create a new ATM service.
- **mas** - Modify a Service. Use this command to modify an existing ATM service.
- **das** - Delete a Service. Use this command to delete an existing ATM service.
- **vas** - View a Service. Use this command to view configuration information for one or all ATM services currently on the switch.

In addition, you can view status and statistical information for LANE Client, Classical IP, VLAN Clusters, and 1483 routed format services with the **vss** command. The **vss** command is part of the ATM menu, but it is not necessary to actually be in the ATM menu when you invoke the command.

Services Menu

To view the Services menu, type **services** at any prompt, then type **?** to see the list of commands.

```
/Services % ?  
  
Command      Service Menu  
-----  
cas          Create a service (PTOP bridging/Classical IP/Trunking/LANE  
mas          Modify a service  
das          Delete a service  
vas          View a service  
  
Main         File      Summary   VLAN      Networking  
Interface   Security  System    Services  Help  
  
Services %
```

Creating a Service

Any of the seven ATM services is created by basically the same process, with additional configuration required for some services. Those parameters unique to a particular service are described under the applicable heading later in this chapter. To create an ATM service:

1. Type **cas**, followed by the slot/port for the service. A screen similar to that shown below is displayed:

```

/Services % cas 3/1

Slot 3 Port 1 Service 1 Configuration

1) Description (30 chars max)      : LAN Emulation Service 2
2) Service type { LANE Client (1),
    1483 Scaling (2),
    Trunking (4),
    Classical IP(5),
    PTOp Bridging(6),
    VLAN cluster(7),
    1483 Routed (14) } : LAN Emulation
21) LAN Type { 802.3 (1),
    802.5 (2) } : 802.3
22) Change LANE Cfg { NO (1),
    YES (2) } : NO
23) V2 Capable { Disable (1),
    Enable (2) } : Enable
24) Persistent Data Direct VC
    { Disable (1),
    Enable (2) } : Disable
3) Connection Type { PVC(1),
    SVC(2) } : SVC
30) SEL for the ATM address : 02
4) LAN Emulated Groups : 1
5) LECS Address (40-char-hex) : Use ILMI (fall back using WKA)
51) Use ILMI { No (1), Yes (2) } : Yes
6) Admin Status { disable(1),
    enable(2) } : Enable
7) Bandwidth Group (1-8) : 1

Enter (option=value/save/cancel) :

```

2. The following fields are common to all ATM service types. Enter values for the remaining fields, as described below:
 - a. **1. Description:** Enter a description of this service (up to 30 characters).
 - b. **2. Service Type:** Note that ATM services for ports on a newly-installed ATM board default to 802.3 LANE Client (LEC), which is described in *Creating a LANE Client Service* on page 36-23. To change the port to another service, enter one of the following:
 - **2=2** for 1483 scaling service, which is described in *Creating a 1483 Scaling Service* on page 36-40.
 - **2=4** for Trunking, which is described in *Creating a Trunking Service* on page 36-31.
 - **2=5** for Classical IP, which is described in *Creating a Classical IP Service* on page 36-33.
 - **2=6** for PTOp Bridging, which is described in *Creating a PTOp Bridging Service* on page 36-36.

- **2=7** for VLAN Cluster, which is described in *Creating a VLAN Cluster Service* on page 36-38.
 - **2=14** for 1483 Routed Format, which is described in *Creating a 1483 Routed Format Service* on page 36-47.
- c. **3. Connection Type:** Enter **3=1** for PVC or **3=2** for SVC. For more details, see *PVC/SVC Support* on page 36-3.
- d. **6. Admin Status:** Enter **6=1** to disable the Administrative Status, **6=2** to enable it. Disabling Admin Status takes the port off-line.
- e. **7. Bandwidth Group:** A bandwidth group is a reserved amount of bandwidth on a port. All ASX, ASM2, and FCSM II modules allow you to configure up to eight (8) bandwidth groups. Bandwidth groups are ordered by priority, with bandwidth group 1 having the highest priority and bandwidth group 8 having the lowest. See Chapter 33, “Managing ATM Access Modules,” for documentation on configuring and displaying bandwidth group parameters.

Creating a LANE Client Service

To create a LANE Client service:

1. Type **cas** followed by the slot/port for the service. A screen similar to that shown below is displayed:

```

/Services % cas 3/1

Slot 3 Port 1 Service 2 Configuration

1) Description (30 chars max)      : PTOp Bridging Service 1
2) Service type { LANE Client (1),
    1483 Scaling (2),
    Trunking (4),
    Classical IP(5),
    PTOp Bridging(6),
    VLAN cluster(7),
    1483 Routed (14) } : PTOp Bridging
10) Encaps Type { Private (1),
    RFC1483(2) } : Private
3) Connection Type { PVC(1),
    SVC(2) } : PVC
4) PTOp Groups : 1
5) PTOp connection : none
6) Admin Status { disable(1),
    enable(2) } : Enable
7) Bandwidth Group (1-8) : 1

Enter (option=value/save/cancel) : 2=1

```

2. Note that, if this is a previously-unconfigured port, the service will have already defaulted to an 802.3 LANE Client service. In that case, this step is not necessary. If you are changing from another service (such as PTOp, as shown above) to LANE Client, enter:

2=1 (for LANE Client)

◆ Note ◆

The connection type must be SVC to use LANE client service. If the connection type is not already SVC, it will automatically be set to SVC when you select LANE Client as the service type. The connection type is configured in the **map** command, which is described in Chapter 33, “Managing ATM Access Modules.”

The LANE Client menu is shown below. This menu contains default values for the new service you are creating.

Slot 3 Port 1 Service 2 Configuration

- 1) Description (30 chars max) : LAN Emulation Service 2
- 2) Service type { LANE Client (1),
1483 Scaling (2),
Trunking (4),
Classical IP(5),
PTOP Bridging(6),
VLAN cluster(7),
1483 Routed (14) } : LAN Emulation
- 21) LAN Type { 802.3 (1),
802.5 (2) } : 802.3
- 22) Change LANE Cfg { NO (1),
YES (2) } : NO
- 23) V2 Capable { Disable (1),
Enable (2) } : Enable
- 24) Persistent Data Direct VC
{ Disable (1),
Enable (2) } : Disable
- 3) Connection Type { PVC(1),
SVC(2) } : SVC
- 30) SEL for the ATM address : 02
- 4) LAN Emulated Group : 1
- 5) LECS Address (40-char-hex) : Use ILMI (fall back using WKA)
- 51) Use ILMI { No (1), Yes (2) } : Yes
- 6) Admin Status { disable(1),
enable(2) } : Enable
- 7) Bandwidth Group (1-8) : 1

Enter (option=value/save/cancel) :

3. To change any of the remaining fields, enter the option number, followed by the value you want to change, as described in the paragraphs below:
 - a. **21. LAN type:** The type of LAN supported by the LAE Client. Enter **21=1** for Ethernet (**802.3**), or **21=2** for Token Ring (**802.5**) clients.
 - b. **22. Change LANE Cfg:** Enter Yes (2) if you want to make LANE configuration changes. A submenu appears, allowing you to change your LANE configuration parameters. This submenu is described in *Setting LANE Client Parameters* on page 36-26.
 - c. **23. V2 Capable:** The version of LANE supported by the LE Client. Enter **23=1** for Version 1.0, or **23=2** for Version 2.0. See *LANE Version 2.0* on page 36-6 for more information on LANE Version 2.0.

- d. **24. Persistent Data Direct VC:** If you enable persistent Data Direct Virtual Connections (VCs), then this LEC will not release its Data Direct VCs if the LAN Emulation Service (LES/BUS) goes down. This ensures faster recovery and can prevent network down times.

Enter **24=1** (the default) to disable persistent Data Direct VCs or **24=2** to enable persistent Data Direct VCs.

◆ **Note** ◆

Enabling persistent Data Direct VCs may cause interoperability problems because this is an Alcatel-proprietary feature.

- e. **3. Connection Type:** Enter **3=2** for SVC. LANE client service supports only SVC. For more details, see *PVC/SVC Support* on page 36-3.
 - f. **30. SEL for the ATM address:** For SVCs, enter a hexadecimal selector (SEL) byte from **0** to **ff** for the ATM address. This value *must* be equal to the last byte of both end point addresses of the SVC. (This option will not appear unless you select SVC as the connection type in option 3.)
 - g. **4. LAN Emulated Group:** Enter the number of the group that is to be part of the LANE client service.
 - h. **5. LECS Address** and **51. Use ILMI:** When you create a new LANE Client (LEC) with the **cas** command, the default method for obtaining the LEC Server (LECS) address is to use Integrated Local Management Interface (ILMI) as the primary method and to use the Well Known Address (WKA) as the backup method. To use the WKA as the LECS address and not use ILMI, see *Using the WKA as the Primary Source for the LECS Address* on page 36-28. To manually enter the LECS address, see *Setting the LECS Manually* on page 36-29.
4. After you have made all the changes, type **save** to create your configuration. If you need to configure additional LANE Client parameters, continue to the next section.

Setting LANE Client Parameters

LANE configuration parameters are set from a submenu that you access from the **cas** or **mas** command by typing **22=2** (change LANE configuration) while the LANE Client menu is displayed. A screen similar to that shown below displays.

◆ **Note** ◆

If you have multiple ELANs configured in your ATM network, you will need to specify an ELAN name (line 16) that this service is to join. The ELAN name must match the name used in the LECS. If the names do not match, this ELAN will be joined with the default ELAN.

```

Enter (option=value/save/cancel) : 22=2
Slot 3 Port 1 Service 4 LANE Configuration Parameters
1) Proxy { NO (1), YES (2) } : YES
2) Max Frame Size { 1516 (1), 4544 (2)
                      9234 (3), 18190 (4)
                      1580 (5) } : 1516
3) Use translation options{NO (1), YES (2) } : YES (use Swch menu to set)
4) Use Fwd Delay time { NO (1), YES (2) } : NO
5) Use LE Cfg Server (LECS) { NO (1), YES (2)} : YES
6) Use Default LECS address { NO (1), YES (2)} : NO
7) Control Time-out (in seconds) : 10
8) Max Unknown Frame Count : 10
9) Max Unknown Frame Time (in seconds) : 1
10) VCC Time-out Period (in minutes) : 20
11) Max Retry Count : 2
12) Aging Time (in seconds) : 300
13) Expected LE_ARP Resp Time (in seconds) : 1
14) Flush Time-out (in seconds) : 4
15) Path Switching Delay (in seconds) : 6
16) ELAN name (32 chars max) : ELAN 1
17) Ring Number (1 - 4095) : 0
18) Bridge Number (1 - 15) : 0
19) Initial Control Timeout (in seconds) : 5
20) Control Timeout Multiplier (2-5) : 2
    
```

Enter (option=value/save/cancel) :

Modify the fields, as applicable, as described below:

1. Proxy: Always set to YES. Instead of registering MAC addresses at initialization time, the switch processes every LE_ARP sent by the LES. It looks up the forwarding table (filtering database) maintained by source learning to check whether the requested MAC address can be reached through another interface on the virtual bridge (same virtual LAN).

2. Max Frame Size: The maximum size of a data (in bytes) that the LANE client will send over the Multicast Send VCC, or receive on either the Multicast Send VCC or the Multicast Forward VCC. Enter **2=1** for 1516 bytes; **2=2** for 4544 bytes; **2=3** for 9234 bytes; **2=4** for 18190 bytes, or **2=5** for 1580 bytes.

3. Use translation options: Indicate whether you want to use the frame translations offered through the **switch** menu, which is described in Chapter 23, "Configuring LAN Switch Translations." If you choose **No**, Ethertype frames will be used by default for 802.3 ELANs.

4. Use Fwd Delay time: (Default NO) If used, it is the maximum time (in seconds) that an LE Client will maintain an entry for a non-local MAC address in its MAC table without verification.

- 5. Use LE Cfg Server:** (Default YES). If you set this parameter to NO, you will need to enter a LES Address, as it will be set to all zeroes. You can enter this address after you exit this submenu and return to the **cas** or **mas** menu.
- 6. Use Default LECS address:** (Default NO). If you set this parameter to NO, you will need to enter a LECS Address. You can enter this address after you exit this submenu and return to the **cas** or **mas** menu.
- 7. Control Time-out:** The timeout period (in seconds) used for most request/response control frame interactions. The default is 120 seconds, the minimum is 10 seconds, and the maximum is 300 seconds.
- 8. Max Unknown Frame Count:** The number of frames as specified in item 9 below.
- 9. Max Unknown Frame Time:** The length of time (in seconds) during which the LANE Client will send no more than the number of frames specified in Maximum Unknown Frame Count (see item 8 above) to the BUS for a given unicast LAN Destination. It is also the maximum time the LANE Client will wait before it must initiate an ARP frame to resolve that LAN Destination. The default is 1 second, the minimum is 1 second, and the maximum is 60 seconds.
- 10. VCC Time-out Period:** The maximum length of time (in minutes) that an LANE Client will keep a Data Direct VCC after it has not been used to transmit or receive frames. Used only for SVC Data Direct VCCs. The default is 20 minutes; there is no maximum or minimum.
- 11. Max Retry Count:** Maximum number of times an LANE Client may retry an **LE_ARP_REQUEST** for a given frame's LAN Destination. The original request does not count. The default is 1, the minimum is 0, and the maximum is 2.
- 12. Aging Time:** The maximum time (in seconds) that an LANE Client will maintain an entry in its **LE_ARP** cache. If the address is not resolved within this time period, the entry is deleted. The default is 300 seconds, the minimum is 10 seconds, and the maximum is 300 seconds.
- 13. Expected LE_ARP Resp Time:** The maximum time (in seconds) the LANE Client expects an ARP request/response cycle to take. Used for retries and verifies. The default is 1 seconds the minimum is 1 second, and the maximum is 30 seconds.
- 14. Flush Time-out:** Length of time (in seconds) an LANE Client will wait for an **LE_FLUSH_RESPONSE** after sending an **LE_FLUSH_REQUEST**, after which it will begin taking recovery action. The default is 4 seconds, the minimum is 1 second, and the maximum is 4 seconds.
- 15. Path Switching Delay:** After sending a frame to the BUS, the length of time (in seconds) the LANE Client will wait before assuming the frame has either been delivered to the client or has been discarded. The default is 6 seconds, the minimum is 1 second, and the maximum is 8 seconds.
- 16. ELAN name:** Enter a name (up to 32 characters) for the emulated LAN that the LEC either wants to join or has last joined.
- 17. Ring Number:** The ring number assigned to the Token Ring for participation in source routing. This field displays only for 802.5 Token Ring clients, not 802.3 Ethernet clients.
- 18. Bridge Number:** A unique number used to identify the source routing bridge. This field displays only for 802.5 Token Ring clients. If you are configuring an 802.3 Ethernet client, this field will not display.
- 19. Initial Control Timeout:** The timeout period (in seconds) used for timing out most request/response control frame interactions. The valid range is 1 to 10 seconds. (The default is 5 seconds.)
- 20. Control Timeout Multiplier:** The retry multiplier of the control timeout parameter (set in option 19 above). The valid range is 2 to 5. (The default is 2.)

Using the WKA as the Primary Source for the LECS Address

To use the ATM Forum-defined, Well Known Address (WKA) as the LANE Client Server (LECS) address and not use Integrated Local Management Interface (ILMI), enter

51=1

at the **cas** command prompt for the new LANE Client (LEC) you are creating or enter

31=1

at the **mas** command prompt for the existing LEC you are modifying to disable ILMI and use the WKA for the LECS address. The **cas** screen will be updated in the following way.

Slot 3 Port 1 Service 2 Configuration

- 1) Description (30 chars max) : LAN Emulation Service 2
- 2) Service type { LANE Client (1),
1483 Scaling (2),
Trunking (4),
Classical IP(5),
PTOP Bridging(6),
VLAN cluster(7),
1483 Routed (14) } : LAN Emulation
- 21) LAN Type { 802.3 (1),
802.5 (2) } : 802.3
- 22) Change LANE Cfg { NO (1),
YES (2) } : NO
- 23) V2 Capable { Disable (1),
Enable (2) } : Enable
- 24) Persistent Data Direct VC
{ Disable (1),
Enable (2) } : Disable
- 3) Connection Type { PVC(1),
SVC(2) } : SVC
- 30) SEL for the ATM address : 02
- 4) LAN Emulated Group : 1
- 5) LECS Address (40-char-hex) :
4700790000000000000000000000A03E00000100
- 51) Use ILMI { No (1), Yes (2) } : No
- 52) Use WKA { No (1), Yes (2) } : Yes
- 6) Admin Status { disable(1),
enable(2) } : Enable
- 7) Bandwidth Group (1-8) : 1

Enter (option=value/save/cancel) :

◆ Note ◆

The **mas** command menu will display the **LECS Address**, **Use ILMI**, and **Use WKA** fields as Options 3, 31, and 32, respectively.

The WKA will be displayed below Option 5 (**LECS Address**) in the **cas** menu and below Option 3 (**LECS Address**) in the **mas** menu. After you have made all of your changes, enter save at the **cas** or **mas** menu prompt.

Setting the LECS Manually

Follow the steps below to manually configure a LANE Client Server (LECS) address.

1. Enter

51=1

at the **cas** command prompt for the new LANE Client (LEC) you are creating or enter

31=1

at the **mas** command prompt for the existing LEC you are modifying to disable the use of ILMI for the LECS address. The **cas** screen will be updated in the following way.

Slot 3 Port 1 Service 2 Configuration

```

1) Description (30 chars max)      : LAN Emulation Service 2
2) Service type { LANE Client (1),
    1483 Scaling (2),
    Trunking (4),
    Classical IP(5),
    PTOP Bridging(6),
    VLAN cluster(7),
    1483 Routed (14) } : LAN Emulation
21) LAN Type { 802.3 (1),
    802.5 (2) } : 802.3
22) Change LANE Cfg { NO (1),
    YES (2) } : NO
23) V2 Capable { Disable (1),
    Enable (2) } : Enable
24) Persistent Data Direct VC
    { Disable (1),
    Enable (2) } : Disable
3) Connection Type { PVC(1),
    SVC(2) } : SVC
30) SEL for the ATM address : 02
4) LAN Emulated Group : 1
5) LECS Address (40-char-hex) :
47007900000000000000000000000000A03E00000100

51) Use ILMI { No (1), Yes (2) } : No
52) Use WKA { No (1), Yes (2) } : Yes
6) Admin Status { disable(1),
    enable(2) } : Enable
7) Bandwidth Group (1-8) : 1

Enter (option=value/save/cancel) :
```

◆ Note ◆

The **mas** command menu will display the **LECS Address**, **Use ILMI**, and **Use WKA** fields as Options 3, 31, and 32, respectively.

2. Enter

51=1

at the **cas** command prompt for the new LEC you are creating or enter

31=1

at the **mas** command prompt for the existing LEC you are modifying to disable the use of ILMI for the LECS address.

3. Enter

52=1

at the **cas** command prompt for the new LEC you are creating or enter

32=1

at the **mas** command prompt for the existing LEC you are modifying to disable the use of the WKA for the LECS address.

4. Enter **5=** at the **cas** menu prompt or **3=** at the **mas** menu prompt followed by the 40-character ATM address for the LECS address in hexadecimal. For example, to set the LECS address as **1111111111222222222233333333334444444444** from the **cas** menu prompt, enter

5=1111111111222222222233333333334444444444

5. If the ATM address you are specifying does not exist, a menu similar to the following will be displayed.

Enter (option=value/save/cancel) : 3=1111111111222222222233333333334444444444

**Address '1111111111222222222233333333334444444444':
doesn't exist, this address will be created with default values!**

Connection Address 1111111111222222222233333333334444444444 Configuration

1) Description (30 chars max)	: Address 3
2) Tx QoS Class { Unspecified }	: Unspecified
3) TX Best Effort { False (1), True (2) }	: True
4) Tx Traffic Descriptor { NoCLPNoSCR(2) }	: NoCLP NoSCR
20) Peak Cell Rate (cells/sec) for CLP=0+1	: 353208
5) Rx QoS Class { Unspecified }	: Unspecified
7) Rx Traffic Descriptor { NoCLPNoSCR(2) }	: NoCLP NoSCR
30) Peak Cell Rate (cells/sec) for CLP=0+1	: 353208
14) Tx Maximum Frame Size	: 4520
15) Rx Maximum Frame Size	: 4520

This menu is the same as the one displayed by the **cva** command, which is described in Chapter 33, "Managing ATM Access Modules."

6. After you have made all of your changes, enter save at the **cas** or **mas** menu prompt.

Creating a Trunking Service

To create a trunking service:

1. Type **cas**, followed by the slot/port for the service:
2. From the **cas** menu, enter:

2=4

This will display the Trunking menu (shown below).

Enter (option=value/save/cancel) : 2=4

Slot 3 Port 1 Service 2 Configuration

```

1) Description (30 chars max)      : Trunking Service 2
2) Service type { LANE client (1),
    1483 Scaling (2),
    Trunking (4),
    Classical IP(5),
    PTOP Bridging(6),
    VLAN cluster(7),
    1483 Routed (14) } : Trunking
3) Connection Type { PVC(1),
    SVC(2) } : PVC
30) SEL for the ATM address : 02
4) Trunked Groups : 1
5) Connection : none
6) Admin Status { disable(1),
    enable(2) } : Enable
7) Bandwidth Group (1-8) : 1

```

3. You must create at least one connection. Type **5=** followed by the connection number, which must be in the range from 1-1023. For example:

5=700

Enter (option=value/save/cancel) : 5=700

Conn VCI 700 doesn't exist, VCI 700 will be created w/default values!

4. Finish your configuration by changing the default values of any of the remaining fields, if required, as described below:
 - a. **3. Connection Type:** Enter **3=1** for PVC or **3=2** for SVC. ATM Trunking supports either connection type. For more details, see *PVC/SVC Support* on page 36-3.
 - b. **30. SEL for the ATM address:** For SVCs, enter a hexadecimal selector (SEL) byte from **0** to **ff** for the ATM address. This value *must* be equal to the last byte of both end point addresses of the SVC. (This option will *not* appear unless you select SVC as the connection type in option 3.)
 - c. **4. Trunked Groups:** Enter the number of the group that is to be part of the trunking service. The group number must match the group number on the remote switch.

◆ Note ◆

The maximum number supported in ATM trunking is 48, depending on the number of MAC addresses available. Each group will use up one (1) MAC address for the vport. Therefore, if you want to trunk 48 groups, you must have 48 MAC addresses.

- d. **5. Connection:** Enter the number of the VCI that is to be part of the trunking service. Use the command **vc** to view VCI numbers. If the VCI you name doesn't exist, it will be created.
5. After you have made all the changes, type **save** to create your configuration.

Creating a Classical IP Service

To create a Classical IP service:

1. Type **cas** followed by the slot/port for the service. It shows the default service:

```

/Services % cas 3/1

Slot 3 Port 1 Service 7 Configuration
1) Description (30 chars max)           : PTOP Bridging Service 7
2) Service type { LANE client (1),
    1483 Scaling (2)
    Trunking (4),
    Classical IP(5),
    PTOP Bridging(6),
    VLAN cluster(7),
    1483 Routed (14) }                 : PTOP Bridging
10) Encaps Type { Private (1),
    RFC1483(2) }                       : Private
3) Connection Type { PVC(1),
    SVC(2) }                           : PVC
4) PTOP Groups                         : 1
5) PTOP connection                     : none
6) Admin Status { disable(1),
    enable(2) }                         : Enable
7) Bandwidth Group (1-8)               : 1
    
```

2. Enter:

```
2=5
```

◆ Note ◆

The group to which you are assigning Classical IP must be a CIP group. If it is not, the following error message will be displayed:

Group is not CIP..

You must create a new group with ATM CIP enabled. You cannot modify an existing group to enable CIP. See the **crgrp** command in the VLAN menu in Chapter 24, “Managing Groups and Ports.”

3. Once the group is defined as a CIP group, you can now run CIP over that group. To do this, you must first assign the service you are creating to the CIP group. For example, to assign the service to Group 4, enter:

```
4=4
```

The following message will be displayed:

Warning Group is CIP, change Group (n)? :

Enter **y**.

- You can now create the CIP service. To create the service, enter:

Enter (option=value/save/cancel) : 2=5

A screen similar to the following will be displayed:

```
Slot 3 Port 1 Service 7 Configuration
1) Description (30 chars max)      : Classical IP Service 7
2) Service type { LANE client (1),
    1483 Scaling (2)
    Trunking (4),
    Classical IP(5),
    PTOP Bridging(6),
    VLAN cluster(7),
    1483 Routed (14) } : Classical IP
3) Connection Type { PVC(1),
    SVC(2) } : PVC
4) Classical IP Groups : 4
5) Neighboring connections : none
6) Admin Status { disable(1),
    enable(2) } : Enable
7) Bandwidth Group (1-8) : 1
```

Enter (option=value/save/cancel) :

- Before you can save the CIP service, you must specify a connection using a VCI. If the VCI doesn't exist, the system will create it. For example to specify the connection as VCI 201, enter:

5=201

A screen similar to the following will be displayed:

Conn VCI 201 doesn't exist, VCI 201 will be created w/ default values!

Enter (option=value/save/cancel) :

- Enter **save** to create the service.
- Enter values for the following fields as described below if any of the defaults do not match your desired configuration:
 - 3. Connection Type:** Choose PVC or SVC. Classical IP supports both. For more details, see *PVC/SVC Support* on page 36-3.

◆ Note ◆

The CIP service uses PVC as the default connection type. With PVCs you do not need an ARP server. To use SVCs, you will need to supply an ARP server address. For details on how to accomplish this, see *Modifying a Classical IP Service* on page 36-51.

- 30. SEL for the ATM address:** For SVCs, enter a hexadecimal selector (SEL) byte from **0** to **ff** for the ATM address. This value *must* be equal to the last byte of both end point addresses of the SVC. (This option will *not* appear unless you select SVC as the connection type in option 3.)
- 4. Classical IP Groups:** Enter the group number that is to be part of the Classical IP service.

Creating a PTOp Bridging Service

To create a PTOp Bridging service:

1. Type **cas**, followed by the slot/port for the service. It shows the current values for the default service. A screen similar to the following will be displayed:

```
Services % cas 3/1

Slot 3 Port 1 Service 1 Configuration
1) Description (30 chars max)      : LANE Client 1
2) Service type { LANE client (1),
    1483 Scaling (2)
    Trunking (4),
    Classical IP(5),
    PTOp Bridging(6),
    VLAN cluster(7),
    1483 Routed (14) } : LANE Client
10) Encaps Type { Private (1),
    RFC1483(2) } : Private
3) Connection Type { PVC(1),
    SVC(2) } : PVC
4) PTOp Groups: 1
5) PTOp connection: none
6) Admin Status { disable(1),
    enable(2) } : Enable
7) Bandwidth Group (1-8) : 1

Enter (option=value/save/cancel) :
```

2. To select PTOp Bridging as the service, enter:

```
2=6
```

A screen similar to the following will be displayed:

```
Slot 3 Port 1 Service 1 Configuration

1) Description (30 chars max)      : PTOp Bridging Service 1
2) Service type { LANE client (1),
    1483 Scaling (2)
    Trunking (4),
    Classical IP(5),
    PTOp Bridging(6),
    VLAN cluster(7),
    1483 Routed (14) } : PTOp Bridging
10) Encaps Type { Private (1),
    RFC1483(2) } : Private
3) Connection Type { PVC(1),
    SVC(2) } : PVC
4) PTOp Groups : 1
5) PTOp connection : none
6) Admin Status { disable(1),
    enable(2) } : Enable
7) Bandwidth Group (1-8) : 1

Enter (option=value/save/cancel) :
```

3. A PTOp bridging service must have at least one connection. To create that connection, type **5=** followed by the connection number, which is in the range from 1-1023. For example:

Enter (option=value/save/cancel) : 5=2

Conn VCI 2 doesn't exist, VCI 2 will be created w/default values!

Services % cas 3/1

4. Finish your configuration by changing the default values of any of the remaining fields, if required, as described below:
 - a. **10. Encaps Type:** Select the encapsulation type to use for frames. You can select RFC 1483 encapsulation or the same encapsulation used for Alcatel ATM trunking (i.e., private encapsulation). The 1483 encapsulation enables interoperability with other vendor switches. Enter **10=1** for private encapsulation or **10=2** for 1483 encapsulation.
 - b. **3. Connection Type:** Enter **3=1** for PVC or **3=2** for SVC. PTOp Bridging supports either type. For more details, see *PVC/SVC Support* on page 36-3.
 - c. **30. SEL for the ATM address:** For SVCs, enter a hexadecimal selector (SEL) byte from **0** to **ff** for the ATM address. This value *must* be equal to the last byte of both end point addresses of the SVC. (This option will *not* appear unless you select SVC as the connection type in option 3.)
 - d. **4. PTOp Groups:** Enter the number of the Group that is to be part of the PTOp service.
 - e. **5. PTOp Connection:** Enter the number of the VCI that is to be part of the PTOp service. Use the **vvc** command first to determine what VCI numbers have been assigned. If the VCI you name doesn't exist, it will be created.
5. After you have made all the changes, type **save** to create your configuration.

Enter (option=value/save/cancel) : save

Creating service, please wait...

Enabling service...

/Services %

Creating a VLAN Cluster Service

To create a VLAN cluster service:

1. Type **cas**, followed by the slot/port for the service. It shows the default service (LANE Client):

```
Services % cas 3/1

Slot 3 Port 1 Service 1 Configuration
1) Description (30 chars max) : LANE Client 1
2) Service type { LANE client (1),
                  1483 Scaling (2)
                  Trunking (4),
                  Classical IP(5),
                  PTOp Bridging(6),
                  VLAN cluster(7),
                  1483 Routed (14) } : LANE Client
10) Encaps Type { Private (1),
                 RFC1483(2) } : Private
3) Connection Type { PVC(1),
                   SVC(2) } : PVC
4) PTOp Groups: 1
5) PTOp connection: none
6) Admin Status { disable(1),
                 enable(2) } : Enable
7) Bandwidth Group (1-8) : 1
```

2. Enter:

```
2=7
```

3. This will display the VLAN Cluster menu, as shown below.

```
Slot 3 Port 1 Service 1 Configuration
1) Description (30 chars max) : VLAN cluster Service 1
2) Service type { LANE client (1),
                  1483 Scaling (2)
                  Trunking (4),
                  Classical IP(5),
                  PTOp Bridging(6),
                  VLAN cluster(7),
                  1483 Routed (14) } : VLAN cluster
21) Number of others in cluster : 0
22) Change cluster information
    { NO (1), YES (2) } : NO
23) Encapsulation format
    { 1483 (1), Private (2) } : 2
3) Connection Type { PVC(1),
                   SVC(2) } : PVC
4) Trunked Groups : 1
5) Broadcast Out VC : 0
6) Admin Status { disable(1),
                 enable(2) } : Enable
7) Bandwidth Group (1-8) : 1
Enter (option=value/save/cancel) :
```

4. Finish your configuration by changing the default values of any of the remaining fields, if required, as described below:

- a. **21. Number of others in cluster:** The number of switches included in this VLAN cluster. You may include up to 32 switches in a single cluster. This field must be greater than zero (0).

◆ **Note** ◆

Only 64 neighbors are supported in a VLAN cluster service (i.e., X-LANE) per ATM access port on OmniSwitches with an MPM-II or MPM-1G.

- b. **22. Change cluster info:** Enter Yes (2) if you want to configure Data Direct and Broadcast virtual circuits. A submenu appears, allowing you to configure these virtual circuits. This submenu is described in *Modifying VLAN Cluster Parameters* on page 36-56.
- c. **23. Encapsulation format:** Select the encapsulation type to use for frames. You can select RFC 1483 encapsulation or the same encapsulation used for Alcatel's proprietary (i.e., private) ATM trunking. The 1483 encapsulation enables interoperability with other vendor switches, such as the Newbridge 36150 and 36170.

◆ **Note** ◆

If you select 1483 encapsulation, you can only multiplex a single group across the switches in a cluster. Alcatel's proprietary trunking encapsulation allows you to multiplex multiple groups across switches in this cluster service.

- d. **3. Connection Type:** Enter **3=1** for PVC. VLAN Clusters supports only PVC. For more details, see *PVC/SVC Support* on page 36-3.
 - e. **4. Trunked/Bridged Groups:** Enter the number of the Group that is to be part of this VLAN cluster service. If you selected 1483 encapsulation in Line 23, this line will read **Bridged Group** and you can specify only one Group. If you select the Alcatel trunking encapsulation in Line 23, this line will read **Trunked Groups** and you can specify multiple Groups.
 - f. **5. Broadcast Out VC:** Enter the number of the VCI where broadcast frames will be sent. Use the command **vc** to see what VCI numbers have already been assigned. If the VCI you name doesn't exist, it will be created.
5. After you have made all the changes, type **save** to create your configuration.

Enter (option=value/save/cancel) : save

Creating service, please wait...

Enabling service...
/Services %

Creating a 1483 Scaling Service

Follow the steps below to create a 1483 scaling service.

◆ Important Note ◆

In the current release, 1483 scaling services are only supported on the FCSM II module and Omni Switch/Router ASX modules.

1. At the system prompt, enter **cas** followed by the slot/port for the 1483 scaling service. For example, to assign a 1483 scaling service on Port 1 in Slot 2, enter

cas 2/1

at the system prompt. A screen similar to the following will be displayed.

```
Slot 2 Port 1 Service 2 Configuration
1) Description (30 chars max)      : PTOp Bridging Service 2
2) Service type { LANE client (1),
                  1483 Scaling (2)
                  Trunking (4),
                  Classical IP(5),
                  PTOp Bridging(6),
                  VLAN cluster(7),
                  1483 Routed (14) } : PTOp Bridging
10) Encaps Type { Private (1),
                 RFC1483(2) }      : Private
3) Connection Type { PVC(1),
                   SVC(2) }        : PVC
4) PTOp Group                               : 1
5) PTOp Connection                           : none
6) Admin Status { disable(1),
                 enable(2) }         : Enable
7) Bandwidth Group (1-8)                   : 1

Enter (option=value/save/cancel) :
```

◆ Note ◆

You *must* create the group(s) before you can create a 1483 scaling service. See Chapter 24, “Managing Groups and Ports,” for more information on creating groups and see Chapter 20, “802.1Q,” for more information on 802.1Q groups.

2. The default service for a port is a PTOp bridging service. To create a 1483 scaling service, enter

2=2

at the prompt. A screen similar to the following will be displayed.

```

Slot 2 Port 1 Service 2 Configuration
1) Description (30 chars max)      : 1483 Scaling Bridge Service 2
2) Service type { LANE client (1),
    1483 Scaling (2),
    Trunking (4),
    Classical IP(5),
    PTOp Bridging(6),
    VLAN cluster(7),
    1483 Routed (14) } : 1483 Scaling
21) Number of entries saved      : 0
22) Change mapping information
    { NO (1), YES (2) }          : NO
3) Connection Type { PVC(1),
    SVC(2) }                     : PVC
4) Primary Group                 : 1
5) Primary Connection            : none
6) Admin Status { disable(1),
    enable(2) }                  : Enable
7) Bandwidth Group (1-8)        : 1

Enter (option=value/save/cancel) :

```

◆ Note ◆

You can create only one 1483 scaling service per physical port.

3. Finish your configuration by changing the default values of any of the remaining fields, if required, as described below:
 - a. **21) Number of entries saved.** This read-only field displays the number of mapping entries (which list the group and the VCI it is mapped to) for this 1483 scaling service. (You *cannot* modify this field.) Mapping entries can be displayed and modified by Option 22, which is described below.
 - b. **22) Change mapping information.** Enter **2** (yes) to enter a submenu for displaying and configuring 1483 mapping parameters. This submenu is described in *Editing and Displaying 1483 Mapping Parameters* on page 36-43.

◆ Note ◆

You *must* set the Virtual Channel Identifier (VCI) with Option 5 (described on the following page) you can enter the 1483 mapping submenu.

- c. **4) Primary Group.** Enter the number of the primary group ID.
- d. **5) Primary Connection.** Enter the number for the primary VCI.

◆ Note ◆

If you configure one or more 1483 scaling services on a FCSM II or ASX module, you will be able to configure one (1) PTOp service on this module but no more additional ATM services of any kind.

Creating a Service

4. After you have made all the changes, type **save** to create your configuration, or **cancel** to discard your changes and exit. If a 1483 scaling service was successfully created, the following messages will be displayed

Creating service, please wait...

Enabling service...

Editing and Displaying 1483 Mapping Parameters

Mapping parameters for 1483 scaling services are displayed and set from a submenu that you access from the **cas** or **mas** command. (See *Modifying a 1483 Scaling Service* on page 36-57 for more information on using the **mas** command on a 1483 scaling service.) While the 1483 scaling services menu is displayed, enter

22=2

at the prompt. A screen similar to the following will be displayed.

Slot 3 port 1 Group ID to Virtual Circuit Mapping

Total number of mapping configured : 1

- 1) Add Mapping Entry.
- 2) Add Mapping Entry by Range.
- 3) Delete Mapping Entry.
- 4) Delete Mapping Entry by Range.
- 5) View All Existing Mapping Entries.
- 6) View Existing Entry by Group ID.
- 7) View Existing Entry by virtual circuit.
- 8) Exit.

Enter option :

Enter one of the eight (8) options described below. You can display and edit mapping entries, which list the group and the Virtual Circuit Identifier (VCI) it is mapped to. Except for Option 8 (Exit), all options will display a concluding message, similar to the following, indicating how many mapping entries have been configured.

Total number of mapping configured : 2

◆ Note ◆

If you are logged into the UI and you do not have the write privilege, you can display 1483 scaling mapping entries with the **vgptovc** command, which is described in *Viewing 1483 Scaling Service Parameters* on page 36-72.

1) Add Mapping Entry

Follow the steps below to add a single mapping entry.

- a. Enter **1** at the prompt. The following prompt will be displayed.

Enter Group number :

- b. Enter the group to be mapped to. The following prompt will be displayed.

Enter Virtual Circuit (1 - 1024) :

- c. Enter the Virtual Circuit Identifier (VCI) to be mapped to the group you selected in Step b. If the mapping entry was successfully created, messages similar to the following will be displayed.

Group 1, vci 101 added to the beginning of the mapping table

Slot 2 port 1 Group ID to Virtual Circuit Mapping

Total number of mapping configured : 2

2) Add Mapping Entry by Range

Follow the steps below to add a range of mapping entries.

- a. Enter **2** at the prompt. The following prompt will be displayed.
Enter Beginning Group number :
- b. Enter the first group to be mapped to. The following prompt will be displayed.
Enter Ending Group number :
- c. Enter the ending group to be mapped to. The following prompt will be displayed.
Enter Beginning Virtual Circuit(1 - 1024) :
- d. Enter the beginning Virtual Circuit Identifier (VCI) to be mapped to the group you selected in Step b. The following prompt will be displayed.
Enter Beginning Virtual Circuit(1 - 1024) :
- e. Enter the ending VCI to be mapped to the group you selected in Step 2. If the mapping entry was successfully created, messages similar to the following will be displayed.

Slot 2 port 1 Group ID to Virtual Circuit Mapping
Total number of mapping configured : 2

3) Delete Mapping Entry

Follow the steps below to delete a single mapping entry.

- a. Enter **3** at the prompt. The following prompt will be displayed.
Enter Group number :
- b. Enter the group to be deleted from the 1483 scaling service. If the group was successfully deleted from the 1483 scaling service, messages similar to the following will be displayed.

Group 1 deleted from the head of the mapping table
Slot 2 port 1 Group ID to Virtual Circuit Mapping
Total number of mapping configured : 1

4) Delete Mapping Entry by Range

Follow the steps below to delete a range of mapping entries.

- a. Enter **4** at the prompt. The following prompt will be displayed.
Enter Beginning Group number :
- b. Enter the first group to be deleted. The following prompt will be displayed.
Enter Ending Group number :

- c. Enter the ending group to be deleted. If the groups were successfully deleted from the 1483 scaling service, messages similar to the following will be displayed.

Slot 2 port 1 Group ID to Virtual Circuit Mapping

Total number of mapping configured : 1

◆ Note ◆

Options 5 (**View All Existing Mapping Entries**) through 7 (**View Existing Entry by virtual circuit**) provide a simple display of mapping entries for 1483 scaling services. Only the group and the VCI associated with it are displayed. To display a more complete set of statistics, use the **vgptovc** command, which is described in *Viewing 1483 Scaling Service Parameters* on page 36-72.

5) View all Existing Mapping Entries

To display all mapping entries, enter

5

at the prompt. A screen similar to the following will be displayed.

Slot 2 port 1 Group ID to Virtual Circuit Mapping

Group ID to Virtual Circuit Mapping table:

Group ID	Virtual Circuit
1	55
2	56

Slot 2 port 1 Group ID to Virtual Circuit Mapping

Total number of mapping configured : 3

6) View Existing Mapping Entries by Group ID

Follow the steps below to display mapping entries by group ID.

- a. Enter **6** at the prompt. The following prompt will be displayed.

Enter Group number :

- b. Enter the group to be displayed in this 1483 scaling service. A screen similar to the following will be displayed.

Slot 2 port 1 Group ID to Virtual Circuit Mapping

Group ID	Virtual Circuit
2	56

Slot 2 port 1 Group ID to Virtual Circuit Mapping

Total number of mapping configured : 3

7) View Existing Entry by virtual circuit

Follow the steps below to display mapping entries by Virtual Circuit Identifier (VCI).

- a. Enter **7** at the prompt. The following prompt will be displayed.

Enter Virtual Circuit Identifier :

- b. Enter the VCI of the virtual circuit to be displayed in this 1483 scaling service. A screen similar to the following will be displayed.

Slot 2 port 1 Group ID to Virtual Circuit Mapping

<u>Group ID</u>	<u>Virtual Circuit</u>
2	56

Slot 2 port 1 Group ID to Virtual Circuit Mapping

Total number of mapping configured : 3

8) Exit

Enter **8** to exit this submenu and return to the main 1483 scaling menu.

Creating a 1483 Routed Format Service

To create a 1483 routed format service, follow the steps below:

◆ Important Note ◆

You *must* configure 1483 routed format services groups at both the source and destination end points. In addition, both groups *must* both be in the same subnet. See Chapter 24, “Managing Groups and Ports,” for more information on creating 1483 routed format services groups.

1. Type **cas** followed by the slot/port for the service. The default service will be displayed:

```

/Services % cas 3/1

Slot 3 Port 1 Service 7 Configuration
1) Description (30 chars max)           : PTOp Bridging Service 7
2) Service type { LANE client (1),
    1483 Scaling (2),
    Trunking (4),
    Classical IP(5),
    PTOp Bridging(6),
    VLAN cluster(7),
    1483 Routed (14) }                 : PTOp Bridging
10) Encaps Type { Private (1),
    RFC1483(2) }                       : Private
3) Connection Type { PVC(1),
    SVC(2) }                           : PVC
4) PTOp Groups                         : 1
5) PTOp connection                     : none
6) Admin Status { disable(1),
    enable(2) }                         : Enable
7) Bandwidth Group (1-8)               : 1

```

2. Enter:

```
2=14
```

◆ Note ◆

The group to which you are assigning 1483 routed service must be a 1483 routed group. If it is not, the following error message will be displayed:

```
Warning Group is 1483 Routed, change group (n)? :
```

You must create a new group with 1483 routed format enabled. You cannot modify an existing group to enable 1483 routed service. See the **crgp** command in the VLAN menu in Chapter 24, “Managing Groups and Ports.”

3. Once the group is defined as a 1483 routed group, you can now run 1483 routed service over that group. To do this, you must first assign the service you are creating to the 1483 routed group. For example, to assign the service to Group 7, enter:

```
4=7
```

The following message will be displayed:

Warning Group is 1483 Routed, change group (n)? :

Enter **y**.

4. You can now create the 1483 routed service. To create the service, enter:

Enter (option=value/save/cancel) : 2=14

A screen similar to the following will be displayed:

```
Slot 3 Port 1 Service 7 Configuration
1) Description (30 chars max)      : 1483 Routed Service 3
2) Service type { LANE client (1),
    1483 Scaling (2),
    Trunking (4),
    Classical IP(5),
    PTOP Bridging(6),
    VLAN cluster(7),
    1483 Routed (14) } : 1483 Routed
4) 1483 routed Groups              : 7
   41) Remote IP address           : 0.0.0.0
   42) Remote IP Subnet Mask       : 0.0.0.0
5) PVC connection                  : none
6) Admin Status { disable(1),
    enable(2) }                    : Enable
7) Bandwidth Group (1-8)          : 1
```

Enter (option=value/save/cancel) :

5. Before you can save the 1483 routed service, you must specify a connection using a VCI. If the VCI doesn't exist, the system will create it. For example, to specify the connection as VCI 201, enter:

5=201

A screen similar to the following will be displayed:

Conn VPI/VCI 0/201 doesn't exist, VPI/VCI 0/201 will be created w/ default values!

Enter (option=value/save/cancel) :

6. Enter values for the following fields as described below if any of the defaults do not match your desired configuration:
 - a. **41. Remote IP address:** Enter **41=** followed by the IP address of the remote node in dotted decimal format. The remote IP address is the IP address of the 1483 routed format group at the other (i.e, destination) end. For example, to set the remote IP address to **10.126.4.2**, enter
41=10.126.4.2
at the **cas** command prompt.
 - b. **42. Remote IP Subnet Mask:** Enter **42=** followed by the subnet mask for the remote node's IP address. For example, to set the subnet mask to **255.255.255.255**, enter
42=255.255.255.255
at the **cas** command prompt.
7. After you have made all the changes, type **save** to create the service.

Modifying a Service

To modify a service, type **mas**, followed by the slot/port and service number for the service. (The **vas** command shows the service numbers.) It shows the current values. Enter the number of the value you want to change followed by an equal sign and the new value.

The following lists the subsection for each service type:

- To modify a LANE client service, see the subsection below.
- To modify a Trunking service, see *Modifying a Trunking Service* on page 36-50.
- To modify a Classical IP (CIP), see *Modifying a Classical IP Service* on page 36-51. To add static ARP entries for a CIP service, see *Adding Static ARP Entries for CIP* on page 36-53.
- To modify a PTOp service, see *Modifying a PTOp Bridging Service* on page 36-54.
- To modify a VLAN cluster service, see *Modifying a VLAN Cluster Service* on page 36-55.
- To Modify a 1483 scaling service, see *Modifying a 1483 Scaling Service* on page 36-57.
- To modify a 1483 routed format service, see *Modifying a 1483 Routed Format Service* on page 36-59.

Modifying a LANE Client Service

To modify a LANE client service, type **mas** followed by the slot/port and service number for the service. It shows the current values.

```
Services % mas 3/1 4
```

```
Slot 3 Port 1 Service 4 Configuration
```

```

1) Description (30 chars max)      : LANE Client Service 4
2) LAN Emulated Groups
  21) LAN Type { 802.3 (1),
              802.5 (2) }          : 802.3
  22) Change LANE Cfg { NO (1),
                    YES (2) }      : NO
  23) V2 Capable { Disable (1),
                  Enable (2) }      : Enable
  24) Persistent Data Direct VC
      { Disable (1),
        Enable (2) }                : Disable
3) LECS Address (40-char-hex)      : Use ILMI (fall back using WKA)
  31) Use ILMI { No (1), Yes (2) } : Yes
4) Admin Status { disable(1),
                 enable(2) }        : Enable
6) Connection Type { PVC(1),
                   SVC(2) }         : SVC
  60) SEL for the ATM address       : 04
7) Bandwidth Group (1-8)           : 1

```

```
Enter (option=value/save/cancel) :
```

Enter the number of the value you want to change followed by an equal sign and the new value. For example, to change the ATM address selector from 04 to 05, enter:

```
60=05
```

at the **mas** command prompt. After you have made all the changes, type **save** to update your configuration.

Modifying a Trunking Service

To modify an ATM trunking service, type **mas** followed by the slot/port and service number for the service. It shows the current values.

```
Services % mas 3/1 2
```

Slot 3 Port 1 Service 2 Configuration

```
1) Description (30 chars max) : Trunking Service 2
2) Trunked Groups             : 1
3) Connection                 : 700
4) Admin Status { disable(1),
                    enable(2) } : Enable
6) Connection Type { PVC(1),
                    SVC(2) }   : PVC
7) Bandwidth Group (1-8)     : 1
```

Enter the number of the value you want to change followed by an equal sign and the new value. For example to change the Connection Type to SVC, type:

```
6=2
```

```
Enter (option=value/save/cancel) : 6=2
```

Slot 3 Port 1 Service 2 Configuration

```
1) Description (30 chars max) : Trunking Service 2
2) Trunked Groups             : 1
3) Address (40-char-hex)     : none
4) Admin Status { disable(1),
                    enable(2) } : Enable
6) Connection Type { PVC(1),
                    SVC(2) }   : SVC
60) SEL for the ATM address   : 02
7) Bandwidth Group (1-8)     : 1
```

```
Enter (option=value/save/cancel) :
```

After you have made all the changes, type **save** to update your configuration.

Modifying a Classical IP Service

To modify a Classical IP service, type **mas**, followed by the slot/port and service number for the service. It shows the current values. Enter the number of the value you want to change followed by an equal sign and the new value. For example, to change the connection type to SVC, type:

6=2

Enter (option=value/save/cancel) : 6=2

```

Slot 3 Port 1 Service 7 Configuration
1) Description (30 chars max)      : Classical IP Service 7
2) Classical IP Groups             : 4
3) Neighboring addresses (40 chr-hex): none
4) Admin Status { disable(1),
   enable(2) }                     : Enable
6) Connection Type { PVC(1),
   SVC(2) }                         : SVC
60) SEL for the ATM address        : 07

7) Bandwidth Group (1-8)          : 1
    
```

Note that when you create an SVC connection, there are several other parameters you can change. The parameters below are the same as those used in the **cva** command, which can be found in the ATM menu. The **cva** command is described in Chapter 33, "Managing ATM Access Modules." The example below shows the service being modified with a new neighboring address:

Enter (option=value/save/cancel) : 3=111111111122222222223333333333334444444444

Address '111111111122222222223333333333334444444444':
doesn't exist, this address will be created with default values!

Connection Address 111111111122222222223333333333334444444444 Configuration

```

1) Description (30 chars max)      : Address 3
2) Tx QoS Class { Unspecified }    : Unspecified
3) TX Best Effort { False (1), True (2) } : True
4) Tx Traffic Descriptor { NoCLPNoSCR(2) } : NoCLP NoSCR
   20) Peak Cell Rate (cells/sec) for CLP=0+1 : 353208
5) Rx QoS Class { Unspecified }    : Unspecified
6) RX Best Effort { False (1), True (2) } : True
7) Rx Traffic Descriptor { NoCLPNoSCR(2) } : NoCLP NoSCR
   30) Peak Cell Rate (cells/sec) for CLP=0+1 : 353208
14) Tx Maximum Frame Size          : 4520
15) Rx Maximum Frame Size          : 4520
    
```

Modifying a Service

After you have made all changes, type **save** to update your configuration.

```
Enter (option=value/save/cancel) : save
Creating address connection, please wait...
```

Slot 3 Port 1 Service 7 Configuration

```
1) Description (30 chars max)      : Classical IP Service 7
2) Classical IP Groups             : 4
3) Neighboring addresses (40 chr-hex) : 1111111111222222222233333333334444444444
4) Admin Status { disable(1),
                    enable(2) }    : Enable
6) Connection Type { PVC(1),
                    SVC(2) }       : SVC
60) SEL for the ATM address        : 07
7) Bandwidth Group (1-8)           : 1
```

```
Enter (option=value/save/cancel) : save
Modifying service, please wait...
```

```
Resetting service, please wait...
Enabling service...
/Services %
```

Adding Static ARP Entries for CIP

To add static entries to the CIP ARP table, use the **aat** command (found in the ATM menu):

1. Enter **aat**, followed by the slot number, a slash (/), the port number and the CIP service number where you want to create this static entry. For example, to add an ARP entry for service number 4 on the first port in slot 3, you would enter:

```
aat 3/1 4
```

Make sure the service number you indicate is an ATM CIP service. You cannot use the **aat** command with any service type but CIP. See *Modifying a Classical IP Service* on page 36-51 for more information on creating a CIP service.

2. The following prompt displays:

```
Enter <IP addr> <vpi> <vci> :
```

Enter the IP address, the Virtual Path Identifier (VPI), and the Virtual Circuit Identifier (VCI) for the CIP ARP entry that you want to add. Press **<Enter>** when complete.

3. A message displays indicating the CIP ARP entry was added to the table:

```
Static entry successfully added to the CIP ARP table.
```

The screen again prompts you to enter more ARP entries.

```
Enter <IP addr> <vpi> <vci> :
```

4. Continue entering ARP entries until you are complete. Press **<Enter>** at the **Enter <IP addr> <vpi> <vci>** : prompt when you are done adding entries, and you exit from the **aat** command.

Modifying a PTOp Bridging Service

To modify a PTOp Bridging service:

1. Type **mas** followed by the slot/port and service number for the service. The current values are displayed.

```
/Services % mas 3/1 1
```

Slot 3 Port 1 Service 1 Configuration

```
1) Description (30 chars max) : PTOp Bridging Service 1
2) PTOp Groups                : 1
3) PTOp connection            : 2
4) Admin Status { disable(1),
                       enable(2) } : Enable
5) Encaps Type { Private (1),
                 RFC1483(2) }     : Private
6) Connection Type { PVC(1),
                    SVC(2) }     : PVC
7) Bandwidth Group (1-8)      : 1
```

```
Enter (option=value/save/cancel) : 5=2
```

2. Enter the number of the value you want to change followed by an equal sign and the new value. For example to change the encapsulation type to RFC1483, type:

```
5=2
```

The modified configuration is now displayed.

Slot 3 Port 1 Service 1 Configuration

```
1) Description (30 chars max) : PTOp Bridging Service 1
2) PTOp Groups                : 1
3) PTOp connection            : 2
4) Admin Status { disable(1),
                       enable(2) } : Enable
5) Encaps Type { Private (1),
                 RFC1483(2) }     : RFC 1483
6) Connection Type { PVC(1),
                    SVC(2) }     : PVC
7) Bandwidth Group (1-8)      : 1
```

3. After you have made all the changes, type **save** to update your configuration.

```
Enter (option=value/save/cancel) : save
Modifying service, please wait...
```

```
Resetting service, please wait...
Enabling service...
```

```
/Services %
```

Modifying a VLAN Cluster Service

To modify a VLAN Cluster service:

1. Type **mas**, followed by the slot/port and service number for the service. The current values are displayed.

```

Services % mas 3/1
Slot 3 Port 1 Service 1 Configuration

1) Description (30 chars max)      : VLAN cluster Service 1
2) Trunked Groups                  : 1
   21) Number of others in cluster : 2
   22) Change cluster information
       { NO (1), YES (2) }         : NO
   23) Encapsulation format
       { 1483 (1), Private (2) }   : 2
3) Broadcast Out VC                : 0
4) Admin Status { disable(1),
                  enable(2) }      : Enable
6) Connection Type { PVC(1),
                    SVC(2) }       : PVC
7) Bandwidth Group (1-8)           : 1
    
```

2. Enter the number of the value you want to change followed by an equal sign and the new value. For example to change the description, type:

```
1=Cluster VLAN 1
```

A screen similar to the following will be displayed:

```

Slot 3 Port 1 Service 1 Configuration

1) Description (30 chars max)      : Cluster VLAN 1
2) Trunked Groups                  : 1
   21) Number of others in cluster : 2
   22) Change cluster information
       { NO (1), YES (2) }         : NO
   23) Encapsulation format
       { 1483 (1), Private (2) }   : 2
3) Broadcast Out VC: 0
4) Admin Status { disable(1),
                  enable(2) }      : Enable
6) Connection Type { PVC(1),
                    SVC(2) }       : PVC
7) Bandwidth Group (1-8)           : 1

Enter (option=value/save/cancel) : save
    
```

3. After you have made all the changes, type **save** to update your configuration.

Modifying VLAN Cluster Parameters

Before you modify VLAN Cluster parameters, make sure you have created at least one VLAN Cluster. To modify VLAN Cluster parameters:

1. Access the VLAN Cluster Service submenu by typing **22=2** from either the **cas** or **mas** menu. A screen similar to that shown below is displayed.

Slot 3 Port 1 Service 5 VLAN Cluster Configuration

Member Index	Description (a)	Data-Direct VCC (b)	Broadcast IN VC (c)
1	CLUSTERNUMBER1	201	202
2	CLUSTERNUMBER2	299	301

The following fields are fields that you can configure:

- a. **Description:** A 30 character description.
 - b. **Data-Direct VCC:** Enter the circuit number to be used as a point-to-point virtual circuit for a known unicast destination.
 - c. **Broadcast IN VC:** Enter the circuit number to be used as a one-way (in) broadcast virtual circuit.
2. To change one of parameters, type the index number of the VLAN Cluster, followed by **a**, **b**, or **c**, depending upon which value you want to change. For example, to change the description for index 1, type:

1a=CLUSTER1

The updated configuration will be displayed, as shown below:

Slot 3 Port 1 Service 5 VLAN Cluster Configuration

Member Index	Description (a)	Data-Direct VCC (b)	Broadcast IN VC (c)
1	CLUSTER1	201	202
2	CLUSTERNUMBER2	299	601

save|cancel|? : save

3. After you have made all the changes, type **save** to update your configuration.

Modifying a 1483 Scaling Service

To modify a 1483 scaling service, follow the steps bellow.

1. Type **mas** followed by the slot/port and service number of the service. A screen similar to the following will be displayed.

Slot 2 Port 1 Service 2 Configuration

```

1) Description (30 chars max)      : 1483 Scaling Bridge Service 2
2) Primary Group                   : 1
   21) Number of entries saved      : 1
   22) Change mapping information
       { NO (1), YES (2) }         : NO
3) Primary connection              : 2
4) Admin Status { disable(1),
   enable(2) }                     : Enable
6) Connection Type { PVC(1),
   SVC(2) }                         : PVC
7) Bandwidth Group (1-8)           : 1

```

Enter (option=value/save/cancel) :

2. Enter the number of the value you want to change followed by an equal sign and the new value. For example to change the bandwidth group to Group No. 2, enter

7=2

A screen similar to the following will be displayed:

Slot 2 Port 1 Service 2 Configuration

```

1) Description (30 chars max)      : 1483 Scaling Bridge Service 2
2) Primary Group                   : 1
   21) Number of entries saved      : 1
   22) Change mapping information
       { NO (1), YES (2) }         : NO
3) Primary connection              : 2
4) Admin Status { disable(1),
   enable(2) }                     : Enable
6) Connection Type { PVC(1),
   SVC(2) }                         : PVC
7) Bandwidth Group (1-8)           : 2

```

Enter (option=value/save/cancel) :

3. To change the mapping characteristics, enter

22=2

at the prompt. A screen similar to the following will be displayed:

Slot 2 port 1 Group ID to Virtual Circuit Mapping

Total number of mapping configured : 1

- 1) Add Mapping Entry.
- 2) Add Mapping Entry by Range.
- 3) Delete Mapping Entry.
- 4) Delete Mapping Entry by Range.
- 5) View All Existing Mapping Entries.
- 6) View Existing Entry by Group ID.
- 7) View Existing Entry by virtual circuit.
- 8) Exit.

Enter option :

Enter one of the eight (8) options, which are described in *Editing and Displaying 1483 Mapping Parameters* on page 36-43.

4. After you have made all the changes, enter **save** to update your configuration or **cancel** to discard your changes and exit the **mas** command.

Modifying a 1483 Routed Format Service

To modify a 1483 routed format service, follow the steps below:

1. Type **mas** followed by the slot/port and service number for the service. The current values are displayed.

```
/Services % mas 5/1 3
```

Slot 5 Port 1 Service 3 Configuration

```
1) Description (30 chars max) : 1483 Routed Service 3
2) 1483 routed Groups       : 7
   41) Remote IP address     : 10.126.4.2
   42) Remote IP Subnet Mask : 255.255.255.255
3) PVC connection           : 0/201
4) Admin Status { disable(1),
   enable(2) }               : Enable

7) Bandwidth Group (1-8)    : 1
```

```
Enter (option=value/save/cancel) :
```

2. Enter the number of the value you want to change followed by an equal sign and the new value. For example to change the remote IP address to **10.126.4.16**, enter:

```
41=10.126.4.16
```

at the **mas** command prompt. The modified configuration is now displayed.

Slot 5 Port 1 Service 3 Configuration

```
1) Description (30 chars max) : 1483 Routed Service 3
2) 1483 routed Groups       : 7
   41) Remote IP address     : 10.126.4.16
   42) Remote IP Subnet Mask : 255.255.255.255
3) PVC connection           : 0/201
4) Admin Status { disable(1),
   enable(2) }               : Enable

7) Bandwidth Group (1-8)    : 1
```

```
Enter (option=value/save/cancel) :
```

3. After you have made all the changes, type **save** to update your configuration.

```
Enter (option=value/save/cancel) : save
Modifying service, please wait...
```

```
Enabling service...
/Services %
```

Deleting a Service

To delete a service, type **das** followed by the slot/port and service number for the service.

das 3/1 4

A screen similar to that shown below is displayed.

/Services % das 3/1 4

ATM Services

Slot	Serv Port	Service Num	Service Description	Type
====	====	====	=====	=====
3	1	1	PTOP Bridging Service 1	PTOP Priv
3	1	2	Trunking Service 2	Trunking
3	1	3	LANE Client Service 3	802.3 LEC
3	1	4	LANE Client Service 4	802.5 LEC

ATM Services

Slot	Port	Serv Num	VC Typ	Oper Status	SEL	Groups	Conn VPI/VCI (Addr Index)
====	====	====	====	=====	====	=====	=====
3	1	1	PVC	Disabled	N/A	1	0/100
3	1	2	PVC	Disabled	N/A	1	0/500
3	1	3	SVC	Initial	03	1	
3	1	4	SVC	Initial	04	1	

Remove ATM Slot 3 Port 1 Service 4 (n)? : y

Type **y**, then press **<Enter>** to delete the service, or type **n** or **<Enter>** to keep the service. If you choose to delete the service, the following messages will be displayed.

Removing ATM Slot 3 Port 1 Service 4, please wait...

ATM Slot 3 Port 1 Service 4 removed

/Services %

Deleting Static ATM ARP Entries for CIP

To delete static entries from the CIP ARP table using the **dat** command:

1. Enter **dat**, followed by the slot number, a slash (/), the port number and the CIP service number where you want to delete this static entry. For example, to delete an ARP entry for service number 4 on the first port in slot 3, you would enter:

```
dat 3/1 4
```

Make sure the service number you indicate is an ATM CIP service. You cannot use the **dat** command with any service type but CIP. See *Modifying a Classical IP Service* on page 36-51 for more information on CIP services.

2. The following prompt displays:

```
Enter <IP addr> <vpi> <vci> :
```

Enter the IP address, the Virtual Path Identifier (VPI), and the Virtual Circuit Identifier (VCI) for the CIP ARP entry that you want to delete. Press **<Enter>** when complete.

3. A message displays indicating the CIP ARP entry was deleted from the table:

```
Static entry successfully deleted from the CIP ARP table.
```

The previous prompt re-displays for you to enter more ARP entries.

```
Enter <IP addr> <vpi> <vci> :
```

Continue entering ARP entries until you are completed. Press **<Enter>** at the **Enter <IP addr> <vpi> <vci> :** prompt when you have finished deleting entries and you will exit from the **dat** command.

Viewing ATM Access Port Services

Before configuring a service, you can view the current ATM service configurations to determine whether you need to add a new service or modify an existing one. To view all ATM services on a switch, type **vas**. If you include the slot/port number, the switch displays only the services related to that port. The display includes the service number. You will need the service number to modify or delete a service.

```
/Services % vas 3/1
```

ATM Services					
Slot	Port	Serv Num	Service Description	Service Type	
====	====	====	=====	=====	
3	1	1	PTOP Bridging Service 1	PTOP Priv	
3	1	2	Trunking Service 2	Trunking	
3	1	3	LAN Emulation Service 3	802.3 LEC	
3	1	4	LAN Emulation Service 4	802.5 LEC	

ATM Services								
Slot	Port	Serv Num	VC Typ	Oper Status	SEL	Groups	Conn VPI/VCI (Addrs Index)	
====	====	====	====	=====	====	=====	=====	
3	1	1	PVC	Disabled	N/A	1	0/100	
3	1	2	PVC	Disabled	N/A	1	0/500	
3	1	3	SVC	Initial	03	1		
3	1	4	SVC	Initial	04	1		

The fields displayed by the **vas** command are described below.

Slot. The slot number of the ATM service.

Port. The port number of the ATM service.

Serv Num. The ATM service number.

Service Description. A text description of the service. This can be entered with the **cas** command or modified with the **mas** command.

Service Type. The Service Type column for Ethernet LECs reads **802.3 LEC**. For Token Ring LECs, this column reads **802.5 LEC**. All ports on a newly-installed switch will automatically configure as 802.3 LECs.

VC Type. The virtual circuit type, which can be PVC (Permanent Virtual Circuit) or SVC (Switched Virtual Circuit).

Oper Status. The operational status of the ATM service, which can be **Enabled**, **Disabled**, or **Initial** (in an initializing mode).

SEL. The last byte of the ATM address.

Groups. The VLAN group number(s) associated with this service.

Conn VPI/VCI. The VPI/VCI (Virtual Path Identifier/Virtual Circuit Identifier) number used in this service.

Addrs Index. The MAC address(es) mapped to this service.

Viewing General Service Statistics on a Port

To view general statistics for LANE Client services on a port, type in **vss** followed by the slot/port. For example, if you wanted to obtain statistics information for port 1 on the board in slot 3, you would enter:

```
vss 3/1
```

This command displays a screen similar to the following:

Statistics for slot 3 interface 1

Srvc	Pkts In	Pkts Out	UPkts In	UPkts Out	BcPkts In	BcPkts Out	McPkts In	McPkts Out
====	=====	=====	=====	=====	=====	=====	=====	=====
1	331	40974	1007	1005	1324	39969	4000	4010
2	300	40001	990	988	1300	30000	3000	3001
3	200	30000	1000	1001	1205	40000	2654	2700

Pkts In. The total number of packets received at this Emulated LAN.

Pkts Out. The total number of packets sent from this Emulated LAN.

UPkts In: The number of packets received in a unicast format at this Emulated LAN. Unicast packets are transmitted to one recipient.

UPkts Out: The number of packets sent in a unicast format from this Emulated LAN.

BcPkts In. The number of packets received in a broadcast format at this Emulated LAN. Broadcast packets are transmitted to all recipients in the network.

BcPkts Out. The number of packets sent in a broadcast format from this Emulated LAN.

McPkts In: The number of packets received in a multicast format at this Emulated LAN. Multicast packets are transmitted to a select group of recipients.

McPkts Out: The number of packets sent in a multicast format from this Emulated LAN.

Viewing Service Statistics for a LANE Client

To view statistics for a specific LANE Client service, type in **vss** (found in the ATM menu), followed by the slot/port and the service number for the service. For example, if you wanted to obtain statistics information for slot 3, port 1, service 1, you would enter:

```
vss 3/1 1
```

This command displays a screen similar to the following:

```
Status/Statistics for slot 3 interface 1 Service 1

Service: LAN Emulation Service 1

LEC status      : Initial
ELAN Name       : default
ELAN Type       : 802.3
LEC ID          : 0
LES version     : ATM Forum 1.0
LES address     : 3903488001bc900001017838c00020da8436a0c1 (learned)
BUS address     : 3903488001bc900001017838c00020da8436a0c1
LECS address    : 4700790000000000000000000000a03e00000100 (ILMI/well-known LECS addr)

BUS
MC Forward VPC/VCC : 0/0      MC Send VPC/VCC      : 0/0
Echo suppress      : 0

LES
Control Direct VPC/VCC : 0/47      Cntl Distribute VPC/VCC : 0: 48
Control Frames Sent   : 19367     Control Frames Rcvd    : 19415
LE arps Sent         : 13          LE arps Received      : 23

LECS
Configuration VPC/VCC : 0/0
Packets Sent         : 0          Packet Received       : 0

STATISTICS
Packets In           : 331      Unicast Packets In    : 1007
Packets Out          : 40974    Unicast Packets Out   : 1005
Broadcast Pkts In    : 1324    Multicast Packets In  : 4000
Broadcast Pkts Out   : 39969    Multicast Packets Out : 4010
```

Token Ring LECs display two additional fields after the **LEC ID** field. These additional fields are **Bridge Num** and **Ring Num**.

The following section describes the fields displayed by the **vss** command for a specific LANE Client service (the fields displayed by the **vss** command for general Lane Client services are also included under the heading labeled **STATISTICS**).

Service: The name of the service.

LEC Status: The current status of the LEC. The LEC may be either **Operational** or **Non-Operational**.

ELAN Name: The name of the Emulated LAN.

ELAN Type: The Emulated LAN type. Possible options are 802.3 (Ethernet) or 802.5 (Token Ring).

LEC ID: The LAN emulation client identifier.

Bridge Num: A unique number used to identify the source routing bridge. This field displays only for 802.5 Token Ring clients.

Ring Num: The ring number assigned to the Token Ring for participation in source routing. This field displays only for 802.5 Token Ring clients.

LES version: The version of the LAN Emulation Server.

LES address: The address of the LAN Emulation Server.

BUS address: The address of the Broadcast Unknown Server.

LECS address: The address of the LAN Emulation Configuration Server.

BUS:

MC Forward VPC/VCC: VPC contains the VPI that identifies the VPC where it connects to this LE Client. VCC contains the VCI that identifies the VCC where it connects to this LE Client.

MC Send VPC/VCC: VPC contains the VPI that identifies the VPC where it connects to this LE Client. VCC contains the VCI that identifies the VCC where it connects to this LE Client.

Echo Suppress: The number of packets received with the client's LEC-ID.

LES:

Control Direct VPC/VCC: VPC contains the VPI that identifies the VPC where it connects to this LE Client. VCC contains the VCI that identifies the VCC where it connects to this LE Client.

Cntl Distribute VPC/VCC: VPC contains the VPI that identifies the VPC where it connects to this LE Client. VCC contains the VCI that identifies the VCC where it connects to this LE Client.

Cntl Frames Sent: The number of control frames sent to the LES.

Cntl Frames Rcvd: The number of control frames received from the LES.

LE arps Sent: The number of LE ARPs sent to the LES.

LE arps Received: The number of LE ARPs received from the LES.

LECS:

Configuration VPC/VCC: VPC contains the VPI that identifies the VPC where it connects to this LE Client. VCC contains the VCI that identifies the VCC where it connects to this LE Client.

Packets Sent: The number of packets sent to the LAN Emulation Configuration Server.

Packets Received: The number of packets received from the LAN Emulation Configuration Server.

STATISTICS :

Packets In: The total number of packets received at this Emulated LAN.

Packets Out: The total number of packets sent from this Emulated LAN.

Broadcast Pkts In: The number of packets received in a broadcast format at this Emulated LAN. Broadcast packets are transmitted to all recipients in the network.

Viewing Service Statistics for a LANE Client

Broadcast Pkts Out: The number of packets sent in a broadcast format from this Emulated LAN.

Unicast Packets In: The number of packets received in a unicast format at this Emulated LAN. Unicast packets are transmitted to one recipient.

Unicast Packets Out: The number of packets sent in a unicast format from this Emulated LAN.

Multicast Packets In: The number of packets received in a multicast format at this Emulated LAN. Multicast packets are transmitted to a select group of recipients.

Multicast Packets Out: The number of packets sent in a multicast format from this Emulated LAN.

Viewing the LANE LE_ARP Table

This command is useful for showing MAC to ATM identifier mappings. To view the ATM LANE LE_ARP table, type in **vlat**, followed by the slot/port and service number for the service.

```
Interface/ATM % vlat 5/1 2
```

ATM LANE LE_ARP Table

MAC Address	ATM Network Prefix	ESI	SEL	VPI/VCI	Age	Remote
0020da0210e0	39000000000000000000000000000000	0020da0210e0	00	101/153	5	True
0020da021210	39000000000000000000000000000000	0020da021210	00	181/106	59	True
0020da05f674	39000000000000000000000000000000	0020da05f674	00	166/138	226	False
0020da220053	39000000000000000000000000000000	0020da220053	00	185/146	233	True
0020da0204b0	39000000000000000000000000000000	0020da0204b0	00	169/108	257	True

```
Interface/ATM %
```

MAC Address: The MAC addresses of learned stations attached to the emulated LAN.

ATM Network Prefix: The first 13 bytes of the ATM address.

ESI: End station identifier, consisting of the next 6 bytes of the ATM address.

SEL: The last byte of the ATM address.

VPI: Virtual Path Identifier.

VCI: Virtual Circuit Identifier.

Age: The time since the MAC has been seen by this service.

Remotes: This field will read **True** if the MAC was learned via the LE-ARP response from the ATM end station. This field will read **False** if the LE-ARP response came from the LES (i.e., the entry was already in the LES database).

Token Ring 802.5 LECs contain an additional display that maps source route descriptor to ATM address. The following table is an example of the **vlat** command issued for a Token Ring LEC:

```
/Services % vlat 3/1 2
```

ATM LANE LE_ARP Table

MAC Address	ATM Network Prefix	ESI	SEL	VPI/VCI	Age	Remote
0020af0133d3	47000580ffe1000000f215120b0020da6fc640	0020da6fc640	02	0/ 47	191	True
0020af0136af	47000580ffe1000000f215120b0020da6d2b4002	0020da6d2b4002		0/ 48	95	True

ATM 802.5 LANE (SR RD to ATM_ADDRESS) LE_ARP Table

SR RD	ATM Network Prefix	ESI	SEL	VPI/VCI	Age	Remote
00e1	47000580ffe1000000f21512	0b0020da6d2760	02	0/ 41	161	False
00a1	47000580ffe1000000f21512	0b0020da6d2760	02	0/ 41	267	False

The top table is the same as a standard **vlat** display. The second table shows how the source route descriptor maps to the ATM address. The **SR RD** field displays the source route descriptor, consisting of 4 hex nibbles. The left three (3) nibbles represent the ring number; the right-most nibble represents the bridge number.

Viewing ATM Service Statistics for Classical IP

To view ATM service statistics, type in **vss** and press **<Enter>**. A screen similar to the following will be displayed:

```
//Interface/ATM % vss 5/1 3

      Status/Statistics for slot 5 interface 1 Service 3

Service      : Classical IP Service 3

>From IP:

      Packets Received = 0   Broadcast Packets Received= 0   Packets Discarded = 0

>To IP:

      Packets Sent      = 0

>From net:

      Packets Received = 0   Packets Discarded      = 0
      ARP Response     = 0   Inv ARP Request      = 0
      Inv ARP Response = 0   Inv ARP Request      = 0   Negative ARP Reply = 0

>To net:

      Packets Received = 0   Packets Discarded      = 0
      ARP Response     = 0   Inv ARP Request      = 0
      Inv ARP Response = 0   Inv ARP Request      = 0   Negative ARP Reply = 0

//Interface/ATM %
```

Service: The name of the service.

From IP:

Packets Received: The number of packets received via IP.

Broadcast Packets Received: The number of broadcast packets received via IP.

Packets discarded: The number of packets received via IP that were discarded.

To IP:

Packets sent: The number of packets sent via IP.

From net:

Packets received: The number of packets received via the network.

Packets discarded: The number of packets received via the network that were discarded.

ARP response: The number of ARP response packets received via the network.

ARP request: The number of ARP request packets received via the network.

Inv ARP response: The number of inverse ARP response packets received via the network.

Inv ARP request: The number of inverse ARP request packets received via the network.

Negative ARP Reply: The number of inverse ARP negative acknowledgment packets received via the network.

To net:

Packets sent: The number of packets sent via the network.

Packets discarded: The number of packets sent via the network that were discarded.

ARP response: The number of ARP response packets sent via the network.

ARP request: The number of ARP request packets sent via the network.

Inv ARP response: The number of inverse ARP response packets sent via the network.

Inv ARP request: The number of inverse ARP request packets sent via the network.

ARP Acknowledge: The number of inverse ARP negative acknowledgment packets sent via the network.

Viewing the CIP ARP Table

To view the ARP table for CIP, enter **vat** followed by **<Enter>**. This table (similar to that shown below) lists the IP addresses that are mapped to an ATM address.

```
Interface/ATM % vat
=====
IP Address          ATM Address          VPI   VCI   TTL   Type
=====
186.207.183.15     470000580ffe1000000f215120b00204815120b  0     0     15   static
186.207.182.11     470000580ffe1000000f215120b0020416ad721  0     16    11   dynamic
/Interface/ATM %
```

IP Address. The IP Address for this entry.

ATM Address. The ATM address to which the IP address maps.

VPI. The Virtual Path Identifier for this ATM address.

VCI. The Virtual Circuit Identifier for this ATM address.

TTL. The Time To Live counter for this address entry expressed in minutes. The entry ages out after the number of minutes indicated in this column.

Type. Indicates whether this address was entered by the user (static) or created by the system (dynamic).

Viewing Service Statistics for VLAN Clusters

To view VLAN Cluster service statistics, type in **vss** and press **<Enter>**. A screen similar to the following will be displayed:

```
/Interface/ATM % vss 3/1 5
  Status/Statistics for slot 3 interface 1 Service 5

Number of additional members in this cluster is : 2
Broadcast Out VCI used on this cluster         : 500

Additional Member : 1
-----
Description       : CLUSTERNUMBER1
Data-Direct VCI   : 201
Broadcast In VCI  : 202

Additional Member : 2
-----
Description       : CLUSTERNUMBER2
Data-Direct VCI   : 299
Broadcast In VCI  : 301

/Interface/ATM %
```

Description: The description for the additional VLAN Cluster member.

Data-Direct VCI: The circuit number of the point-to-point virtual circuit for a known unicast destination.

Broadcast In VCI: The circuit number of the one-way (in) broadcast virtual circuit.

Viewing 1483 Scaling Service Parameters

You can display 1483 scaling parameters with the **vgptovc** command. The syntax for this command is as follows:

```
vgptovc slot/port service_ID [beginning_group_ID/ ending_group_ID]
```

The **beginning_group_ID/ ending_group_ID** option will display a range of groups on a 1483 scaling service. If you do not use this option, then all groups will be displayed.

◆ Note ◆

If you have logged into the UI with the write privilege and you just want to display a simple list of the mapping entries for a 1483 scaling service, you can use the 1483 mapping submenu. This submenu is accessed through either the **cas** or **mas** commands and is described in *Editing and Displaying 1483 Mapping Parameters* on page 36-43.

For example, to display all groups on 1483 scaling service No. 2 on Slot 2, Port 1, enter

```
vgptovc 2/1 2
```

at the system prompt. A screen similar to the following will be displayed.

Slot 2 Port 1 Service 2 Group ID to Virtual Circuit Mapping

Group Id to VC Mapping and Connection Statistics

Slot /Port	Group	VCI	Rx SDUs	Tx SDUs	Rx Cells	Tx Cells	Rx Octets	Tx Octets
2/1	1	100	0	0	0	0	0	0
2/1	2	101	0	0	0	0	0	0
2/1	3	104	0	0	0	0	0	0

END OF MAPPING TABLE

The fields displayed by the **vgptovc** command are described below.

Slot. The slot number for this group.

Port. The port number for this group.

VCI. The Virtual Circuit Identifier (VCI) for this group.

Rx SDUs. The number of Service Data Units (SDUs), or frames, received on this group.

Tx SDUs. The number of SDUs (frames) transmitted on this group.

Rx Cells. The number of cells received on this group. The value is derived from the **Rx SDUs** statistic. Once an SDU (frame) is received on the port, the cells in the SDU are counted and added to this statistic.

Tx Cells. The number of cells transmitted on this group. The value is derived from the **Tx SDUs** statistic. Once an SDU (frame) is transmitted on the port, the cells in the SDU are counted and added to this statistic.

Rx Octets. The number of octets (bytes) received in the form of SDUs (frames) on this group.

Tx Octets. The number of octets (bytes) transmitted in the form of SDUs (frames) on this group.

Viewing 1483 Routed Format Services Statistics

To view ATM service statistics for 1483 routed format services, enter **vss** followed by the slot number of the ATM access port, a slash (/), the port number of the ATM access port, a space, and the service number. For example, to display the service statistics for 1483 routed format service 3 on Port 1 in Slot 5, enter

```
vss 5/1 3
```

at the system prompt. A screen similar to the following will be displayed.

```
Status/Statistic for slot 5 interface 1 Service 3
```

```
Service      : 1483 Routed Service 3
```

```
From IP:
```

```
  Packets Received = 0   Broadcast Packets Received = 0  
  Packet Discarded = 0
```

```
To IP:
```

```
  Packets Sent      = 0
```

The statistics displayed by the **vss** command for 1483 routed format services are described below.

Service. The name of the 1483 routed format service.

The next set of statistics under the heading “**From IP:**” describe incoming packets.

Packets Received: The number of packets received via IP.

Broadcast Packets Received: The number of broadcast packets received via IP.

Packets discarded: The number of packets received via IP that were discarded.

The next set of statistics under the heading “**To IP:**” describe outgoing packets.

Packets sent: The number of packets sent via IP.

Debugging LANE Client Problems

You use the **atmlsem** command to enable or disable debug messages on LANE clients. The syntax for this commands is as follows:

```
atmlsem <slot>/<port> <service> [-1| 0]
```

You *must* specify **-1** to enable debug messages or **0** to disable them. For example, to enable debug message on LANE client 2 on Port 1 in Slot 3, enter

```
atmlsem 3/1 1 -1
```

at the system prompt. The following is a sample of debug messages displayed after a LANE client was modified with the **mas** command.

```
LECCTL EVNT 'Proxy Logical Port': lc_bringdown_elan --> LC_ELAN resetting
LECDAT EVNT 'Proxy Logical Port': ELAN Status Notification - ELAN is Down
LECCTL EVNT 'Proxy Logical Port': Multicast VCC Torn Down, 0/64 cause = 31
LECCTL EVNT 'Proxy Logical Port': Multicast VCC Torn Down, 0/67 cause = 31
LECCTL TRAN 'Proxy Logical Port': (S_DISABLED, E_BUS_SVC_REL_NORM) -> S_DISABLED
LECCTL TRAN 'Proxy Logical Port': (S_DISABLED, E_BUS_SVC_REL_NORM) -> S_DISABLED
LECCTL EVNT 'Proxy Logical Port': Control VCC Torn Down, 0/60 cause = 31
LECCTL EVNT 'Proxy Logical Port': Control VCC Torn Down, 0/63 cause = 31
LECCTL TRAN 'Proxy Logical Port': (S_DISABLED, E_LES_SVC_RELEASE) -> S_DISABLED
LECCTL TRAN 'Proxy Logical Port': (S_DISABLED, E_LES_SVC_RELEASE) -> S_DISABLED
LECCTL TRAN 'Proxy Logical Port': (S_DISABLED, E_JOIN_START) -> S_ATM_WAIT
LECCTL TRAN 'Proxy Logical Port': (S_ATM_WAIT, E_AREG_DONE) -> S_ILMI_WAIT
LECCTL EVNT 'Proxy Logical Port': Use ILMI = TRUE, use WKA = TRUE
LECCTL EVNT 'Proxy Logical Port': Using ILMI to discover LECS ATM address
/LECCTL EVNT 'Proxy Logical Port': Unable to local LECS addr using ILMI, using WKA.
LECCTL TRAN 'Proxy Logical Port': (S_ILMI_WAIT, E_ILMI_NO_MORE) -> S_LECS_WSVS_WAIT
LECCTL EVNT 'Proxy Logical Port': LECS addr used pre:47007900000000000000000000000000
esi:00:a0:3e:00:00:01 sel:00.
LECCTL EVNT 'Proxy Logical Port': Configuration Direct VCC 0/86 Ready
LECCTL TRAN 'Proxy Logical Port': (S_LECS_WSVS_WAIT, E_LECS_SVC_READY) ->
S_CONFIG_WAIT
LECCTL TRAN 'Proxy Logical Port': (S_CONFIG_WAIT, E_RVC_CONFIG_RSP) -> S_LES_SVC_WAIT
LECCTL EVNT 'Proxy Logical Port': Configuration Direct VCC 0/86 Torn Down, cause = 31
LECCTL EVNT 'Proxy Logical Port': Control Direct VCC 0/88 Ready
LECCTL TRAN 'Proxy Logical Port': (S_LES_SVC_WAIT, E_LES_SVC_READY) -> S_JOIN_WAIT
LECCTL EVNT 'Proxy Logical Port': Accepting Control Distribute VCC.
LECCTL EVNT 'Proxy Logical Port': Control Distribute VCC 0/91 Ready
LECCTL EVNT 'Proxy Logical Port': Joined V0 LES ELAN=elan1
LECCTL EVNT 'Proxy Logical Port': Join same LES, keep all persistent VC.
LECCTL TRAN 'Proxy Logical Port': (S_JOIN_WAIT, E_RCV_JOIN_RSP) -> S_BUS_ARP_WAIT
LECCTL TRAN 'Proxy Logical Port': (S_BUS_ARP_WAIT, E_RCV_BUS_ARP_RSP) ->
S_BUS_SVC_WAIT
LECCTL EVNT 'Proxy Logical Port': Accepting Multicast Distribute VCC.
LECCTL EVNT 'Proxy Logical Port': Multicast Send VCC 0/92 Ready
LECCTL TRAN 'Proxy Logical Port': (S_BUS_SVC_WAIT, E_BUS_SVC_READY) -> S_OPERATIONAL
LECDAT EVNT 'Proxy Logical Port': ELAN Status Notification - ELAN is Up
LECCTL EVNT 'Proxy Logical Port': Multicast Forward VCC 0/95 Ready
```

To disable debug messages on LANE client 1 on Port 1 in Slot 3, for example, enter

```
atmlsem 3/1 1 0
```

at the system prompt.

37 Multi-Protocol Over ATM (MPOA)

Introduction

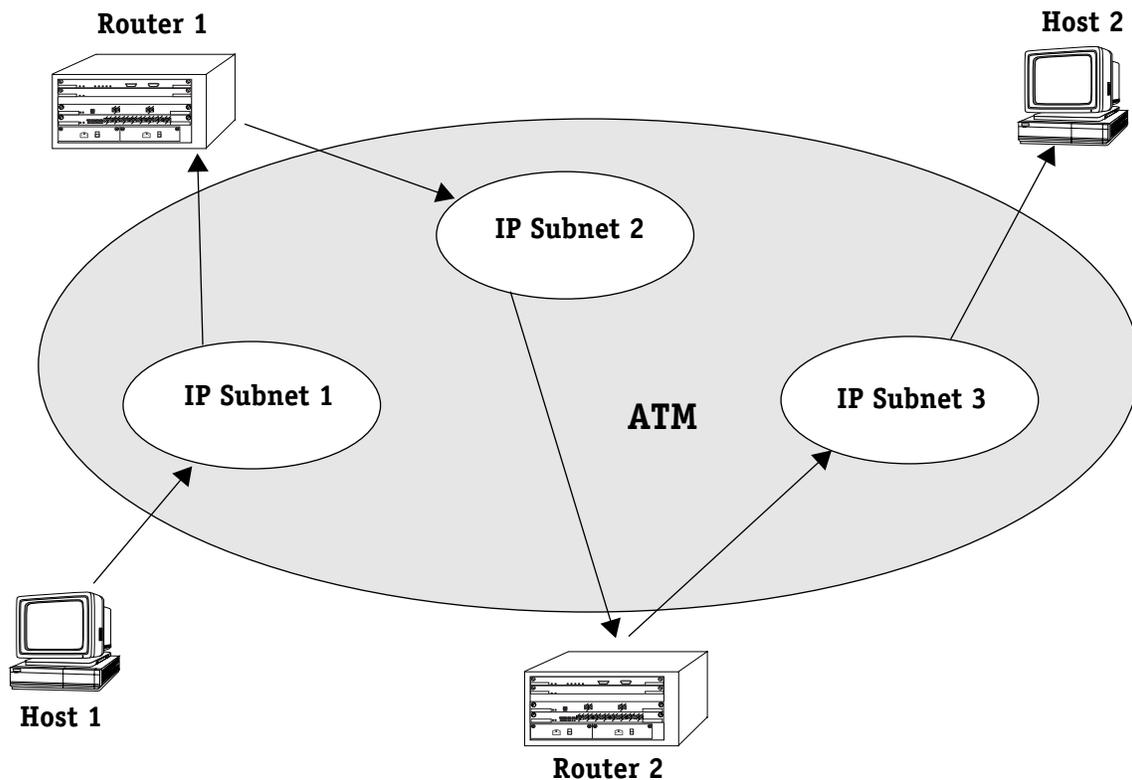
Multi-Protocol Over ATM (MPOA) eliminates problems with latency and increases throughput by reducing router hops in an IP or IPX network. In an MPOA based network, routing functionality is only required at the MPOA Server, hence reducing the number of devices participating in the routed network and reducing the need for complex configurations.

In regular router networks, each network device must participate in routing updates. Bringing routing functionality to the edge of the network increases configuration complexity and limits network scalability, since multiple devices participate in routing network traffic. An MPOA network is not required to participate in the routing functionality.

As a result, MPOA delivers manageable routing functionality in multi-gigabit networks by enabling existing and new applications to use the maximum available capacity in that network.

Network Functionality and MPOA

In an IP (or IPX) network, the path between a source network or host, and a destination network or host, can include multiple routed hops. In a routed network across ATM, additional latency is introduced when each router hop performs a frame-to-cell and cell-to-frame conversion. Due to the increased latency, router hops are a potential bottleneck. The following diagram demonstrates how Host 1 sends traffic in an IP network through two separate routers in order to communicate with Host 2:



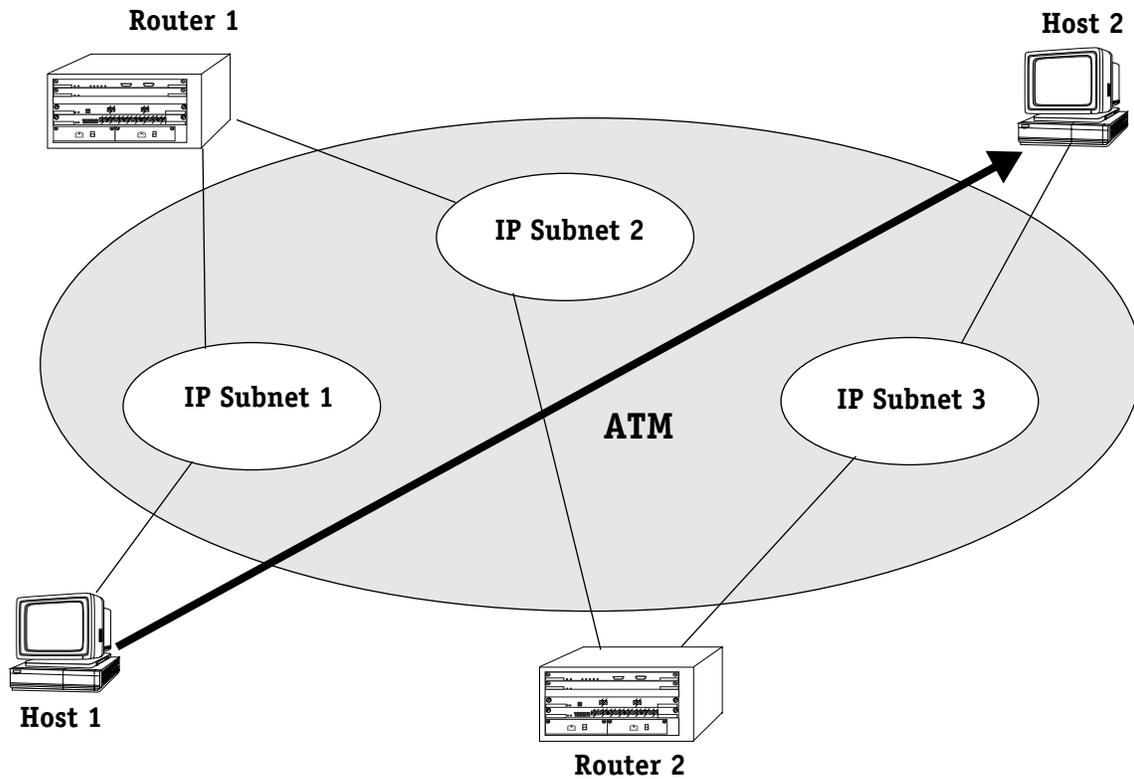
Traditional IP Routed Network

When Host 1 sends traffic to Host 2, it must go through Subnet 1, be routed by Router 1 to Subnet 2, be routed by Router 2 to Subnet 3, where it final is passed to Host 2. This process gets very complicated as more subnets are added to the network.

◆ Note ◆

Though these diagrams show an IP network, MPOA works with both IP and IPX networks.

Since all networking components are attached directly to the same physical ATM network, Host 1 should be capable of establishing a direct connection (i.e., a Virtual Channel Connection, or VCC) with Host 2. This connection is called a shortcut and optimizes the data path between Host 1 and Host 2, since no router hops are used. Using shortcuts to bypass traditional routing in networks is called Cut-Through routing, as demonstrated in the diagram below:



Cut-Through Routing

Though the network is still connected using the routed path described earlier, the router hops are avoided by when Host 1 can establish a direct path to Host 2 using Cut-Through routing, thus reducing latency and improving throughput times. This can be effectively done using Multi-Protocol over ATM (MPOA).

MPOA Requirements

MPOA is a Client/Server protocol with four main components:

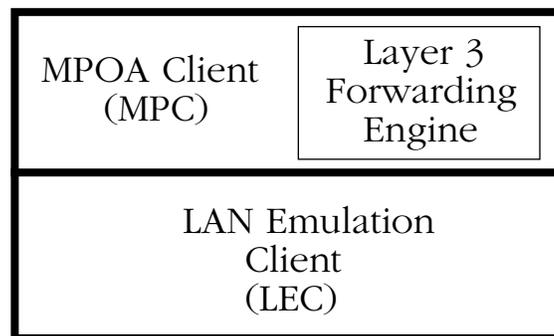
- The MPOA Client (MPC)
- The MPOA Server (MPS)
- LANE V2.0 for communication between network devices in the same subnet and for communication between the MPC and MPS.
- NHRP (Next Hop Resolution Protocol) for ATM address resolution of hosts in the network.

◆ Note ◆

The OmniSwitch and Omni Switch/Router require their respective versions of the High-speed Routing Engine (HRE, HRE-VX, and HRE-X) for MPOA to function

The MPOA Client (MPC)

The MPOA Client (MPC) resides on the edge device (a switch) or on a server directly attached to ATM. The primary function of the MPC is to control and monitor traffic that passes through the ATM uplink, and to setup a shortcut virtual circuit (VC) between two edge devices (switches). The MPC sets up short-cut VCs by providing address resolution obtained from the MPOA Server (MPS). The MPC also relies on a Layer 3 forwarding engine to format IP or IPX frames before they are transmitted on the shortcut VC.



MPC Components

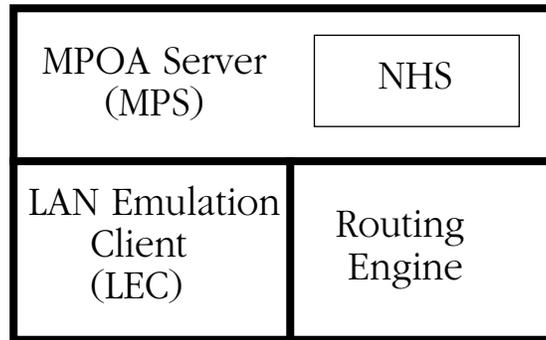
In the MPC's ingress role (sending data to another MPC or MPS), it detects traffic that is being forwarded over an ELAN to a router that contains an MPS. If the flow could benefit from a shortcut (i.e., bypass a routed path) the MPC initiates a query-response request to the MPS to get the information required to establish a shortcut to the destination. If a shortcut is available, the MPC caches the information in its ingress cache, sets up a shortcut Virtual Channel Connection (VCC), and forwards the traffic to its destination using the established shortcut.

In the MPC's egress role (receiving data from other MPOA objects), it forwards information from other MPCs to its local interfaces or users. For data received over a shortcut, it adds the appropriate Data Link Layer (DLL) encapsulation and forwards them to higher layers. The DLL encapsulation information is provided by an egress MPS and stored in the MPC's egress cache.

An MPC can service one or more LECs and communicate with multiple MPSs.

MPOA Server (MPS)

The MPOA Server (MPS) communicates with other MPSs and the MPCs in its ELAN. Typically, one MPS is assigned to a single subnet, or ELAN. For redundancy purposes, more MPSs can be assigned to a single subnet. The MPS provides a routing functionality and works with routing protocols (such as RIP, RIP II and OSPF) to find other subnets in the network. The MPS resolves the ATM address of a Layer 3 address. This resolution is required by the MPCs to set up the shortcut VCs. MPOA uses Next Hop Resolution Protocol (NHRP) to gather the address information from other subnets in the network.



MPS Components

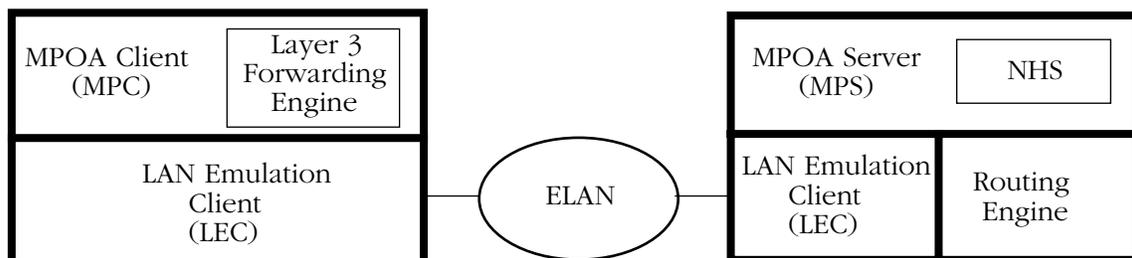
An MPS is the logical component of a router that provides internetwork layer forwarding to MPCs. It includes a full Next Hop Server (NHS) as defined by NHRP. The MPS interacts with its local NHS and routing functions to answer queries from ingress MPCs and provides Data Link Layer (DLL) encapsulation information to egress MPCs.

An MPS converts between MPOA requests and replies, and NHRP requests and replies for MPCs.

◆ Important Note ◆

The rest of this chapter describes the commands for configuring the MPOA client. Alcatel provides an optional MPOA server with the OmniMSS product. The MPOA server functionality is not described in this chapter.

The relationship of the MPC to the MPS and their respective components is shown below:



An MPOA Client and Server Connected Through an Emulated LAN

The MPC and MPS are connected by LANE, using locally configured LECs that communicate via an ELAN.

LAN Emulation (LANE)

LAN Emulation (LANE) version 2 is a requirement of MPOA. LANE is used for intra-subnet communications and is a Layer 2 framework that makes a connection-oriented ATM network seem like a shared connectionless Ethernet or Token Ring LAN segment.

LANE uses a client/server model with Emulated LANs (ELANs) made up of multiple LANE clients (LECs) and a LANE Server (LES). The LES provides a MAC to ATM address resolution and broadcast service to the LECs. Clients are implemented on ATM/LAN edge devices and ATM attached hosts, while the LESs can be implemented in a router, LAN or ATM switch, or in a stand alone ATM equipped device.

LANE still requires tradition network layer routers to interconnect these workgroups, or ELANS, significantly limiting the overall performance and scalability of the network. As the number of hosts and subnets grow, routers tend to be overwhelmed by complex routing paths and memory requirements.

For more specific information on LANE and LANE services, see Chapter 35, "LANE Server Configuration," and Chapter 36, "Configuring ATM Services."

Next Hop Resolution Protocol (NHRP)

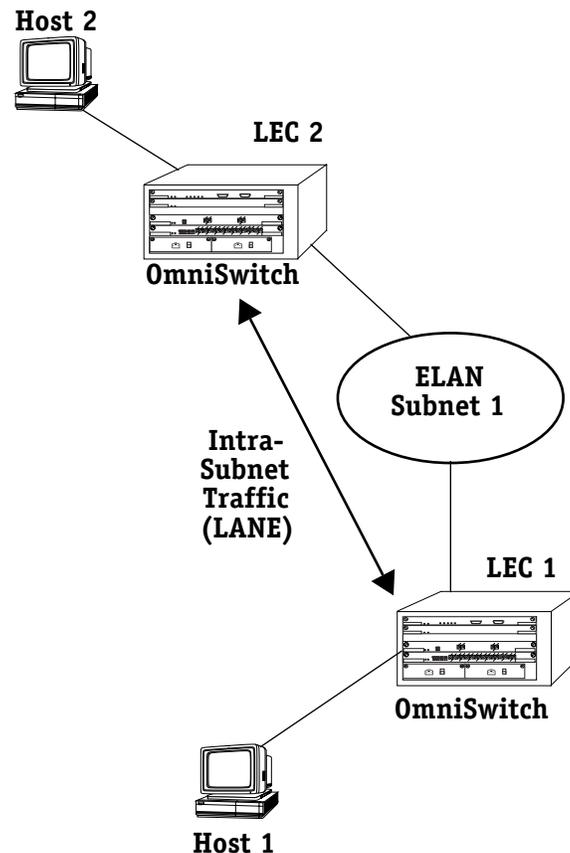
MPOA servers use Next Hop Resolution Protocol (NHRP) to learn network addresses. These addresses allow MPOA to create the shortcuts necessary for Cut-Through routing. NHRP provides an extended address resolution protocol that permits Next Hop Clients (NHCs) to send queries between different logical IP subnets (LISs), sometimes referred to as Local Address Groups (LAGs).

Once network address are learned and cached, ATM Switched Virtual Circuits (SVCs) can be established across subnet boundaries, allowing inter-subnet communication without intermediate routers.

An MPC transmitting data sends queries to an MPS for an address resolution for the destination MPC. The MPS's Next Hop Server (NHSs) obtains address information for the query through the standard routing path. Once the address is resolved, the MPS replies to the MPC query with the address of the destination MPC.

The MPOA Network

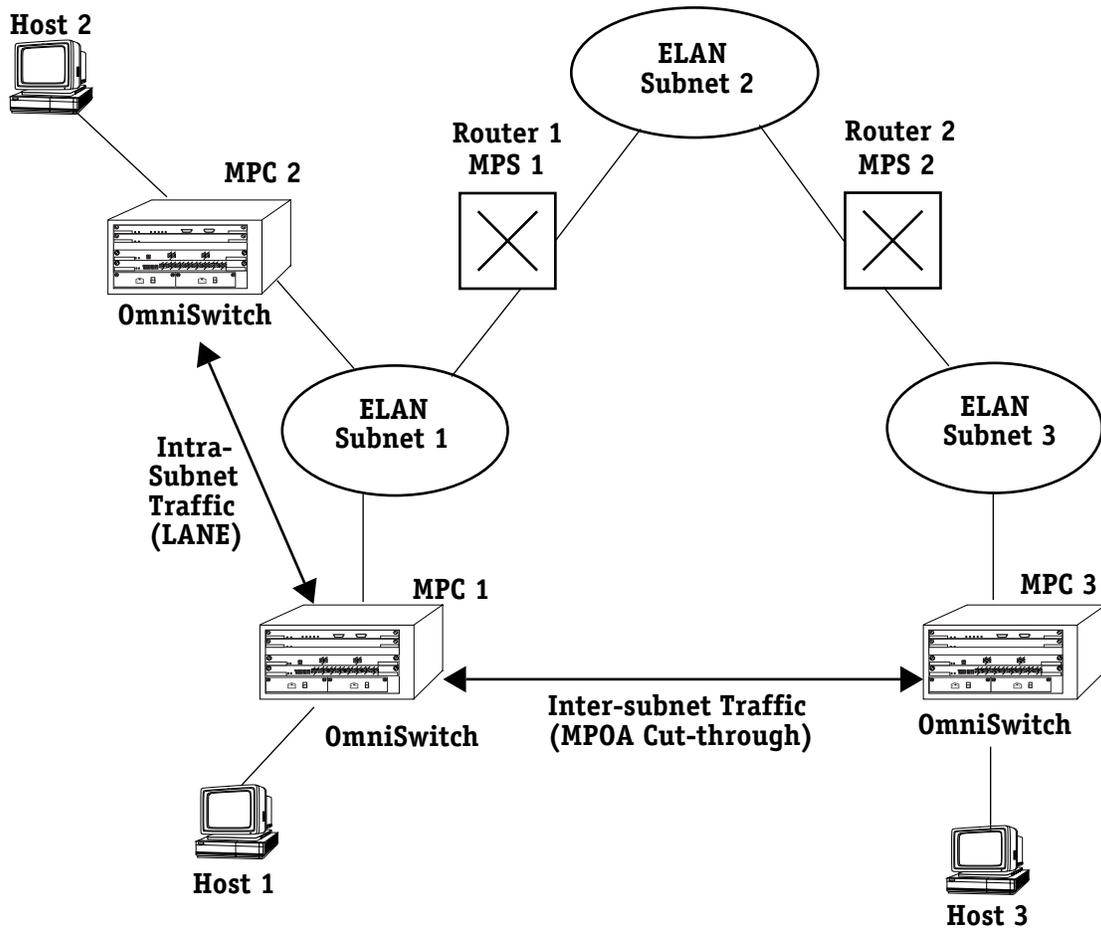
LAN Emulation (LANE) allows for intra-subnet Virtual Circuits (VCs) to be created. These VCs provide end devices with specific entry points of destination devices. This is useful when more than one switch is attached to a subnet, as demonstrated in the following diagram:



Simple LANE Configuration

LAN Emulation Clients (LECs) sit on the switches and communicate through an Emulated LAN (ELAN) address for Subnet 1. When Host 1 sends traffic to Host 2, any intra-subnet switching that would normally take place within Subnet 1 is now bypassed because the LECs provide points of access for the switches directly responsible for the hosts in question. Using the points of access, a VC is created.

MPOA allows for similar connections to be made between different subnets using cut-through routing. The MPOA Clients (MPCs) sit on the switches alongside the LANE clients, and uses the same functionality as the LECs to communicate with other MPCs or MPSs in the network. By adding to the above diagram, we can illustrate this idea:



MPOA Network

This diagram is a simple MPOA network with three subnets. Subnet 1 has two edge device switches and Subnet 3 has one. The three subnets are connected by two routers (Routers 1 and 2) that each have an MPS.

Three hosts are used in this example. Host 1 and 2 are part of Subnet 1 (hosts can be connected to their edge device switches using specific protocol such as Ethernet). Host 3 is part of Subnet 3.

◆ Note ◆

The MPSs could be co-located with the MPCs on one of the switches or can reside in a separate device. The functionality of the network remains the same either way. A single MPS device can have multiple MPS instances. Each MPS is responsible for its own subnet and the MPC's servicing that subnet.

This model works as follows:

1. If Host 1 wants to communicate with Host 3, the standard traffic path without MPOA is through Subnet 1 to Router 1 (co-located with MPS 1) via the edge device (i.e., ATM access module). Router 1 forwards the data to Router 2 via Subnet 2, and the data is received by Host 3 through the switch for Subnet 3. As more routers are involved, this process can slow down traffic speeds.
2. MPOA addresses this problem. Outward bound traffic is monitored by MPC 1. When a preset threshold (in number of packets per set time period) is exceeded, MPC 1 tries to use a shortcut between MPC 1 and MPC 3 (or another remote destination).
3. If no shortcut exists, MPC 1 requests the resolution of MPC 3's ATM address from MPS 1. If MPS 1 has the resolution in its cache, it returns it immediately to MPC 1. When no cache information is available, MPS 1 resolves the requests and sends it to MPS 2. MPS 2 returns the information to MPS 1 and MPS 1 forwards the response to MPC 1. MPC 1 uses the ATM address to create a short-cut to MPC 3, bypassing all the router hops. MPC 3 sends the received data to Host 3.
4. Entries are created in the ingress and egress cache tables of MPC 1 and MPC 3, so that it is not necessary to reinitiate address resolution for this destination.
5. If Host 2 wants to communicate with Host 3, the process is the same as above. Note that communications between Host 1 and Host 2 is handled by LANE, as they are part of the same subnet, or ELAN.

If another host is connected to the edge device MPC 1 and sends data to Host 3, the same short-cut can be used. This avoids the resolution phase and saves on VC resources.

Alcatel's implementation of MPOA follows the above design. The MPC resides on the edge device (i.e., ATM access module), and works together with the local LEC V2.0 defined on the ATM uplink port.

◆ Important Note ◆

The MPOA Client requires the HRE or HRE-X to perform the MPOA encapsulation (Ethernet or Token Ring to RFC1483 routed BPDU).

Since most users in a routed internetwork connect to repetitive or habitual external addresses, the edge device can save (cache) VC information to be reused without having to address resolution requests for every flow. To this end, the MPC maintains an ingress (for outward bound data) and egress (for inward bound data) cache tables for routing on shortcuts. For information on viewing the ingress and egress caches, see *Viewing Entries in the Ingress Cache Table* on page 37-19 and *Viewing Entries in the Egress Cache Table* on page 37-20, respectively.

◆ Important Note ◆

The OmniMSS does not support the MPOA server using IPX at this time.

The MPOA Management Menu

The user interface commands for configuring and monitoring the MPOA Client (MPC) are listed in the **mpc** submenu. To access this submenu, enter

mpc

followed by **<return>**, at the system prompt. If you are in verbose mode, a screen similar to the following is displayed. Otherwise, enter a question mark (?) to see the **mpc** menu commands:

Command	MPC Service Menu				
mpccfg	Configuration of MPC Service				
vmcpc	Show status of a MPC Service				
vmcpcst	Show statistics of a MPC Service				
vmcpci	Show Ingress Cache Table of a MPC Service				
vmcpcce	Show Egress Cache Table of a MPC Service				
vmcpcs	List all MPOA servers per MPC				
	Main Interface	File Security	Summary System	VLAN Services	Networking Help

To use a command from the menu enter it at the command prompt. The commands are used in the following manner:

mpccfg. Allows you to enable, disable, or configure an MPOA client service for a particular port. See *Configuring an MPOA Client Service* on page 37-11 for more information.

vmcpc. Displays the current status of an MPOA client service. See *Viewing Client Service Status* on page 37-14 for more information.

vmcpcst. Displays the statistics of an MPOA client service. See *Viewing Client Service Statistics* on page 37-15 for more information.

vmcpci. Displays all entries in the Ingress Cache Table for an MPOA client service. The Ingress Cache Table is a list of records for routing outgoing traffic. Each record consists of a network address, an ATM address, a VSC, and a hold time. See *Viewing Entries in the Ingress Cache Table* on page 37-19 for more information.

vmcpcce. Displays all records in the Egress Cache Table for an MPOA client service. The Egress Cache Table is a list of records for routing incoming traffic. Each record consists of a network address, an ATM address, a VSC, and a hold time. See *Viewing Entries in the Egress Cache Table* on page 37-20 for more information.

vmcpcs. Displays all the MPOA servers (MPSS) associated with this client. Each MPS entry shows the ATM address, MAC address, and the MPC associated ELAN. See *Viewing MPOA Servers* on page 37-21 for more information.

Configuring an MPOA Client Service

The MPOA client (MPC) resides on the edge device, or switch, and monitors traffic from its associated ELANs. Along with the MPOA Server (MPS), it can create internetwork shortcuts to reduce the number of router hops necessary for data traffic by maintaining egress and ingress tables for routing outgoing and incoming traffic.

The MPC automatically detects if there are any LANE client services (LEC services) on a given slot and port. If so, it creates an MPOA Client service for each LEC service. You can let the MPC service be configured automatically based on the network LANE configuration, or configure it manually on a slot and port basis. To configure a service:

1. From the **mpc** menu, enter the **mpccfg** command as follows:

```
mpccfg <slot>/<port>
```

where **<slot>** is the slot number of the board on which the port is located and **<port>** is the port number on the selected board you want to modify. For example, to configure an MPOA client service on port 2 of slot 3, you would enter

```
mpccfg 3/2
```

The following menu appears for all services automatically generated by the MPOA client:

```
1) Enable Service {No(1), Yes(2)}           : Yes
2) Configuration Mode {Auto(1), Manual(2)}  : Auto
```

```
Enter (option=value/save/cancel) :
```

2. If you want the MPC service to be configured automatically (based on the LEC configurations), make sure the service is enabled, leave the **Configuration Mode** set to **Auto**, and then save the configuration (if any changes were made). It uses configuration information from the LEC service, and can now route traffic.
3. If you wish to manually configure the service, then change the **Configuration Mode** to **Manual**. This is done by entering **2** (the line number for **Configuration Mode**), an equal sign (=), then a **2** (the value for **Manual**), as shown:

```
2=2
```

4. The menu is now expanded to include options that are manually configurable, as shown below:

1) Enable Service {No(1), Yes(2)}	: Yes
2) Configuration Mode {Auto(1), Manual(2)}	: Manual
3) Setup Frame Count {1-65535}	: 10
4) Setup Frame Time {1-60 sec.}	: 1
5) Initial Retry Time {1-300 sec.}	: 5
6) Retry Time Maximum {10-300 sec.}	: 40
7) Hold Down Time {30-1200 sec.}	: 160
8) IP Protocol Enable {Disable(1), Enable(2)}	: Enable
9) IPX Protocol Enable {Disable(1), Enable(2)}	: Disable
10) VCC Aging Time {10-300 sec.}	: 300

Enter (option=value/save/cancel) :

To change a field value, type the line number, an equals sign, and the new value at the system prompt. For example, to change the **Setup Frame Count** to **20**, you would enter **3** (the line number for **Setup Frame Count**), an equal sign (=), and then **20**, as follows:

3=20

The **Setup Frame Count** would now be set to **20**.

5. When you are finished making changes to the service configuration, remember to save the configuration by typing **save** and then **<return>** at the system prompt.

◆ Important Note ◆

There can be multiple services created on a single slot/port by the MPC, depending on the configuration of your LANE environment. When you configure or change settings for a slot and port, all services on that slot and port are affected. You must reboot the switch to apply the changes.

Field Descriptions

The following sections describe the configurable options in the **mpccfg** menu.

Enable Service {No(1), Yes(2)}

This field allows you to enable or disable a service. An enabled service is active and can transmit or receive data, while a disabled service is inactive and nonfunctional. **Yes (2)** enables the service and **No (1)** disables it.

Configuration Mode {Auto(1), Manual(2)}

This field allows you to select the configuration mode, either **Auto (1)** or **Manual (2)**. In automatic configuration mode, the service uses the settings of the LEC for its configuration options. If set to manual, the user can change the default settings for the available options.

Setup Frame Count {1-65535}

The field, combined with the **Setup Frame Time**, determines when the MPC attempts to create a internetwork shortcut. This field represents the number of frames necessary in a data flow before a shortcut attempt is made. (A data flow is a uni-directional flow of data packets to a single destination.) If this field is set to **1**, a shortcut attempt is made for every data flow regardless of size, however this is not advisable as it is a waste of network resources.

Setup Frame Time {1-60 sec.}

This field, combined with the **Setup Frame Count**, determines when the MPC attempts to create an internetwork shortcut. This field represents a period of time (in seconds) during which the number of frames in a data flow are counted. If the number of frames during this time period equals or exceeds the value set in the **Setup Frame Count**, an internetwork shortcut is attempted.

Initial Retry Time {1-300 sec.}

This field is the initial number of seconds allowed for a MPC resolution request before the operation times out. The retry time consists of the number of seconds set in this field multiplied by a retry multiplier (a constant value of 2). If a resolution request times out, a new request is sent with the same value, until the maximum retry time is matched or exceeded.

Retry Time Maximum {10-300 sec.}

The maximum number of seconds allowed for MPC resolution request retries.

Hold Down Time {30-1200 sec.}

The number of seconds the MPC must wait before reinitiating a failed resolution attempt.

IP Protocol Enable {Disable(1), Enable(2)}

If your network uses IP to route data, set this field to **Enable**. If this field is set to **Disable**, IP traffic is not routed.

IPX Protocol Enable {Disable(1), Enable(2)}

If your network uses Internet Package Exchange (IPX) to route data, set this field to **Enable**. If this field is set to **Disable**, IPX traffic is not routed.

VCC Aging Time {10-300 sec.}

The number of seconds an idle Virtual Channel Connection (VCC) is allowed to remain open. VCCs are shortcuts created by MPCs to transmit and receive internetwork data flows. If a VCC is open and idle (no data transmitted or received) for a period of time greater than the number of seconds specified in this field, it is shut down.

Viewing Client Service Status

Once you have configured a client service, you can view the status of the service with the **vmpc** command. To view the status of a service enter the **vmpc** command as follows:

```
vmpc <slot>/<port>
```

where **<slot>** is the slot number of the board on which the port is located and **<port>** is the port number on the selected board you want to modify. For example, to view the status of an MPOA client service on port 2 of slot 3, you would enter:

```
vmpc 3/2
```

A screen similar to the following appears:

```
Control ATM Address : 3903488001bc900001019657700020da9c6c2c03
Operation State     : Up
Data ATM Address    : 3903488001bc900001019657700020da9c6c2cbf
```

```
*Current Configuration*
Configuration Mode      : Manual
Setup Frame Count       : 10
Setup Frame Time {sec.} : 5
Initial Retry Time {sec.} : 300
Retry Time Maximum {sec.} : 40
Hold Down Time {sec.}   : 160
IP Protocol Enable      : Enable
IPX Protocol Enable     : Disable
VCC Aging Time {sec.}  : 20
```

```
*ELANs with the MPC*
1) 180_1_4
```

None of these fields can be modified on this screen. To modify the configuration of a service, see *Configuring an MPOA Client Service* on page 37-11.

Field descriptions

The following section describes the fields associated with the **vmpc** command.

Control ATM Address. The address used to set up a switch virtual circuit (SVC) for sending control packets to an MPS. This address may be different from the Data ATM Address.

Operational State. Shows whether the service is running or not. **Up** means the service is operational and can pass data, and **Down** means the service is not running. See *Configuring an MPOA Client Service* on page 37-11 for information on changing the service status.

Data ATM Address. An ATM address used to set up a shortcut for data traffic between MPCs on the network. This address may be different from the Control ATM Address.

Current Configuration. For a description of these fields, see *Configuring an MPOA Client Service* on page 37-11.

ELANs with the MPC. Shows all ELANs names associated with this MPC service.

Viewing Client Service Statistics

You can view the statistics for an MPC service once it has been configured using the **vmcst** command. To view service statistics, enter the **vmcst** command as follows:

```
vmcst <slot>/<port>
```

where **<slot>** is the slot number of the board on which the port is located and **<port>** is the port number on the selected board you want to modify. For example, to view the statistics of an MPOA client service on port 2 of slot 3, you would enter:

```
vmcst 3/2
```

A screen similar to the following appears:

```

txMpoaResolveRequests           : 0
rxMpoaResolveReplyAcks          : 0
rxMpoaResolveReplyInsufECResources : 0
rxMpoaResolveReplyInsufSCResources : 0
rxMpoaResolveReplyInsufEitherResources : 0
rxMpoaResolveReplyUnsupportedInetProt : 0
rxMpoaResolveReplyUnsupportedMacEncaps : 0
rxMpoaResolveReplyUnspecifiedOther : 0
rxMpoaImpRequests               : 0
txMpoaImpReplyAcks              : 0
txMpoaImpReplyInsufECResources  : 0
txMpoaImpReplyInsufSCResources  : 0
txMpoaImpReplyInsufEitherResources : 0
txMpoaImpReplyUnsupportedInetProt : 0
txMpoaImpReplyUnsupportedMacEncaps : 0
txMpoaImpReplyUnspecifiedOther  : 0
txMpoaEgressCachePurgeRequests  : 0
rxMpoaEgressCachePurgeReplies   : 0
rxMpoaKeepAlives                : 0
rxMpoaTriggers                  : 0
rxMpoaDataPlanePurges           : 0
txMpoaDataPlanePurges           : 0
rxNhrpPurgeRequests             : 0
txNhrpPurgeReplies              : 0
rxErrUnrecognizedExtensions     : 0
rxErrLoopDetecteds              : 0
rxErrProtoAddrUnreachables      : 0
rxErrProtoErrors                 : 0
rxErrSduSizeExceededs           : 0
rxErrInvalidExtensions          : 0
rxErrInvalidReplies             : 0
rxErrAuthenticationsFailures    : 0
rxErrHopCountExceededs          : 0

```

You cannot modify the fields displayed in this screen.

Field descriptions

The following section describes the various fields in the **vmcst** command.

◆ Note ◆

The values for these counters are reset to zero when the management system or the MPC device is re-initialized.

txMpoaResolveRequests. The number of MPOA Resolution Requests transmitted by this client to other MPOA objects on the network. An MPOA Resolution Request is sent from an ingress MPC to an ingress MPS to request the egress ATM address corresponding to an internetwork layer destination address.

rxMpoaResolveReplyAcks. The number of positively acknowledged successful MPC Resolution Replies received by this MPC. An MPOA Resolution Reply is sent from an ingress MPS to an ingress MPC in reply to a corresponding MPOA Resolution Request upon receiving an NHRP Resolution Reply from the egress MPS.

rxMpoaResolveReplyInsufECResources. The number of MPOA Resolve Replies received with the message “Insufficient resources to accept egress cache entry.” This could refer to lack of memory or other resources.

rxMpoaResolveReplyInsufSCResources. The number of MPOA Resolve Replies received with the message “Insufficient resources to accept the shortcut.” This could refer to lack of memory or other resources.

rxMpoaResolveReplyInsufEitherResources. The number of MPOA Resolve Replies received with the message “Insufficient resources to accept either shortcut or egress cache entry.” This could refer to lack of memory or other resources.

rxMpoaResolveReplyUnsupportedInetProt. The number of MPOA Resolve Replies received with the message “Unsupported Internetwork Layer protocol.” This includes anything other than IP or IPX.

rxMpoaResolveReplyUnsupportedMacEncaps. The number of MPOA Resolve Replies received with the message “Unsupported MAC layer encapsulation.” Supported protocols include Ethernet, 802.3, 802.2 SNAP, and Token Ring.

rxMpoaResolveReplyUnspecifiedOther. The number of MPOA Resolve Replies received with the message “Unspecified other.”

rxMpoaImpRequests. The number of MPOA Cache Imposition Requests received by this MPC. An MPOA Cache Imposition Request is sent from an ingress cache MPS to an egress MPC to record an egress cache entry upon the receipt of an NHRP Resolution Request from the ingress MPS.

txMpoaImpReplyAcks. The number of successful MPOA Cache Imposition replies transmitted by this MPC.

txMpoaImpReplyInsufECResources. The number of successful MPOA Cache Imposition replies transmitted by this MPC denying the egress table entry because of insufficient resources to accept an egress cache entry.

txMpoaImpReplyInsufSCResources. The number of successful MPOA Cache Imposition replies transmitted by this MPC informing the MPS that a shortcut was not made due to insufficient resources.

txMpoaImpReplyInsufEitherResources. The number of successful MPOA Cache Imposition replies transmitted by this MPC denying the egress table entry because of insufficient resources to accept either a shortcut or egress cache entry.

txMpoaImpReplyUnsupportedInetProt. The number of successful MPOA Cache Imposition replies transmitted by this MPC denying the egress cache entry because of an unsupported Internetwork Layer protocol.

txMpoaImpReplyUnsupportedMacEncaps. The number of successful MPOA Cache Imposition replies transmitted by this MPC denying the egress cache entry because of an unsupported MAC Layer encapsulation.

txMpoaImpReplyUnspecifiedOther. The number of successful MPOA Cache Imposition replies transmitted by this MPC denying the egress cache entry because of some unspecified reason.

txMpoaEgressCachePurgeRequests. The number of MPOA Egress Cache Purge Requests transmitted by this MPC. An MPOA Egress Cache Purge Request is sent from an egress MPC to and egress MPS to purge an egress cache entry.

rxMpoaEgressCachePurgeReplies. The number of MPOA Egress Cache Purge Replies received by this MPC. An MPOA Cache Purge Reply is sent from an egress MPS to an egress MPC in reply to an MPOA Egress Cache Purge Request.

rxMpoaKeepAlives. The number of MPOA Keep Alive messages received by this MPC. A Keep Alive message is sent from the MPC to MPSs to make sure the MPSs that have supplied cache entries are alive and able to maintain those cache entries.

rxMpoaTriggers. The number of MPOA Trigger messages received by this MPC. An MPOA trigger is sent from an ingress MPS to an ingress MPC to request the ingress MPC to issue MPOA Resolution Requests.

rxMpoaDataPlanePurges. The number of MPOA Data Plane Purge messages received by this MPC. A Data Plane Purge is an NHRP Purge message sent on the data plane by an egress MPC to an ingress MPC to purge ingress cache entries.

txMpoaDataPlanePurges. The number of MPOA Data Plane Purge messages sent by this MPC.

rxNhrpPurgeRequests. The number of Purge Requests received by this MPC. A Purge Request is sent by an ingress MPS to an ingress MPC to purge ingress cache entries.

txNhrpPurgeReplies. The number of Purge Replies sent by this MPC.

rxErrUnrecognizedExtensions. The number of Error Indication packets received by this MPC with the error code "Unrecognized Extension." An Error Indication packet is sent to the sender of an NHRP packet to convey error indications. All MPOA control packets have extensions that control receiving component function or provide information. Examples of extension are DLL headers, egress cache tags, or hop counts.

rxErrLoopDetecteds. The number of Error Indication packets received by this MPC with the error code "Loop Detected." A Loop Detected error is generated when it is determined that an NHRP packet is being forwarded in a loop.

rxErrProtoAddrUnreachables. The number of Error Indication packets received by this MPC with the error code "Protocol Address Unreachable." A Protocol Address Unreachable error is generated when a packet is moving along the routed path and it reaches a point where the protocol address of interest is not reachable.

rxErrProtoErrors. The number of Error Indication packets received by this MPC with the error code "Protocol Errors." A Protocol Errors error is sent when a generic packet processing error has occurred.

rxErrSduSizeExceededs. The number of Error Indication packets received by this MPC with the error code "SDU Size Exceeded."

rxErrInvalidExtensions. The number of Error Indication packets received by this MPC with the error code "Invalid Extensions." Invalid extensions are any extension received by the MPOA client that is supported, but the content is wrong or undecipherable.

rxErrInvalidReplies. The number of Error Indication packets received by this MPC with the error code "Invalid Replies." Replies are sent by other MPOA components in response to requests by this MPC. An invalid reply is a reply that contains unexpected or undecipherable data.

rxErrAuthenticationsFailures. The number of Error Indication packets received by this MPC with the error code "Authentication Failure." This occurs if a request is denied because it failed security authentication.

rxErrHopCountExceededs. The number of Error Indication packets received by this MPC with the error code "Hop Count Exceeded."

Viewing Entries in the Ingress Cache Table

When the MPC uses a shortcut to route traffic between subnets, it looks up the address for the point of entry into the other subnet and records the address in its ingress cache table. To view entries in the MPC service ingress cache table enter the **vmpci** command as follows:

```
vmpci <slot>/<port>
```

where **<slot>** is the slot number of the board on which the port is located and **<port>** is the port number on the selected board you want to modify. For example, to view the ingress cache table of an MPC service on port 2 of slot 3, you would enter:

```
vmpci 3/2
```

A screen similar to the following appears:

Type	Network Address	ATM Address	VPI/VCI	Hold Time
IP	208.7.8.5	3903488001bc900001000100010020da048731c0	0/100	4

You cannot modify this screen with the **vmpci** command.

Field descriptions

The following section describes the fields available in the **vmpci** command.

Type. The routing type employed by the MPC service. It can be IP, Internetwork Packet Exchange (IPX), or both. If both IP and IPX are valid, then the **Type** display reads as follows:

```
IP/IPX
```

Network Address. The network address (IP) for this record in the ingress cache table of the MPC service. If the client is configured for IPX, an IPX address is displayed.

ATM Address. The ATM address for this record in the ingress cache table of the MPC service.

VPI/VCI. The Virtual Path Indicator (VPI) and Virtual Channel Indicator (VCI) for this record in the ingress cache table of the MPC service. These combined numbers act as an address for a Virtual Channel Connection (VCC).

Hold Time. The hold time, in seconds, between attempts to establish a connection with the destination listed in this record.

◆ Note ◆

The entries in the ingress cache table refer to *entry points* into other remote subnets (i.e., another MPC or MPS). whereas entries in the egress cache table refer to *destinations* in the subnet or subnets managed by the local MPC service.

Viewing Entries in the Egress Cache Table

When the MPC receives routed traffic from another MPOA component, it looks up the address for the destination of the traffic in its egress cache table. To view entries in the MPC service egress cache table enter the **vmpce** command as follows:

```
vmpce <slot>/<port>
```

where **<slot>** is the slot number of the board on which the port is located and **<port>** is the port number on the selected board you want to modify. For example, to view the egress cache table of an MPC service on port 2 of slot 3, you would enter:

```
vmpce 3/2
```

A screen similar to the following appears:

Type	Network Address	ATM Address	VPI/VCI	Hold Time
IP	208.6.8.1	3903488001bc900001000100010020da048730c0	0/153	4

You cannot modify this screen with the **vmpce** command.

For a definition of the fields displayed with the **vmpce** command, see *Viewing Entries in the Ingress Cache Table* on page 37-19.

◆ **Note** ◆

The entries in the egress cache table refer to *destinations* in the subnet or subnets managed by the local MPC service, whereas entries in the ingress cache table refer to *entry points* into other remote subnets (i.e., another MPC or MPS).

Viewing MPOA Servers

When an MPC service is established and active, it notes its own MPOA server (MPS) as well as any other MPS it becomes aware of while routing traffic. You can view all MPSs associated with an MPC service. To view a list of all MPSs associated with an MPC service, enter the **vmpcs** command as follows:

```
vmpcs <slot>/<port>
```

where **<slot>** is the slot number of the board on which the port is located and **<port>** is the port number on the selected board you want to modify. For example, to view associated servers for an MPC service on port 2 of slot 3, you would enter:

```
vmpcs 3/2
```

A screen similar to the following appears:

MPS ATM Address	MAC Address	ELAN

3903488001bc900001000100010020da048733c1	0020da048799	elan1_802.3

You cannot modify this screen with the **vmpcs** command.

Field descriptions

The following section describes the fields displayed with the **vmpcs** command.

MPS ATM Address. The ATM address of this MPS.

MAC Address. The Media Access Control (MAC) address of this MPS.

ELAN. The Emulated LAN associated with this MPS.

38 Frame Relay/ATM Internetworking

Alcatel's Frame Relay (FR)/Asynchronous Transfer Mode (ATM) Internetworking Function (IWF) software provides a smooth interworking between Alcatel's Frame Relay and ATM network interfaces. You can create an IWF *service* between a Frame Relay device and an ATM device, or you can trunk several Frame Relay devices over a single ATM connection in an FR/ATM IWF *network*.

◆ Important Note ◆

You *must* install the **frlmi.img** image file to run the Frame Relay/ATM internetworking software.

Specifications for FR/ATM IWF services are defined in the Frame Relay Forum (FRF) document FRF.8. And specifications for FR/ATM IWF networks are defined in FRF document FRF.5.

◆ Note ◆

See *ATM and Frame Relay Interworking Services (FRF.8)* on page 38-9 for more information on FR/ATM IWF services and *ATM as a Backbone for Frame Relay Users (FRF.5)* on page 38-2 for more information on FR/ATM IWF networks.

FR/ATM IWF Hardware Support

On the Frame Relay side, Alcatel's FR/ATM IWF software is supported on all OmniSwitch Wide Area Network (WAN) modules (i.e., all switching modules that begin with the prefix WSM) and all Omni Switch/Router WAN modules (i.e., switching modules with the prefix WSX).

On the ATM side, Alcatel's FR/ATM IWF software is supported on all OmniSwitch Cell Switching Modules (CSMs), and OmniSwitch and Omni Switch/Router ATM access module that use the SAHI ASIC (the FCSM-II and modules with the prefix ASM2 on the OmniSwitch and modules with the prefix ASX on the Omni Switch/Router). It is not supported on OmniSwitch ATM access modules that use the Midway ASIC (the FCSM-I and modules with the prefix ASM).

FR/ATM IWF User Interface Commands

User Interface (UI) commands to load the FR/ATM IWF software, to enable and disable FR/ATM IWF, to configure FR/ATM IWF services and networks, and to display statistics for FR/ATM IWF networks and services are described in the sections beginning on page 38-19. You *cannot* monitor or configure FR/ATM IWFs with Command Line Interface (CLI) commands.

◆ Important Note ◆

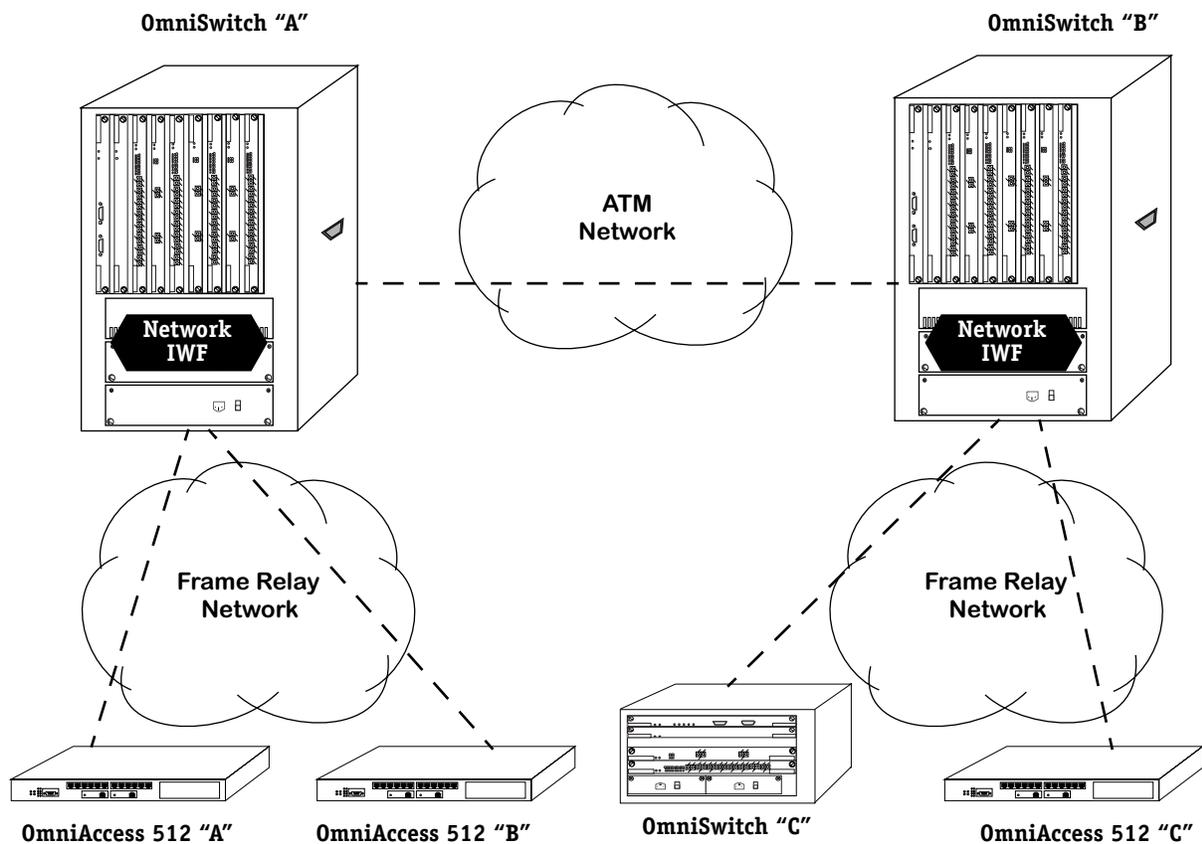
In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory configured to boot up in CLI mode, rather than the UI mode. See Chapter 8, "The User Interface," for documentation on changing from CLI mode to UI mode.

Frame Relay/ATM Internetworking Overview

The sections below describe Frame Relay (FR)/ATM Internetworking Function (IWF) networks (FRF.5) and services (FRF.8). In addition, each section documents the necessary steps to create a sample FR/ATM IWF network or service.

ATM as a Backbone for Frame Relay Users (FRF.5)

The figure below illustrates a sample FR/ATM IWF network. A Frame Relay Permanent Virtual Circuit (PVC) with a Data Link Connection Identifier (DLCI) of 300 connects OmniAccess 512 "A" across a Frame Relay network to WSM Port 1 in Slot 6 on OmniSwitch "A." A Frame Relay PVC with a DLCI of 350 connects OmniAccess 512 "B" across a Frame Relay network to WSM Port 2 in Slot 6 on OmniSwitch "A." An FR/ATM IWF network with a Virtual Path Identifier (VPI)/Virtual Channel Identifier (VCI) of 0/200 on OmniSwitch "A" trunks both Frame Relay PVCs on ASM2 Port 1 in Slot 2 across an ATM network to OmniSwitch "B."



Example of an FR/ATM IWF Network (FRF.5)

On OmniSwitch "B," an FR/ATM IWF network trunks Frame Relay PVCs connected to OmniSwitch "C" and OmniAccess 512 "C" across an ATM network to OmniSwitch "A." In this and all FR/ATM IWF network configurations, the FR/ATM IWF performs all the necessary mapping and encapsulation functions. The PVC status from the ATM layer is used by the Frame Relay Service Specific Convergence Sublayer (FR-SSCS) to determine the status of the Frame Relay PVCs. In the figure above, for example, the FR/ATM IWF network allows OmniAccess 512 "A" and OmniAccess 512 "C" to communicate transparently.

How to Set Up This FR/ATM IWF Network

Follow the steps below to set up the FR/ATM IWF network on OmniSwitch “A” shown in the figure on page 38-2. (The steps for setting up the FR/ATM IWF network on OmniSwitch “B” would be similar.) These steps assume that the **asm.img** image file, **wsm.img**, and any necessary port driver (e.g., **t1e1drv.img**) image files have been loaded and are running on this switch.

Step 1. Load the Frame Relay/ATM Internetworking Software

- a. Load the **frlmi.img** image file into flash memory with FTP or ZMODEM.
- b. To activate the **frlmi.img** image file, either reboot your switch or use the **loadfrlmi** command. To use the **loadfrlmi** command, enter

```
loadfrlmi
```

at the system prompt. Messages similar to the following will be displayed.

```
frlmi.img loaded...  
frlmi.img image loaded ! Task tFrLmiTask spawned successfully !
```

◆ **Note** ◆

See Chapter 9, “Installing Switch Software,” for more information on loading image files.

Step 2. Enable the Frame Relay/ATM Internetworking Software

- a. Enter

```
fratm on
```

at the system prompt. A screen similar to the following will be displayed.

```
FR-ATM Interworking Enabled!
```

◆ **Note** ◆

See *Enabling and Disabling FR/ATM Internetworking Software* on page 38-20 for more information on the **fratm** command.

Step 3. Configure the Frame Relay Ports for Networking

- a. Before a Frame Relay port can be used for FR/ATM IWFs, it must be configured as a network-side (DCE) port. To do this, enter **frmodify** followed by the slot number of the Frame Relay module, a slash (/), and the port number of the Frame Relay module.

In the example on page 38-2, you would modify Ports 1 and 2 on the WSM module in Slot 6. To modify the Frame Relay port No. 1 in Slot 6, enter

frmodify 6/1

at the system prompt. A screen similar to the following will be displayed.

Modify Frame Relay port for Slot: 6, Port: 1.

```

1) Description..... =
   {Enter Up to 30 Characters}
2) Administrative Status ..... = Up
   {(U)p, (D)own}
3) DLCMI Type ..... = ANSI T1.617 Annex D
   {(L)MI Rev. 1.0, T1.617 Annex (D), Q.933 Annex (A), (N)one }
   31) LMI Procedure Type ..... = User
      { (B)idirectional, (U)ser, (N)etwork }
4) Polling Interval T391/nT1 ..... = 10
   {1 through 255 seconds}
5) Full Status Interval N391/nN1 ..... = 6
   {1 through 10}
6) Error Threshold N392/nN2 ..... = 3
   {1 through 10}
7) Monitored Events Counter N393/nN3 ..... = 4
   {1 through 10}
8) Default Bridging Group..... = 1
   {1-65535}
9) Default Frame Relay Bridging Mode..... = Bridge All
   {1=Bridge All, 2=Ethernet only,
   (AN) Bridge All No FCS, (EN) Ethernet Only No FCS}
10) Default Routing Group..... = 0
    {1-65535}
11) Default Compression Admin Status ..... = Enabled
    {(E)nable, (D)isable}
12) Default Compression PRetry Time ..... = 3
    {1-10}
13) Default Compression PRetry Count ..... = 10
    {3-255}

```

To change a value, enter the corresponding number, an '=', and the new value. For example to set a new clocking, use

: 2=i

When complete enter "save" to save all changes, or cancel or Ctrl-C to cancel all changes. Enter ? to view the new configuration.

(save/quit/cancel)

:

- b. Enter

31=n

to configure the port as a network-side port.

- c. Enter

save

to save your settings. Messages similar to the following will be displayed.

**Saving the configuration now....Please wait...
Done.**

- d. Enter

frmodify 6/2

at the system prompt. (See Step **a** on page 38-4 for a sample of the **frmodify** menu screen.)

- e. Enter

31=n

to configure the port as a network-side port.

- f. Enter

save

to save your settings. Messages similar to the following will be displayed.

**Saving the configuration now....Please wait...
Done.**

◆ **Note** ◆

See Chapter 49, “Managing Frame Relay,” for more information on the **frmodify** command.

Step 4. Configure the FR/ATM IWF Network

- a. In the example on page 38-2, you would configure an FR/ATM IWF network with a PVC with a DLCI of 300 on WSM Port 1 in Slot 6, a PVC with a DLCI of 350 on WSM Port 2 in Slot 6, and a PVC with a VPI/VCI of 0/200 on ASM2 Port 1 in Slot 2.

To configure this FR/ATM IWF network, enter **frscvc** followed by the slot number of the Frame Relay module, a slash (/), the port number of the Frame Relay module, a slash (/), and the Frame Relay DLCI number for both Frame Relay ports. (The PVC on the ASM2 module is configured with the **frscvc** command as shown in Step **d** below.) To configure the Frame Relay PVC with a DLCI of 300 on Port No. 1 in Slot 6, enter

frscvc 6/1/300

A screen similar to the following will be displayed.

**Create/Add FR PVC(DLCI) for FR-ATM Interworking
for Slot: 6, Port: 1 DLCI: 300.**

- 1) Service Type { FRF.5(1), FRF.8(2)} = FRF.5
- 2) Outgoing Slot Number = 6
- 3) Outgoing Port Number = 1
- 4) Outgoing VPI {0..3} = 0
- 5) Outgoing VCI {33..1023} = 300
- 51) Outgoing DLCI {16..991} = 300

- 7) Committed Information Rate (CIR) in BPS = 0
{0 through line speed in BPS}
- 8) Committed Burst Rate (Bc) in Bits = 0
{0 through positive number in Bits}
- 9) Excess Burst Size (Be) in Bits = 0
{0 through positive number in Bits}
- 10) Compression Administrative Status = Enabled
{Enabled(1), Disabled(2)}
- 11) Compression PRetry Time in seconds {1..10} = 3
- 12) Compression PRetry Count {3..255} = 10

Option=value/save/cancel :

- b. Enter **2=** followed by the slot number of the ATM port. In the example on page 38-2, you would enter

2=2

at the prompt.

- c. Enter **3=** followed by the port number of the ATM port. In the example on page 38-2, you would enter

3=1

at the prompt.

- d. In the example on page 38-2, you need to create an ATM PVC with a VPI/VCI number of 0/200. The VPI number in this example is already 0 so there is no need to change it. However, you must change the VCI number to 200 in this example. Therefore, you would enter

5=200

at the prompt.

- e. Enter

save

to save your settings. Messages similar to the following will be displayed.

**Validating Configuration...
Saving Valid Configuration... Done !**

- f. Enter

frscvc 6/2/350

at the system prompt to configure the Frame Relay PVC with a DLCI of 350 on Frame Relay Port 2 in Slot 6. (See Step **a** on page 38-6 for a sample **frscvc** menu screen.)

- g. Enter **2=** followed by the slot number of the ATM port. In the example on page 38-2, you would enter

2=2

at the prompt.

- h. Enter **3=** followed by the port number of the ATM port. In the example on page 38-2, you would enter

3=1

at the prompt.

- i. In the example on page 38-2, you need to create an ATM PVC with a VPI/VCI number of 0/200. The VPI number in this example is already 0 so there is no need to change it. However, you must change the VCI number to 200 in this example. Therefore, you would enter

5=200

at the prompt.

- j. Enter

save

to save your settings. Messages similar to the following will be displayed.

**Validating Configuration...
Saving Valid Configuration... Done !**

◆ **Note** ◆

See *Creating an FR/ATM Internetworking Function* on page 38-23 for more information on the optional parameters for the **frscvc** command.

Step 5. Enable the Frame Relay PVC for the FR/ATM IWF Network

- a. If the Frame Relay Permanent Virtual Circuit (PVC) for an FR/ATM IWF network has been disabled, then you need to enable it with the **frsmvc** command. In the example on page 38-2, an FR/ATM IWF network with a Frame Relay PVC with a DLCI of 300 on WSM Port 1 in Slot 6 and a Frame Relay PVC with a DLCI of 350 on WSM Port 2 in Slot 6 are trunked over an ATM PVC with a VPI/VCI of 0/200 on ASM2 Port 1 in Slot 2.

To enable the Frame Relay PVC with a DLCI of 300 on Port 1 in Slot 6, you would enter

```
frsmvc 6/1/300
```

at the prompt. A screen similar to the following will be displayed.

```
Modify Interworked Frame Relay PVC on Slot: 6, Port:1 DLCI: 300.
```

```
Outgoing ATM Slot : 2,   ATM Port : 1
```

```
Outgoing VPI : 0,   VCI : 200, FR-SSCS DLCI : 300
```

```
1) Administrative State {Down(1), Up(2)} ..... = Down  
Option=value/save/cancel :
```

- b. Enter

```
1=2
```

at the prompt to enable this PVC of the FR/ATM IWF network on the Frame Relay side.

- c. Enter

```
save
```

to save your settings.

- d. To enable the Frame Relay PVC with a DLCI of 350 on Port 2 in Slot 6, you would enter

```
frsmvc 6/2/350
```

at the prompt. (See Step **a** above for an example of the **frsmvc** screen.)

- e. Enter

```
1=2
```

at the prompt to enable this PVC of the FR/ATM IWF network on the Frame Relay side.

- f. Enter

```
save
```

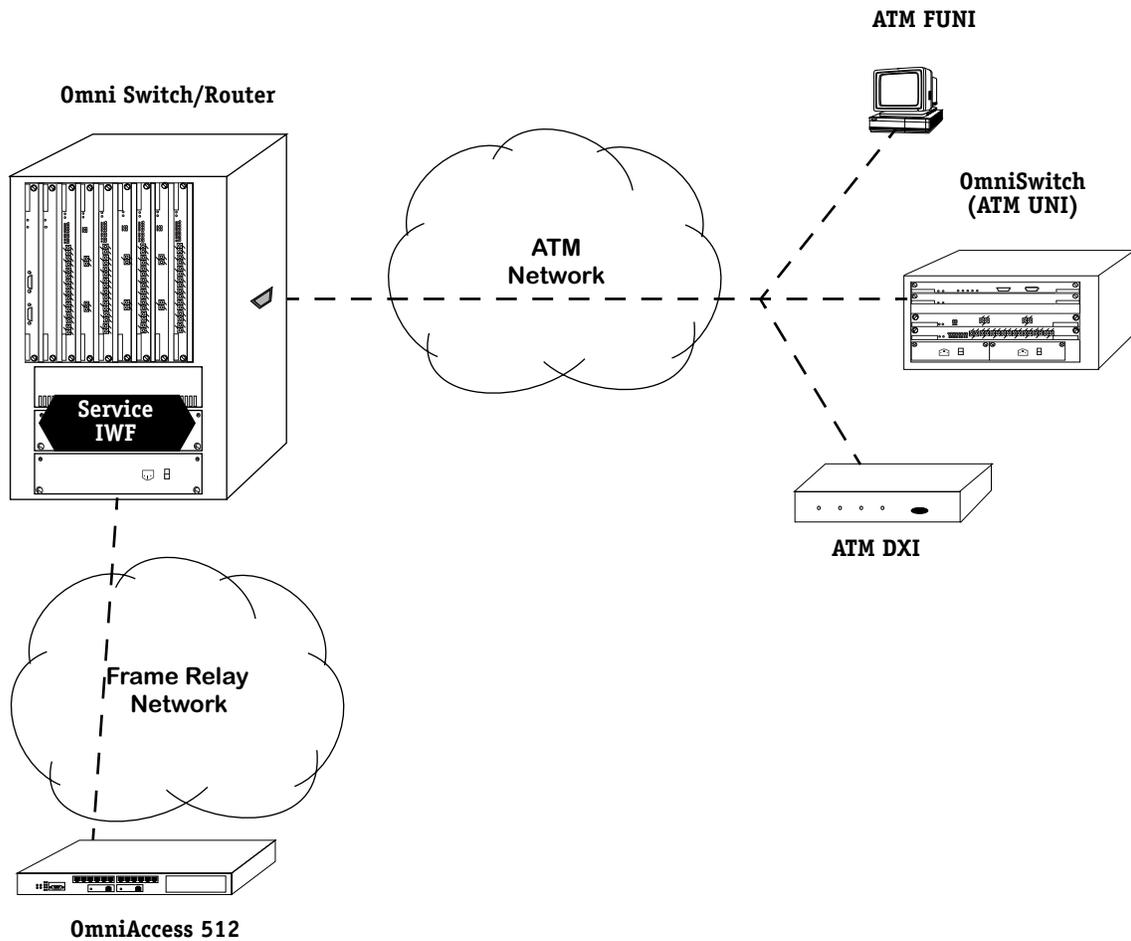
to save your settings.

◆ Note ◆

See *Enabling/Disabling the Frame Relay PVC on an FR/ATM IWF* on page 38-27 for more information on the **frsmvc** command.

ATM and Frame Relay Interworking Services (FRF.8)

The figure below illustrates several sample FR/ATM IWF services. FR/ATM services on the Omni Switch/Router connect to the ATM Frame-based User-to-Network Interface (FUNI), User-to-Network (UNI), and Data Exchange Interface (DXI) devices. In the example below, an FR/ATM IWF service has been configured on the Omni Switch/Router that connects the OmniSwitch and OmniAccess 512 switches. It has a Frame Relay PVC with a DLCI of 200 on WSX Port 1 in Slot 6 and an ATM PVC with a VPI/VCI of 0/200 on ASX Port 1 in Slot 2.



Example of an FR/ATM IWF Service (FRF.8)

FR/ATM IWF services act as protocol converters between Frame Relay and ATM devices. In the Frame-Relay-to-ATM direction, Frame Relay frames are mapped into ATM Adaptation Layer 5 (AAL5) Protocol Data Units (PDUs). As an option, the Frame Relay Discard Eligibility (DE) field can be mapped to ATM Cell Loss Priority (CLP) bits and/or the Frame Relay Forward Explicit Congestion Notification (FECN) field can be mapped to ATM Explicit Forward Congestion Indication (EFCI) bits.

In the ATM-to-Frame-Relay direction, the process is reversed. The message delineation provided by the AAL5 layer is used to identify frame boundaries. You can also map ATM CLP bits to the Frame Relay DE field or EFCI bits to the Frame Relay FECN field.

How to Set Up This FR/ATM IWF Service

Follow the steps below to set up the FR/ATM IWF service that connects the Omni Switch/Router and OmniAccess 512 switches shown in the figure on page 40-8. These steps assume that the **asm.img** image file, **wsx.img**, and any necessary port driver (e.g., **t1e1drv.img**) image file have been loaded and are running on this switch.

Step 1. Load the Frame Relay/ATM Internetworking Software

- a. Load the **frlmi.img** image file into flash memory with FTP or ZMODEM.
- b. To activate the **frlmi.img** image file, either reboot your switch or use the **loadfrlmi** command. To use the **loadfrlmi** command, enter

```
loadfrlmi
```

at the system prompt. Messages similar to the following will be displayed.

```
frlmi.img loaded...  
frlmi.img image loaded ! Task tFrLmiTask spawned successfully !
```

◆ **Note** ◆

See Chapter 9, “Installing Switch Software,” for more information on loading image files.

Step 2. Enable the Frame Relay/ATM Internetworking Software

- a. Enter

```
fratm on
```

at the system prompt. A screen similar to the following will be displayed.

```
FR-ATM Interworking Enabled!
```

◆ **Note** ◆

See *Enabling and Disabling FR/ATM Internetworking Software* on page 38-20 for more information on the **fratm** command.

Step 3. Configure the Frame Relay Port for Networking

- a. Before a Frame Relay port can be used for FR/ATM, it must be configured as a network-side (DCE) port. To do this, enter **frmodify** followed by the slot number of the Frame Relay module, a slash (/), and the port number of the Frame Relay module.

In the example on page 38-9, you would modify Port 1 on the WSX module in Slot 6. To modify the Frame Relay port No. 1 in Slot 6, enter

frmodify 6/1

at the system prompt. A screen similar to the following will be displayed.

Modify Frame Relay port for Slot: 6, Port: 1.

```

1) Description..... =
   {Enter Up to 30 Characters}
2) Administrative Status ..... = Up
   {(U)p, (D)own}
3) DLCMI Type ..... = ANSI T1.617 Annex D
   {(L)MI Rev. 1.0, T1.617 Annex (D), Q.933 Annex (A), (N)one }
   31) LMI Procedure Type ..... = User
      { (B)idirectional, (U)ser, (N)etwork }
4) Polling Interval T391/nT1 ..... = 10
   {1 through 255 seconds}
5) Full Status Interval N391/nN1 ..... = 6
   {1 through 10}
6) Error Threshold N392/nN2 ..... = 3
   {1 through 10}
7) Monitored Events Counter N393/nN3 ..... = 4
   {1 through 10}
8) Default Bridging Group..... = 1
   {1-65535}
9) Default Frame Relay Bridging Mode..... = Bridge All
   {1=Bridge All, 2=Ethernet only,
   (AN) Bridge All No FCS, (EN) Ethernet Only No FCS}
10) Default Routing Group..... = 0
    {1-65535}
11) Default Compression Admin Status ..... = Enabled
    {(E)nable, (D)isable}
12) Default Compression PRetry Time ..... = 3
    {1-10}
13) Default Compression PRetry Count ..... = 10
    {3-255}

```

To change a value, enter the corresponding number, an '=', and the new value. For example to set a new clocking, use

: 2=i

When complete enter "save" to save all changes, or cancel or Ctrl-C to cancel all changes. Enter ? to view the new configuration.

(save/quit/cancel)

:

- b. Enter

31=n

to configure the port as a network-side port.

- c. Enter

save

to save your settings. Messages similar to the following will be displayed.

**Saving the configuration now....Please wait...
Done.**

◆ **Note** ◆

See Chapter 49, “Managing Frame Relay,” for more information on the **frmodify** command.

Step 4. Configure the FR/ATM IWF Service

- a. In the example on page 38-9, you would configure an FR/ATM IWF service with a PVC with a DLCI of 200 on WSX Port 1 in Slot 6 and a PVC with a VPI/VCI of 0/200 on ASX Port 1 in Slot 2.

To configure an FR/ATM IWF service, enter **frscvc** followed by the slot number of the Frame Relay module, a slash (/), the port number of the Frame Relay module, a slash (/), and the Frame Relay DLCI number. (Since the VCI on the ATM side and the DLCI on the Frame Relay side are the same in this example, there is no need to configure the VCI.) To configure this FR/ATM IWF service on Frame Relay port No. 1 in Slot 6, enter

frscvc 6/1/200

at the prompt. A screen similar to the following will be displayed.

**Create/Add FR PVC(DLCI) for FR-ATM Interworking
for Slot: 6, Port: 1 DLCI: 200.**

```
1) Service Type { FRF.5(1), FRF.8(2)} ..... = FRF.5
2) Outgoing Slot Number ..... = 6
3) Outgoing Port Number ..... = 1
4) Outgoing VPI {0..3} ..... = 0
5) Outgoing VCI {33..1023} ..... = 200
   51) Outgoing DLCI {16..991} ..... = 200

7) Committed Information Rate (CIR) in BPS ..... = 0
   {0 through line speed in BPS}
8) Committed Burst Rate (Bc) in Bits ..... = 0
   {0 through positive number in Bits}
9) Excess Burst Size (Be) in Bits ..... = 0
   {0 through positive number in Bits}
10) Compression Administrative Status ..... = Enabled
   {Enabled(1), Disabled(2)}
11) Compression PRetry Time in seconds {1..10} ..... = 3
12) Compression PRetry Count {3..255} ..... = 10
```

Option=value/save/cancel :

- b. To configure an FR/ATM Internetworking service instead of an FR/ATM IWF network, enter

1=2

at the prompt.

- c. Enter **2=** followed by the slot number of the ATM port. In the example on page 38-9, you would enter

2=2

at the prompt.

- d. Enter **3=** followed by the port number of the ATM port. In the example on page 38-9, you would enter

3=1

at the prompt.

◆ **Note** ◆

Since the VCI on the ATM side and the DLCI on the Frame Relay side are the same in this example, there is no need to configure the VCI.

- e. Enter

save

to save your settings. Messages similar to the following will be displayed.

Validating Configuration...
Saving Valid Configuration... Done !

◆ **Note** ◆

See *Creating an FR/ATM Internetworking Function* on page 38-23 for more information on the optional parameters for the **frscvc** command.

Step 5. Enable the Frame Relay PVC for the FR/ATM IWF Service

- a. If the Frame Relay Permanent Virtual Circuit (PVC) for an FR/ATM IWF service has been disabled, then you need to enable it with the **frsmvc** command. In the example on page 38-9, an FR/ATM IWF service with a DLCI of 200 on WSX Port 1 in Slot 6 and an ATM PVC with a VPI/VCI of 0/200 on ASX Port 1 in Slot 2 has been configured. In this example, you would enter

```
frsmvc 6/1/200
```

at the prompt. A screen similar to the following will be displayed.

```
Modify Interworked Frame Relay PVC on Slot: 6, Port:1 DLCI: 200.
```

```
Outgoing ATM Slot : 2,   ATM Port : 1
```

```
Outgoing VPI : 0,   VCI : 200, FR-SSCS DLCI : 200
```

```
1) Administrative State {Down(1), Up(2)} ..... = Down  
Option=value/save/cancel :
```

- b. Enter

```
1=2
```

at the prompt to enable the PVC of the FR/ATM IWF service on the Frame Relay side.

- c. Enter

```
save
```

to save your settings.

◆ Note ◆

See *Enabling/Disabling the Frame Relay PVC on an FR/ATM IWF* on page 38-27 for more information on the **frsmvc** command.

Configuring an FR/ATM IWF on an FCSM-II

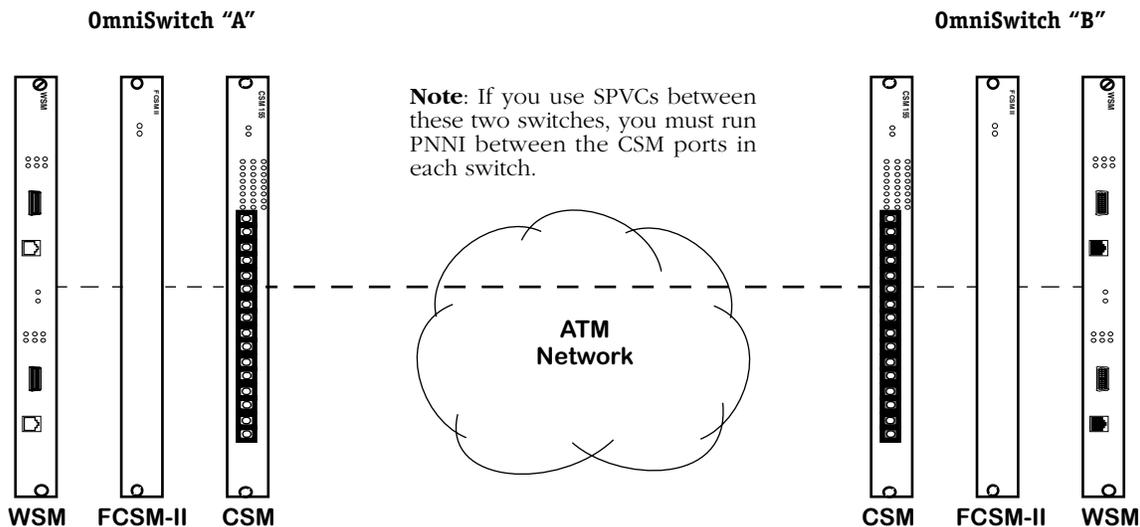
You can configure Frame Relay (FR)/ATM services or networks between WSM modules and FCSM-II modules. However, there are steps you must take to ensure that signaling is activated for Virtual Connections (VCs) on the CSM ports in the switch. See the section below for the required steps.

◆ **Note** ◆

You *cannot* configure an FR/ATM IWF on an FCSM-I.

Sample WSM/FCSM-II Frame Relay/ATM IWF

The figure below shows FR/ATM IWFs with a Data Link Connection Identifier (DLCIs) of 16 and a Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI) of 0/116 configured between WSM Port 5/1 and FCSM-II Port 2/1 on each switch. In addition, an ATM VC — either a Permanent Virtual Circuit (PVC) or a Soft PVC (SPVC) — with a VPI/VCI of 0/116 has been configured on the ingress Port 2/1 on the FCSM-II and the egress Port 7/1 on the CSM modules on both switches.



On OmniSwitch "A," an FR/ATM IWF has been configured on WSM Port 5/1 and FCSM-II Port 2/1, and an ATM VC has been configured with an ingress port on FCSM-II Port 2/1 and an egress port on CSM Port 7/1.

On OmniSwitch "B," an FR/ATM IWF has been configured on WSM Port 5/1 and FCSM-II Port 2/1, and an ATM VC has been configured with an ingress port on FCSM-II Port 2/1 and an egress port on CSM Port 7/1.

FCSM-II and WSM Modules Used in FR/ATM IWFs

Follow the steps in the subsection on the following page to configure this network with PVCs, or follow the steps in described in *How to Set Up This Network with Soft Permanent Virtual Circuits (SPVCs)* on page 38-18 to configure this network with SPVCs. Please note that both procedures assume that the logical ATM ports on the FCSM-IIs (with the **map** command) and the Frame Relay ports (with the **frmodify** command) have been properly configured.

How to Set Up This Network with Permanent Virtual Circuits (PVCs)

1. On OmniSwitch “A,” enter

frscvc 5/1/16

at the system prompt.

2. Enter

2=2

at the **frscvc** prompt to terminate the FR/ATM IWF on the logical ATM port of the FCSM-II.

3. Enter

5=116

at the **frscvc** prompt to set the VCI to 116.

4. Enter any other required parameters. (See *Creating an FR/ATM Internetworking Function* on page 38-23 for more information on the **frscvc** command.)

5. Enter

save

at the **frscvc** prompt to save your settings.

6. Enter

frsmvc 5/1/166

at the system prompt.

7. Enter

1=2

at the **frsmvc** prompt to enable this PVC of the FR/ATM IWF network on the Frame Relay side.

8. Enter

save

to save your settings.

◆ Note ◆

See *Enabling/Disabling the Frame Relay PVC on an FR/ATM IWF* on page 38-27 for more information on the **frsmvc** command.

9. Repeat Steps 1 through 8 on OmniSwitch “B.”

10. On OmniSwitch “A,” enter

cvc 2/1 0/116

at the system prompt. A screen similar to the following will be displayed.

Slot 2 Port 1 Connection VPI 0 VCI 116 Configuration

Available bandwidth: Tx=353208 Rx=353208

- 1) Description (30 chars max) : Connection 116
- 2) Outgoing Slot (1-9) : 2
- 3) Outgoing Port (1-08) : 1
- 4) Outgoing VPI (1-0015) : 0
- 5) Outgoing VCI (1-0255) : 116

- 6) Channel Type { vc-nni(3), vc-uni(4) } : VC-UNI
- 7) Transport Priority { CBR(1), CBR_PRS(2), VBR_RT(3), VBR_NRT(4), ABR(5), UBR(6) } : UBR
- 8) Multicast Enable { disable(0), enable(1) } : Disabled
- 10) AAL5 Discard Continue { disable(0), enable(1) } : Disabled

- 11) Traffic Parameters
- 13) Advanced Parameters

Enter (option=value/save/cancel) :

11. Enter

2=7

at the **cvc** prompt to set the egress port to CSM Port 7/1.

12. Enter any other required parameters. (See Chapter 41, “Managing Cell Switching Modules (CSMs),” for more information on the **cvc** command.)

13. Enter

save

at the **cvc** prompt to save your settings.

14. Repeat Steps 10 through 13 on OmniSwitch “B.”

How to Set Up This Network with Soft Permanent Virtual Circuits (SPVCs)

1. Perform Steps 1 through 9 in *How to Set Up This Network with Permanent Virtual Circuits (PVCs)* on page 38-16.

◆ **Note** ◆

For SPVCs, you need to run PNNI between the CSM ports of the two switches. See Chapter 46, “Configuring and Monitoring PNNI,” for more information on PNNI.

2. On OmniSwitch “A,” enter

scvc 2/1 0/116

at the system prompt. A screen similar to the following will be displayed.

Slot 2 Port 1 Connection VPI 0 VCI 116 Configuration

Available bandwidth: Tx=353209 Rx=353209

- 1) Description (30 chars max) : Connection 116
- 2) End point Id (1..65535) : 1
- 3) Terminating ATM Address : 000000000000000000000000000000000000
- 4) Other End VPI (0..4095) : 1
- 5) Other End VCI (0..65535) : 1
- 6) Channel Type { vc-nni(3), vc-uni(4) } : VC-UNI
- 7) Transport Priority { CBR(1), CBR_PRS(2), VBR_RT(3), VBR_NRT(4), ABR(5), UBR(6) } : UBR
- 8) Point to Multipoint { disable(0), enable(1) } : disabled
- 9) Channel Redirect { not allowed(0), allowed(1) } : not allowed
- 10) AAL5 Discard Continue { disable(0), enable(1) } : enable

- 11) Traffic Parameters
- 13) Advanced Parameters
- 14) Target Selector Type { required(1), any(2) } : required
- 15) SoftPvc Retry parameters
- 16) Broadband Bearer Capability Parameters

Enter (option=value/save/cancel) :

3. Enter **3=** followed by the ATM address of the FCSM-II (the CSM side of the module) of the other OmniSwitch.
4. Enter any other required parameters. (See Chapter 42, “Advanced CSM Management,” for more information on the **scvc** command.)
5. Enter

save

at the **scvc** prompt to save your settings.

6. Perform Steps 1 through 5 above on OmniSwitch “B.”

Dynamically Loading the FR/ATM Image File

You use the **loadfrlmi** command to dynamically load the **frlmi.img** image file, which is required to run Frame Relay (FR)/ATM internetworking software, without rebooting your switch. After you have transferred the **frlmi.img** file to your switch through FTP or ZMODEM, enter

```
loadfrlmi
```

at the prompt. Messages similar to the following will be displayed.

```
frlmi.img loaded...  
frlmi.img image loaded ! Task tFrLmiTask spawned successfully !
```

◆ **Note** ◆

See Chapter 9, “Installing Switch Software,” for more information on loading image files with ZMODEM or FTP.

Enabling and Disabling FR/ATM Internetworking Software

The **fratm** command can be used to enable Frame Relay (FR)/ATM Internetworking, disable FR/ATM Internetworking, and show the status of FR/ATM internetworking software. The syntax for this command is as follows:

```
fratm [on | off]
```

The subsection below describe the three ways the **fratm** command can be used.

Displaying the Status of FR/ATM Internetworking

To display whether FR/ATM internetworking has been enabled or are disabled, enter

```
fratm
```

at the system prompt. The following status information will be displayed.

```
Usage: fratm status  
status "on" - To Enable FR-ATM interworking  
status "off" - To Disable FR-ATM interworking
```

Enabling FR/ATM Internetworking

To enable the FR/ATM internetworking, enter

```
fratm on
```

at the system prompt. After a few seconds, a screen similar to the following will be displayed.

```
FR-ATM Interworking Enabled!
```

Disabling FR/ATM Internetworking

To disable the FR/ATM internetworking, enter

```
fratm off
```

at the system prompt. No confirmation message is displayed.

The Frame Relay/ATM Internetworking Submenu

The Frame Relay (FR)/ATM internetworking commands are contained within the **frs** submenu, which is part of the **interface** menu. In addition, the **fratm** command (described in *Enabling and Disabling FR/ATM Internetworking Software* on page 38-20) and the **loadfrlmi** command (described in *Dynamically Loading the FR/ATM Image File* on page 38-19) are also part of the **interface** submenu.

To enter the **interface** menu, enter

interface

at the system prompt. Enter a question mark (?) to display the **interface** menu, as shown below.

Command	Physical Interface Menu
slipc	Configure SLIP (Serial Line IP) on a TTY Port
eth100	Enter the 100BaseT sub-menu
10/100	Enter the 10/100BaseT sub-menu
sonet	Enter Sonet Sub-Menu
fratm	Enable/Disable FR-ATM Interworking
loadfrlmi	Load/Enable Standalone Frame Relay LMI
atm	Enter the ATM Management sub-menu
wan	Enter the Wide Area Networking submenu.
backup	Enter Backup networking command submenu
frs	Enter the FR-ATM Interworking submenu
ds3	Enter DSX3 Port Management sub-menu
te	Enter T1/E1 Port Management sub-menu

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

To enter the **frs** submenu, enter

frs

at the system prompt. Enter a question mark (?) to display the **frs** submenu commands, as shown below.

Command	FR-ATM Interworking / FR Switching Menu
frscvc	Create/add FR PVC(DLCI) for FR-ATM Interworking
frsdvc	Delete an FR PVC from an FR-ATM FRF.5 Interworking
frsmvc	Modify FR PVC for FR-ATM Interworking
frsmc	Modify FR-ATM Interworking Function configuration
frsdvc	Delete FR-ATM Interworking Function
frsvc	View FR-ATM Interworking Function configuration
frsvs	View FR-ATM Interworking Function statistics

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

The Frame Relay/ATM Internetworking Submenu

The commands in the **frs** submenu are described in the sections that follow:

- **frscvc** This command is described in *Creating an FR/ATM Internetworking Function* on page 38-23.
- **frsdvc** This command is described in *Deleting FR/ATM PVCs on a Port* on page 38-36.
- **frsmvc** This command is described in *Enabling/Disabling the Frame Relay PVC on an FR/ATM IWF* on page 38-27.
- **frsmc** This command is described in *Modifying an FR/ATM Internetworking Function* on page 38-28.
- **frsdc** This command is described in *Deleting the FR/ATM Internetworking Function on a Port* on page 38-35.
- **frsvc** This command is described in *Displaying FR/ATM IWF Configurations* on page 38-37.
- **frsvs** This command is described in *Displaying FR/ATM IWF Statistics* on page 38-42.

Creating an FR/ATM Internetworking Function

You use the **frscvc** command to create a Frame Relay (FR)/ATM Internetworking Function (IWF). The syntax for this command is as follows:

frscvc <frame relay slot>/<frame relay port>/<DLCI>

For example, to create an FR/ATM IWF with a Data Link Connection Identifier (DLCI) of 300 on Frame Relay Port 1 in Slot 6, enter

frscvc 6/1/300

at the system prompt. A screen similar to the following will be displayed.

```

Create/Add FR PVC(DLCI) for FR-ATM Interworking
for Slot: 6, Port: 1 DLCI: 300.

1) Service Type { FRF.5(1), FRF.8(2)} ..... = FRF.5
2) Outgoing Slot Number ..... = 6
3) Outgoing Port Number ..... = 1
4) Outgoing VPI {0..3} ..... = 0
5) Outgoing VCI {33..1023} ..... = 300
   51) Outgoing DLCI {16..991} ..... = 300

7) Committed Information Rate (CIR) in BPS ..... = 0
   {0 through line speed in BPS}
8) Committed Burst Rate (Bc) in Bits ..... = 0
   {0 through positive number in Bits}
9) Excess Burst Size (Be) in Bits ..... = 0
   {0 through positive number in Bits}
10) Compression Administrative Status ..... = Enabled
    {Enabled(1), Disabled(2)}
11) Compression PRetry Time in seconds {1..10} ..... = 3
12) Compression PRetry Count {3..255} ..... = 10
  
```

Option=value/save/cancel :

Select the number of the item you want to change. To change any of the values listed above, enter the line number, followed by an equal sign, and then the new value. For example, to set the outgoing VCI number to 100, enter

5=100

at the prompt. To update the values you have changed, enter **save**. If you do not want to save the changes enter **quit** or **cancel**, or press **Ctrl-D**. If your changes have been successfully made, the following confirmation messages will be displayed.

```

Validating Configuration...
Saving Valid Configuration... Done !
  
```

The configurable parameters in the **frscvc** command are described on the following pages.

1) Service Type

Enter **1=1** (the default) to create an FR/ATM IWF network (FRF.5) or **1=2** to create an FR/ATM IWF service (FRF.8). See *ATM as a Backbone for Frame Relay Users (FRF.5)* on page 38-2 for more information on FRF.5 networks and *ATM and Frame Relay Interworking Services (FRF.8)* on page 38-9 for more information on FRF.8 services.

◆ Important Note ◆

On an FRF.5 network only, you can map several Frame Relay PVCs to a single ATM virtual channel (VPI/VCI). This *cannot* be done on an FRF.8 service.

2) Outgoing Slot Number

Enter the slot number of the ATM port for this FR/ATM IWF.

3) Outgoing Port Number

Enter the port number of the ATM port for this FR/ATM IWF.

If the outgoing port is an FCSM-II port, then you will need to create an ATM VCC (either a an ATM PVC or Soft PVC) the FCSM-II port and a CSM port. To create a PVC, use the **cvc** command, which is described in Chapter 41, “Managing Cell Switching Modules (CSMs).” To create a Soft PVC, use the **scvc** command, which is described in Chapter 42, “Advanced CSM Management.”

◆ Note ◆

See *Sample WSM/FCSM-II Frame Relay/ATM IWF* on page 38-15 for more information on configuring an FR/ATM IWF on an FCSM-II.

4) Outgoing VPI

Enter the Virtual Path Identifier (VPI) of the ATM port for this FR/ATM IWF. The valid range is displayed between the brackets.

5) Outgoing VCI

Enter the Virtual Channel Identifier (VCI) of the ATM port for this FR/ATM IWF. The valid range is displayed between the brackets.

51) Outgoing DLCI

Enter the outgoing Data Link Connection Identifier (DLCI) of the Frame Relay port for this FR/ATM IWF. The valid range is displayed between the brackets.

◆ Important Note ◆

The outgoing DLCI is only valid for an FRF.5 network. You *cannot* set the outgoing DLCI on an FRF.8 service.

7) Committed Information Rate (CIR) in BPS

Enter the Committed Information Rate (CIR) of the Frame Relay port for this FR/ATM IWF in bits per second (BPS).

8) Committed Burst Size (Bc) in Bits

Enter the Committed Burst Size (Bc) of the Frame Relay port for this FR/ATM IWF in bits. The Committed Burst Size is the amount of data that the network will guarantee to transfer under normal conditions.

9) Excess Burst Size (Be) in Bits

Enter the Excess Burst Size (Be) for this FR/ATM IWF in bits. The Excess Burst Size is the amount of data over-and-above the Committed Burst Size (Bc) that the network will transmit as long as excess bandwidth is available.

10) Compression Administrative State

Enter **10=1** (the default) to enable the Compression Administrative State (as defined in the Frame Relay Forum *Data Compression Implementation Agreement*, (FRF.9)) or **10=2** to disable it for this FR/ATM IWF.

◆ Note ◆

The compression administrative state only applies to the Frame Relay link and not to the ATM port.

This field enables and disables compression negotiation for this FR/ATM IWF. If set to enable, then the Frame Relay port will query the bridge/router on the other end of the Frame Relay link as to whether it supports compression. Compressed data will be sent only when the other bridge/router also supports compression. If the bridge/router on the other end is an OmniSwitch or Omni Switch/Router, then data would be sent compressed as long as you set the Compression Administrative State to Enabled.

Disabling Compression Administrative State means that data will not be sent compressed even if the other Bridge/Router supports compression. Data compression is always negotiated before it is activated.

11) Compression PRetry Time in seconds

Enter the compression PRetry time for this FR/ATM IWF in seconds. The valid range is displayed between the brackets.

◆ Note ◆

The compression PRetry time only applies to the Frame Relay link and not to the ATM port.

This option sets the number of seconds between compression negotiation messages on this FR/ATM IWF. If compression negotiation is enabled, the Frame Relay port will send compression negotiation messages as many times as you indicate in the **Compression PRetry Count**. The time between these tries is indicated in this field. The number of seconds between retries may range between 1 and 10 seconds. The default is 3 seconds. The value you enter for this field overrides the **Default Compression PRetry Time** set up for the physical port with which this virtual circuit is associated.

◆ Important Note ◆

The Compression PRetry Time should only be modified by experienced Frame Relay network administrators. In addition, it should match the setting for the remote switch or bridge/router.

12) Compression PRetry Count

Enter the compression PRetry count for this FR/ATM IWF in seconds. The valid range is displayed between the brackets.

◆ Note ◆

The compression PRetry count only applies to the Frame Relay link and not to the ATM port.

This option sets the total number of compression negotiation messages that will be sent before giving up and not running compression on this FR/ATM IWF. You enter the time between these retries in the **Compression PRetry Time** field. The number of retries can range from 3 to 255. The default is 10. The value you enter for this field overrides the **Default Compression PRetry Count** set up for the physical port with which this virtual circuit is associated.

◆ Important Note ◆

The Compression PRetry Count should only be modified by experienced Frame Relay network administrators. In addition, it should match the setting for the remote switch or bridge/router.

Enabling/Disabling the Frame Relay PVC on an FR/ATM IWF

If the Frame Relay (FR) Permanent Virtual Circuit (PVC) link in an FR/ATM Interworking Function (IWF) network (FRF.5) or service (FRF.8) is disabled, then the Frame Relay Service Specific Convergence Sublayer (FR-SSCS) DLCI of the corresponding Frame Relay PVC in the FR/ATM network or service will also be down. You use the **frsmvc** command to enable or disable the Frame Relay PVC on the Frame Relay link for an existing FR/ATM IWF. The syntax for this command is as follows:

```
frsmvc <frame_relay_slot>/<frame_relay_port>/ <dcli>
```

For example, to administratively enable an FR/ATM IWF with a Data Link Connection Identifier (DLCI) of 300 on Frame Relay Port 1 in Slot 6, enter

```
frsmvc 6/1/300
```

at the system prompt. A screen similar to the following will be displayed.

```
Modify Interworked Frame Relay PVC on Slot: 6, Port:1 DLCI: 300.
```

```
Outgoing ATM Slot : 2,   ATM Port : 1
```

```
Outgoing VPI : 0,   VCI : 300, FR-SSCS DLCI : 300
```

```
1) Administrative State {Down(1), Up(2)} ..... = Up  
Option=value/save/cancel :
```

Enter **1=1** to disable the PVC on the Frame Relay link for the FR/ATM IWF or **1=2** (the default) to enable it.

Modifying an FR/ATM Internetworking Function

You use the **frsmc** command to modify an existing Frame Relay (FR)/ATM Internetworking Function (IWF). The syntax for this command is as follows:

```
frsmc <atm_slot>/<atm_port> <vpi>/ <vci>
```

For example, to modify FR/ATM IWF with a Virtual Path Identifier (VPI)/Virtual Channel Identifier (VCI) of 0/300 on ATM Port 1 in Slot 2, enter

```
frsmc 2/1 0/200
```

at the system prompt. A screen similar to the following will be displayed.

```
FRF.5 IWF Configuration for Slot 2 Port 1 Connection 0/200

1) Description (30 chars max.) ..... : Connection 0/200
2) ATM Traffic Parameters
3) DE-CLP Mapping { Enabled(1), Disabled(2) } ..... : Enabled
   31) Default CLP Value { CLP=0(1), CLP=1(2) }..... : CLP=0
4) Congestion Notification Mapping ..... : Enabled
   { Enabled(1), Disabled(2) }
5) Upper Layer Protocol Encapsulation Mapping ..... : Enabled
   { Enabled(1), Disabled(2) }
   51) Encapsulation Mode ..... : Translation
       { Translation(1), Transparent(2) }
6) Administrative Status { Down(1), Up(2) } ..... : Up

7) LIV Polling Interval T391 (in secs) { 5..30 } ..... : 180
8) Full Status Polling Counter N391 { 1..255 } ..... : 1
9) User Error Threshold Counter N392 { 1..10 } ..... : 3
10) User Monitored Events Counter N393 { 1..10 } ..... : 4
11) Network Poll Verification Interval T392 ..... : 20
    (in secs) { 5.. 30 }
12) Network Error Threshold Counter N392 {1..10} ..... : 3
13) Network Monitored Events Counter N393 {1..10} ..... : 4

Enter (option=value/save/cancel) :
```

◆ Important Note ◆

Options 7 (LIV Polling Interval T391) through 13 (Network Monitored Events Counter N393) will *not* be displayed if you are modifying an FR/ATM IWF service (FRF.8).

Select the number of the item you want to change. To change any of the values listed above, enter the line number, followed by an equal sign, and then the new value. For example, to change the connection's description to **FR-ATM Connection 0/300**, enter

```
1=FR-ATM Connection 0/300
```

at the prompt. To update the values you have changed, enter **save**. If you do not want to save the changes enter **quit** or **cancel**, or press **Ctrl-D**. If you enter **save**, the following confirmation prompt will be displayed.

```
Connection 200 is in use, reset connection (n) ? : y
```

Enter **y** to confirm any changes you have made or enter **n** to discard them. If your changes have been successfully made, a message similar to the following will be displayed

```
Connection being disabled and re-enabled with new parameters...
```

The configurable parameters in the **frsmc** command are described below.

1) Description

Enter **1=** followed by a text description up to 30 characters long.

2) ATM Traffic Parameters

Enter **2** to enter the ATM parameter modification submenu, which is described in *Modifying ATM Parameters on a FR/ATM Internetworking Function* on page 38-32.

3) DE-CLP Mapping

Enter **3=1** to enable Frame Relay Discard Eligibility (DE) flag to ATM Cell Loss Priority (CLP) bit mapping (the default) or **3=2** to disable it.

If DE-CLP mapping is enabled, then the DE field in the Q.922 core frame shall be copied unchanged into the DE field in the FR-SSCS PDU header and mapped to the ATM CLP of every ATM cell generated by the segmentation process of that frame in the Frame Relay to ATM direction. In the ATM to Frame Relay direction, if one or more ATM cells belonging to a frame has its CLP field set to **1** or if the DE field of the FR-SSCS PDU is set to **1**, the FR/ATM IWF shall set the DE field of the Q.922 core frame.

If DE-CLP mapping is disabled, then the DE field in the Q.922 core frame shall be copied unchanged into the DE field in the FR-SSCS PDU header and the ATM CLP of every ATM cell generated by the segmentation process of that frame shall be set to a constant value (either **0** or **1**) in the Frame Relay to ATM direction. In the ATM to Frame Relay direction, no mapping is performed from the ATM layer to Q.922 core layer. The FR-SSCS PDU DE field is copied unchanged to the Q.922 core frame DE field, independent of CLP indications(s) received at the ATM layer.

31) Default CLP Value

If Frame Relay DE flag to ATM CLP bit mapping has *not* been enabled, enter **31=1** to set the ATM Cell Loss priority (CLP) to 0 or enter **31=2** to set it to 1.

4) Congestion Notification Mapping

Enter **4=1** to enable Frame Relay Forward Explicit Congestion (FECN) to ATM Explicit Forward Congestion Indication (EFCI) bit mapping (the default) or **4=2** to disable it.

If congestion notification mapping is enabled, the FECN field in the Q.922 core frame shall be mapped to the ATM EFCI field of every cell generated by the segmentation process of the AAL5 PDU containing the information of that frame in the Frame Relay to ATM direction. This method provides congestion indication to the end points where higher level protocol entities might be involved in traffic control mechanisms.

If congestion notification mapping is disabled, then the FECN field in the Q.922 core frame shall not be mapped to the ATM EFCI field of cells generated by the segmentation process of the AAL5 PDU containing the information of that frame in the Frame Relay to ATM direction. The EFCI field is always set to “congestion not experienced.”

In the ATM to Frame Relay direction, if the EFCI field in the last cell of a segmented frame received is set to “congestion experienced,” then the FR/ATM IWF shall set the FECN of the Q.922 Core frame to “congestion experienced.”

5) Upper Layer Protocol Encapsulation Mapping

Enter **5=1** to enable Upper Layer Protocol (ULP) encapsulation (the default), or **5=2** to disable it.

◆ **Note** ◆

See the Frame Relay Forum *Multiprotocol Encapsulation Agreement*, (FRF.3), for more information on Frame Relay encapsulation methods.

51) Encapsulation Mode

If Frame Relay ULP encapsulation mapping has been enabled, enter **51=1** to set the encapsulation method to translation (the default), where the Frame Relay upper layer protocols will be encapsulated according to FRF.3 and the ATM upper layer protocols will be encapsulated according to RFC 1483, or enter **51=2** to set it to transparent, where upper layer encapsulation methods will be unaltered.

In transparent mode, upper layer encapsulation methods will not work unless the end terminal equipment is compatible on the near and far side of the links.

6) Administrative Status

Enter **6=1** to disable the this FR/ATM IWF or enter **6=2** (the default) to enable it.

7) LIV Polling Interval T391

Enter **7=** followed by the user-side T391 integrity verification polling timer value in seconds for this port. The valid range is displayed between brackets.

◆ **Note** ◆

The LIV Polling Interval T391 is only valid on FRF.5 networks and therefore is not displayed nor configurable on FRF.8 services.

8) Full Status Polling Counter N391

Enter **8=** followed by the user-side N391 full status polling cycle value for this port. The valid range is displayed between brackets.

◆ **Note** ◆

The Full Status Polling Counter N391 is only valid on FRF.5 networks and therefore is not displayed nor configurable on FRF.8 services.

9) User Error Threshold Counter N392

The number of DLCMI protocol errors that will be tolerated before determining the Frame Relay line is down and all associated virtual circuits are inactive. These errors may include timeouts from STATUS ENQUIRY polls and invalid STATUS messages returned from the Frame Relay network.

Enter **9=** followed by the user-side N392 error threshold value for this port. The valid range is displayed between brackets.

◆ **Note** ◆

The User Error Threshold Counter N392 is only valid on FRF.5 networks and therefore is not displayed nor configurable on FRF.8 services.

10) User Monitored Events Threshold Counter N393

The number of status polling intervals over which the **User Error Threshold N392** is counted. This value should be greater than or equal to the **User Error Threshold N392**. If the station received the number of errors specified in **User Error Threshold N392** within the number of polling intervals specified for the **User Monitored Events Threshold Counter N393**, then the Frame Relay line is considered down and all associated virtual circuits are considered inactive.

Enter **10=** followed by the user-side N393 monitored events count value for this port. The valid range is displayed between brackets.

◆ **Note** ◆

The User Monitored Events Threshold Counter N393 is only valid on FRF.5 networks and therefore is not displayed nor configurable on FRF.8 services.

11) Network Poll Verification Interval T392

Enter **11=** followed by the network-side T392 polling verification timer value in seconds for this port. The valid range is displayed between brackets.

◆ **Note** ◆

The Network Poll Verification Interval T392 is only valid on FRF.5 networks and therefore is not displayed nor configurable on FRF.8 services.

12) Network Error Threshold Counter N392

Enter **12=** followed by the network-side N392 error threshold value for this port. The valid range is displayed between brackets.

◆ **Note** ◆

The Network Poll Verification Interval T392 is only valid on FRF.5 networks and therefore is not displayed nor configurable on FRF.8 services.

13) Network Error Threshold Counter N393

Enter **12=** followed by the network-side N393 monitored events count value for this port. The valid range is displayed between brackets.

◆ **Note** ◆

The Network Poll Verification Interval T392 is only valid on FRF.5 networks and therefore is not displayed nor configurable on FRF.8 services.

Modifying ATM Parameters on a FR/ATM Internetworking Function

When you select option 2 from the main **frsmc** menu, a submenu to the following will be displayed:

ATM Traffic Parameters for FRF.5 IWF Connection 0/200

Available bandwidth: Tx = 81056 Rx = 81056

- 1) Tx QoS Class { Unspecified(0) } : Unspecified
- 2) Tx Best Effort { False(1), True(2) } : False
- 3) Tx Traffic Descriptor { NoCLPNoSCR(2) } : NoCLP NoSCR
 - 20) Peak Cell Rate (cells/sec) for CLP=0+1 : 81056
- 4) Rx QoS Class { Unspecified(0) } : Unspecified
- 5) Rx Traffic Descriptor { NoCLPNoSCR(2) } : NoCLP NoSCR
 - 30) Peak Cell Reate (cells/sec) for CLP=0+1 : 81056
- 11) Tx Maximum Frame Size : 8192
- 12) Rx Maximum Frame Size : 8192

Enter (option=value/save/cancel) :

Select the number of the item you want to change. To change any of the values listed above, enter the line number, followed by an equal sign, and then the new value. For example, to set the Tx Best Effort to False, enter

2=1

at the prompt. To update the values you have changed, enter **save**. If you do not want to save the changes enter **quit** or **cancel**, or press **Ctrl-D**. When you exit this submenu you will return to the main **frsmc** menu, which is described in *Modifying an FR/ATM Internetworking Function* on page 38-28.

The configurable parameters in this submenu are described below.

1) Tx QoS Class

The Quality of Service (QoS) for cells transmitted (from source to destination) on this port. For ATM uplink connections to an ATM switch, only the **Unspecified** QoS is supported. This QoS transmits data on a best effort basis; bandwidth is not guaranteed, but as much data as possible will be transmitted as long as bandwidth is available.

2) Tx Best Effort

This field indicates whether you want this port to transmit traffic on a “best effort” basis or to use a Peak Cell Rate (PCR) parameter to transmit traffic. If you select True (option **2**), then the port will transmit traffic if any bandwidth is available on the port. If you select False (option **1**), then the Peak Cell Rate (PCR) parameter will be used to transmit traffic on this VCC. You enter a PCR value in option 20 of this screen. If data cannot be sent at the PCR you specify, then no data will be sent on the Virtual Channel Connection (VCC).

3) Tx Traffic Descriptor

The traffic descriptor to be used. The traffic descriptor determines which traffic parameters you specify. Only the **NoCLPNoSCR** traffic descriptor is supported. **NoCLPNoSCR** requires you to enter the Peak Cell Rate (PCR) on option 20. However, if you select **True** on option 2 (**Tx Best Effort**), then the PCR will not be used to determine traffic flow, and traffic will be transmitted on a best effort basis.

20) Peak Cell Rate (cells/sec) for CLP=0+1

This value is only relevant if you enter **False** on option 2, **Tx Best Effort**. In this field you specify the Peak Cell Rate (PCR), in cells per second, allowed for traffic transmitted on this VCC. The PCR is the fastest cell rate allowed on the connection. When using Peak Cell Rate, the bandwidth of an ATM uplink port can be partitioned among multiple connections each with a dedicated bandwidth. The ATM driver calculates the best rate nearest to the requested rate that the ATM hardware can support. This rate is shown using the **vvcc** command, which is described in Chapter 33, "Managing ATM Access Modules," for ATM uplink ports and Chapter 41, "Managing Cell Switching Modules (CSMs)," for CSM ports.

The CLP=0+1 in this field means that both high priority (CLP=0) and low priority (CLP=1) cells will be checked for PCR. See Chapter 41, "Managing Cell Switching Modules (CSMs)," for further information on CLP (Cell Loss Priority).

4) Rx Qos Class

The Quality of Service (QoS) for cells received (from destination to source) on this FR/ATM IWF. For ATM uplink connections to an ATM switch only the **Unspecified** QoS is supported. This QoS receives data on a best effort basis; bandwidth is not guaranteed, but as much data as possible will be received as long as bandwidth is available.

5) RX Traffic Descriptor

The traffic descriptor to be used. Only the **NoCLPNoSCR** traffic descriptor is supported. **NoCLPNoSCR** requires you to enter the Peak Cell Rate (PCR) on option 20. However, if you select **True** on option 5 (**Rx Best Effort**), then the PCR will not be used to determine traffic flow, and traffic will be received on a best effort basis.

30) Peak Cell Rate (cells/sec) for CLP=0+1

This value is only relevant if you enter **False** on option 5, **Rx Best Effort**. In this field, you specify the Peak Cell Rate (PCR) in cells per second, allowed for traffic received on this VCC. The PCR is the fastest cell rate allowed on the connection. When using PCR, the bandwidth of an ATM uplink port can be partitioned among multiple connections each with dedicated bandwidth. The ATM driver calculates the best rate nearest to the requested rate that the ATM hardware can support. This rate is shown using the **vvcc** command. The CLP=0+1 in this field means that both high priority (CLP=0) and low priority (CLP=1) cells will be checked for PCR.

11) Tx Maximum Frame Size

The maximum frame size for traffic transmitted on this connection. Frames are composed of ATM cells. You specify the largest possible frame size (in bytes) in this field. If a frame exceeds this size, it will be discarded and counted as an error in statistics tables. The value in this field must be greater than zero (0), but less than the **Tx Frame Buffer Size**.

12) Rx Maximum Frame Size

The maximum frame size for traffic received on this connection. Frames are composed of ATM cells. You specify the largest possible frame size (in bytes) in this field. If a frame exceeds this size, it will be discarded and counted as an error in statistics tables. The value in this field must be greater than zero (0), but less than the **Rx Frame Buffer Size**.

Deleting the FR/ATM Internetworking Function on a Port

You use the **frsdc** command to delete a Frame Relay (FR)/ATM Internetworking Function (IWF) on a port. The syntax for this command is as follows:

```
frsdc <atm_slot>/<atm_port> <vpi>/<vci>
```

For example, to delete the FR/ATM IWF with a Virtual Path Identifier (VPI) of 0 and Virtual Channel Identifier (VCI) of 200 on ATM Port 1 in Slot 2, enter

```
frsdc 2/1 0/200
```

at the system prompt. A screen similar to the following will be displayed.

```
Delete FR-ATM FRF.5 IWF on Slot 2 Port 1 VPI 0 VCI 200 (n) ?
```

Enter **y** to delete the FR/ATM IWF on the port or enter **n** (the default) to exit the command. If you entered **y**, a confirmation message similar to the following will be displayed.

```
Deleting FR-ATM Connection ....Done.
```

Deleting FR/ATM PVCs on a Port

You use the **frsdvc** command to delete one or more Frame Relay (FR)/ATM Data Link Connection Identifier (DLCI) Permanent Virtual Circuits (PVCs) on a single port. The syntax for this command is as follows:

```
frsdvc <frame_relay_slot>/< frame_relay_port> [/<dldci>]
```

To delete all FR/ATM PVCs on a port, see the subsection below. To delete a single FR/ATM PVC, see *Deleting One FR/ATM PVC on a Port* on page 38-36.

Deleting All FR/ATM PVCs on a Port

To delete all FR/ATM PVCs on a port, enter **frsdvc** followed by the slot number of the Frame Relay port, a slash (/), and the port number of the Frame Relay port. For example, to delete all FR/ATM PVCs on Frame Relay Port 1 in Slot 6, enter

```
frsdvc 6/1
```

at the system prompt. A screen similar to the following will be displayed

Slot	Port	DLCI	Slot	Port	VPI	VCI	PVC Type
----	----	-----	----	----	---	---	-----
6	1	200	2	1	0	200	INTERWORKED
6	1	300	2	1	0	300	INTERWORKED

Delete FR-ATM DLCIs on Slot 6 Port 1 (n)? :

Enter **y** to delete all the FR/ATM PVCs or enter **n** (the default) to exit the command. If you entered **y**, a confirmation message similar to the following will be displayed.

```
Deleted all FR-ATM DLCIs on Slot 6 Port 1.
```

Deleting One FR/ATM PVC on a Port

To delete a single FR/ATM PVC on a port, enter **frsdvc** followed by the slot number of the Frame Relay port, a slash (/), the port number of the Frame Relay port, a slash (/), and the DLCI number of the PVC. For example, to delete the FR/ATM PVC with a DLCI number of 300 on Frame Relay Port 1 in Slot 6, enter

```
frsdvc 6/1 /300
```

at the system prompt. A screen similar to the following will be displayed

Slot	Port	DLCI	Slot	Port	VPI	VCI	PVC Type
----	----	-----	----	----	---	---	-----
6	1	300	2	1	0	300	INTERWORKED

Delete FR-ATM DLCI 300 on Slot 6 Port 1 (n)? :

Enter **y** to delete all the FR/ATM PVCs or enter **n** (the default) to exit the command. If you entered **y**, a confirmation message similar to the following will be displayed.

```
Deleted FR-ATM DLCI 300 on Slot 6 Port 1.
```

Displaying FR/ATM IWF Configurations

You use the **frsvc** command to display the Frame Relay (FR)/ATM Internetworking Function (IWF) configurations on an entire switch, on a single port, or for a single FR/ATM IWF. The syntax for the command is as follows:

```
frsvc [<atm_slot>/<atm_port>[<vpi>/<vci>]]
```

See the subsection below to display all FR/ATM PVCs on a switch. See *Displaying the Configurations of All FR/ATM IWFs on a Port* on page 38-38 to display all FR/ATM PVCs on a port. And see *Displaying the Detailed Configuration of a Single FR/ATM IWF* on page 38-39 to display a detailed configuration of a single FR/ATM PVC on a switch.

Displaying the Configurations of All FR/ATM IWFs on a Switch

To display the configurations of all FR/ATM IWFs on a switch, enter

```
frsvc
```

at the system prompt. A screen similar to the following will be displayed.

FR-ATM IWF Connections							
Slot	Port	VPI	VCI	Slot	Port	DLCI	IWF Type
----	----	----	----	----	----	-----	-----
4	1	0	200	2	1	100	Network (FRF.5)
4	1	0	200	2	1	102	Network (FRF.5)
4	2	0	400	3	3	120	Service (FRF.8)
6	1	0	800	5	1	300	Network (FRF.5)
6	1	0	800	3	2	310	Network (FRF.5)

The fields displayed by the **frsvc** command for an entire switch are described below

Slot. The first slot number displayed is the slot number of the ATM port for this FR/ATM IWF.

Port. The first port number displayed is the port number of the ATM port for this FR/ATM IWF.

VPI. The ATM Virtual Path Identifier (VPI) of this FR/ATM IWF.

VCI. The ATM Virtual Channel Identifier (VCI) of this FR/ATM IWF.

Slot. The second slot number displayed is the slot number of the Frame Relay port for this FR/ATM IWF.

Port. The second port number displayed is the port number of the Frame Relay port for this FR/ATM IWF.

DLCI. The Frame Relay Data Link Connection Identifier (DLCI) of this FR/ATM IWF.

IWF Type. The FR/ATM Internetworking Function (IWF) type. This will display **Network (FRF.5)** if this FR/ATM IWF is an FR/ATM IWF network, or **Service (FRF.8)** if this FR/ATM IWF is an FR/ATM IWF service.

Displaying the Configurations of All FR/ATM IWFs on a Port

To display the configurations of all FR/ATM IWFs on a port, enter **frsvc** followed by the slot number of the ATM port, a slash (/), and the port number of the ATM port. For example, to display the configurations of all FR/ATM IWFs on ATM Port 1 in Slot 4, enter

```
frsvc 4/1
```

at the system prompt. A screen similar to the following will be displayed

FR-ATM IWF Configuration for Slot 4 Port 1

Slot	Port	VPI	VCI	Slot	Port	DLCI	IWF Type
----	----	----	----	----	----	-----	-----
4	1	0	200	2	1	100	Network (FRF.5)
4	1	0	200	2	1	102	Network (FRF.5)
4	2	0	400	3	3	120	Service (FRF.8)

See *Displaying the Configurations of All FR/ATM IWFs on a Switch* on page 38-37 for descriptions of the fields displayed by the **frsvc** command for all FR/ATM IWFs on a port.

Displaying the Detailed Configuration of a Single FR/ATM IWF

To display the detailed configuration of a single FR/ATM IWF on a port, enter **frsvc** followed by the slot number of the ATM port, a slash (/), the port number of the ATM port, the VPI number, a slash (/), and the VCI number. For example, to display the configuration of FR/ATM IWF 0/300 on ATM Port 1 in Slot 2, enter

```
frsvc 2/1 0/300
```

at the system prompt. A screen similar to the following will be displayed.

```
FR-ATM IWF Configuration for Slot 2 Port 1 Connection 0/300

IWF Type : Service (FRF.8)

IWF Status (Admin/Oper) : UP / UP

ATM PVC Information:

```

Slot	Port	VPI	VCI	Connection Description	Conn Type	Circuit Type	Operational Status
2	1	0	300	Connection 0/300	VCC	PVC	LocalUp End2endUnknown

```

FR PVC Information:

```

Slot	Port	DLCI	FR-SSCS DLCI	OperStatus	DLCI Type
6	1	300	300	INACTIVE	Configured

```

IWF Information:
DE-CLP Mapping : Enabled
Default CLP Value : 0
Congestion Notification Mapping : Enabled
Upper Layer Protocol Encapsulation : Enabled
Encapsulation Mode : Translation
LIV Polling Interval T391(in secs) : 15
Full Status Polling Counter N391 : 1
User Error Threshold Counter N392 : 3
User Monitored Events Counter N393 : 4

Poll Verification Interval T392(in secs) : 20
Network Error Threshold Counter N392 : 3
Network Monitored Events Counter N393 : 4

```

The fields displayed by the **frsvc** command for a single FR/ATM IWF are grouped into four groups. The first group displays general information on the FR/ATM IWF. The second group (under the **ATM PVC Information** heading) displays information on the ATM side of this IWF. The third group (under the **FR PVC Information** heading) displays information on the Frame Relay side of this IWF. And the fourth group (under the **IWF Information** heading) displays detailed information on this ATM IWF.

◆ Important Note ◆

The fields **LIV Polling Interval T391** through **Network Monitored Events Counter N393** will *not* be displayed on an FR/ATM IWF service (FRF.8).

The fields displayed by the **frsvc** command for a single FR/ATM IWF are described below.

IWF Type. The FR/ATM Internetworking Function (IWF) type. This will display **Network (FRF.5)** if this FR/ATM IWF is an FR/ATM IWF network, or **Service (FRF.8)** if this FR/ATM IWF is an FR/ATM IWF service.

IWF Status (Admin). The administrative status for this FR/ATM IWF. This field will display **UP** if the ATM and Frame Relay Ports have been enabled and the operational status for this FR/ATM IWF (see the following page) is also Up. If this field displays **DN** (down), then the ports will not pass data.

IWF Status (Oper). The operational status for this FR/ATM IWF. This field will display **UP** if the IWF administrative state is Up (see previous page) and the ATM and Frame Relay ports are passing data. This field will display or **DN** if the administrative state is down or there is a problem in the physical connections.

ATM PVC Information

Slot. The slot number of the ATM port for this FR/ATM IWF.

Port. The port number of the ATM port for this FR/ATM IWF.

VPI. The ATM Virtual Path Identifier (VPI) for this FR/ATM IWF.

VCI. The ATM Virtual Channel Identifier (VCI) for this FR/ATM IWF.

Connection Description. A textual description of up to 30 characters for this FR/ATM IWF.

Conn Type. Indicates whether this connection is a virtual path or a virtual channel. All FR/ATM IWFs are virtual channels. Therefore, this column will always display **VCC** (Virtual Channel Connection).

Circuit Type. The circuit type for this FR/ATM IWF. Since only PVCs are supported on FR/ATM IWFs, this field will always display **PVC**.

Operational Status. The current operational status of this FR/ATM IWF. This status will display as one of the following:

LocalUp End2endUnknown	Only local information is known. The local end of the connection is operational, but the switch cannot tell if the remote end is up or down.
LocalDown	Only local information is known. The local end of the connection is not operational.

◆ Note ◆

FR/ATM IWFs will always have an operational status in which the remote end status is unknown (i.e., **LocalUp End2endUnknown** or **LocalDown**).

FR PVC Information

Slot. The slot number of the Frame Relay port for this FR/ATM IWF.

Port. The port number of the Frame Relay port for this FR/ATM IWF.

DLCI. The local Frame Relay Data Link Connection Identifier (DLCI) of this FR/ATM IWF.

FR-SSCS DLCI. The Frame Relay Service Specific Convergence Sublayer (FR-SSCS) DLCI. This field displays the DLCI agreed between the two ATM end systems (e.g., ATM end users or IWFs).

OperStatus. The operational status of the Frame Port. If **UP**, then the virtual circuit is capable of passing data. If **DN**, then the FR/ATM IWF cannot pass data because the network has declared the FR/ATM IWF inactive, the network does not respond to STATUS ENQUIRY messages, or the FR/ATM IWF is Administratively Down.

DLCI Type. In Frame Relay networks, the DLCI type will be either **Configured** or **Learned**. This field will always display **Configured** for FR/ATM IWF networks and services.

IWF Information

DE-CLP Mapping. This field will display **Enabled** if Frame Relay Discard Eligibility (DE) to ATM Cell Loss Priority (CLP) has been enabled, or **Disabled** if it has been disabled.

Default CLP Value. The value of the ATM Cell Loss Priority (CLP), which will be either **0** or **1**.

Congestion Notification Mapping. This field will display **Enabled** if Frame Relay Forward Explicit Congestion (FECN) to ATM Explicit Forward Congestion Indication (EFCI) has been enabled, or **Disabled** if it has been disabled.

Upper Layer Protocol Encapsulation. If this field displays **Translation**, then the Frame Relay upper layer protocols are encapsulated according to FRF.3 and the ATM upper layer protocols are encapsulated according to RFC 1483. If this field displays **Transparent**, then the upper layer encapsulation methods are unaltered.

◆ Note ◆

The fields **LIV Polling Interval T391** through **Network Monitored Events Counter N393** will *not* be displayed on an FR/ATM IWF service (FRF.8).

LIV Polling Interval T391. This field displays the user-side T391 integrity verification polling timer value (in seconds) for this FR/ATM IWF.

Full Status Polling Counter N391. This field displays the user-side N391 full status polling cycle value for this FR/ATM IWF.

User Error Threshold Counter N393. This field displays the number of status polling intervals over which the **User Error Threshold N392** is counted. If the station received the number of errors specified in **User Error Threshold N392** within the number of polling intervals specified for the **User Monitored Events Threshold Counter N393**, then the Frame Relay line is considered down and all associated virtual circuits are considered inactive.

Poll Verification Interval T392. This field displays the network-side T392 polling verification timer value (in seconds) for this FR/ATM IWF.

Network Error Threshold Counter N392. This field displays the network-side N392 error threshold value for this FR/ATM IWF.

Network Monitored Events Counter N393. This field displays the network-side N393 monitored events count value for this FR/ATM IWF.

Displaying FR/ATM IWF Statistics

You use the **frsvs** command to display the Frame Relay (FR)/ATM Internetworking Function (IWF) statistics for an entire switch, an ATM switching module, a single port, or a single FR/ATM IWF. The syntax for this command is as follows:

```
frsvs [<atm_slot>[/<atm_port>[<vpi>/<vci>]]]
```

To display the FR/ATM statistics for an entire switch, see the subsection below. To display the statistics for all FR/ATM IWFs on an ATM switching module, see *Displaying the Statistics for All FR/ATM IWFs on an ATM Switching Module* on page 38-43. To display the statistics for all FR/ATM IWFs on a single port, see *Displaying the Statistics for All FR/ATM IWFs on a Port* on page 38-43. To display detailed statistics for a single FR/ATM IWF, see *Displaying the Statistics for a Single FR/ATM IWF on a Port* on page 38-44.

Displaying the Statistics for All FR/ATM IWFs on a Switch

To display the statistics for all FR/ATM IWFs on a switch, enter

```
frsvs
```

at the system prompt. A screen similar to the following will be displayed.

Slot	Port	VPI	VCI	FR-ATM IWF Statistics		ATM-to-FR Direction	
				FR-to-ATM Direction Frames In	Octets Out	Octets In	Frames Out
4	1	0	200	100	30962	824585	42
4	2	0	400	200	56024	980352	68
6	1	0	800	43	3637	20326	36

The fields displayed by the **frsvs** command for an entire switch are described below.

Slot. The slot number of the ATM port for this FR/ATM IWF.

Port. The port number of the ATM port for this ATM/FR IWF.

VPI. The Virtual Path Identifier (VPI) for this FR/ATM IWF.

VCI. The Virtual Channel Identifier (VCI) for this FR/ATM IWF.

FR-to-ATM Direction Frames In. The number of frames received by the ATM port of this FR/ATM IWF.

FR-to-ATM Direction Octets Out. The total number of octets transmitted by the ATM port of this FR/ATM IWF.

ATM-to-FR Octets In. The number of octets received by the Frame Relay port (or ports) of this FR/ATM IWF.

ATM-to-FR Frames Out. The number of frames transmitted by the Frame Relay port (or ports) of this FR/ATM IWF.

Displaying the Statistics for All FR/ATM IWFs on an ATM Switching Module

To display the statistics for all FR/ATM IWFs on an ATM module, enter **frsvs** followed by the slot number of the ATM port. For example, to display the statistics for all FR/ATM IWFs on the ATM module in Slot 4, enter

frsvs 4

at the prompt. A screen similar to the following will be displayed.

FR-ATM IWF Statistics for Slot 4							
Slot	Port	VPI	VCI	FR-to-ATM Direction		ATM-to-FR Direction	
				Frames In	Octets Out	Octets In	Frames Out
4	1	0	200	100	824585	30962	42
4	2	0	400	200	56024	980352	68

The statistics displayed by the **frsvs** command for an ATM module are described in *Displaying the Statistics for All FR/ATM IWFs on a Switch* on page 38-42.

Displaying the Statistics for All FR/ATM IWFs on a Port

To display the statistics for all FR/ATM IWFs on a single port, enter **frsvs** followed by the slot number of the ATM port, a slash (/), and the port number of the ATM port. For example, to display the statistics for all FR/ATM IWFs on Port 1 in Slot 4, enter

frsvs 4/1

at the prompt. A screen similar to the following will be displayed.

FR-ATM IWF Statistics for Slot 4 Port 1							
Slot	Port	VPI	VCI	FR-to-ATM Direction		ATM-to-FR Direction	
				Frames In	Octets Out	Octets In	Frames Out
4	1	0	200	100	824585	30962	42
4	1	0	240	50	3895	2490	28
TOTAL			=	150	828480	33352	70

The statistics displayed by the **frsvs** command for a single port are described in *Displaying the Statistics for All FR/ATM IWFs on a Switch* on page 38-42. The only difference is that this option also displays the total frames in and octets out for all FR/ATM IWFs received and transmitted in the Frame Relay to ATM direction, and all the octets in and frames out received in the ATM to Frame Relay direction.

Displaying the Statistics for a Single FR/ATM IWF on a Port

To display the statistics for a single FR/ATM IWF on a port, enter **frsvs** followed by the slot number of the ATM port, a slash (/), the port number of the ATM port, the VPI number, a slash (/), and the VCI number.

The statistics displayed by the **frsvs** command for a single FR/ATM IWF vary depending on if the FR/ATM IWF is an FRF.5 network or an FRF.8 service. See the subsection below for FRF.5 network statistics and see *Displaying FR/ATM IWF Statistics for FRF.8 Services* on page 38-45 for FRF.8 service statistics.

Displaying FR/ATM IWF Statistics for FRF.5 Networks

To display the statistics for the FRF.5 network with a VPI number of 0 and a VCI number of 200 on Port 1 in Slot 4, for example, enter

```
frsvs 4/1 0/200
```

A screen similar to the following will be displayed.

FR-ATM IWF Statistics for Slot 4 Port 1 Connection 0/200

Slot	Port	VPI	VCI	FR-to-ATM Direction Frames In	Direction Octets Out	ATM-to-FR Direction Octets In	Direction Frames Out
4	1	0	200	100	824585	30962	42

LMI Frames Statistics :

FR-to-ATM (Outgoing Frames)

100

ATM-to-FR (Incoming Frames)

42

The statistics displayed by the **frsvs** command for a single FRF.5 network are displayed in two sets. The first set, displayed under the **FR-ATM IWF Statistics** heading, is described in *Displaying the Statistics for All FR/ATM IWFs on a Switch* on page 38-42. The second set, displayed under the **LMI Frames Statistics** heading, shows statistics for the Frame Relay side of this FRF.5 network. These statistics are described below.

FR-to-ATM Outgoing Frames). The total number of frames transmitted in the Frame-Relay-to-ATM direction on the Frame Relay side of this FRF.5 network.

ATM-to-FR (Incoming Frames). The total number of frames received in the ATM-to-Frame-Relay direction on the Frame relay side of this FRF.5 network.

Displaying FR/ATM IWF Statistics for FRF.8 Services

To display the statistics for the FRF.8 service with a VPI number of 0 and a VCI number of 300 on Port 2 in Slot 4, for example, enter

```
frsvs 4/1 0/200
```

at the prompt. For FRF.8 services, a screen similar to the following will be displayed.

FR-ATM IWF Statistics for Slot 4 Port 2 Connection 0/300

Slot	Port	VPI	VCI	FR-to-ATM Direction		ATM-to-FR Direction	
				Frames In	Octets Out	Octets In	Frames Out
4	1	0	200	100	824585	30962	42

Encapsulation Statistics:

Frame Type	FR-to-ATM	ATM-to-FR
Ethernet	20	10
Token Ring	8	0
FDDI	0	0
IP	12	8
IPX	0	0
BPDU	0	0
ARP	8	0
InARP	0	0
ISO	0	0
(CLNP,ISIS,ESIS)		

The statistics displayed by the **frsvs** command for a single FRF.8 service are displayed in two sets. The first set, displayed under the **FR-ATM IWF Statistics** heading, is described in *Displaying the Statistics for All FR/ATM IWFs on a Switch* on page 38-42. The second set, displayed under the **Encapsulation Statistics** heading, is described below.

Frame Type. The frame format type sent either in the Frame-Relay-to-ATM direction or in the ATM-to-Frame-Relay direction. The valid frame formats are displayed in rows and are described below:

Ethernet. Statistics in this row indicate traffic for Ethernet (bridged 802.3 or trunked format) frames on this FR/ATM IWF.

Token Ring. Statistics in this row indicate traffic for Token Ring (802.5 format) frames on this FR/ATM IWF.

FDDI. Statistics in this row indicate traffic for FDDI frames on this FR/ATM IWF.

IP. Statistics in this row indicate traffic for routed IP format frames on this FR/ATM IWF.

IPX. Statistics in this row indicate traffic for routed IPX format frames and octets on this FR/ATM IWF.

BPDU. Statistics in this row indicate traffic for BPDU frames on this FR/ATM IWF.

ARP. Statistics in this row indicate traffic for frames that use Address Resolution Protocol (ARP), which matches IP addresses with MAC addresses, on this FR/ATM IWF.

InARP. Statistics in this row indicate traffic for Inverse Address Resolution Protocol (InARP) RFC 1293 frames on this FR/ATM IWF.

ISO (CLNP,ISIS,ESIS). Statistics in this row indicate traffic for ISO 8473 Connectionless Network Protocol (CLNP), ISO 10589 Intermediate System to Intermediate System Routing Information Exchange Protocol (ISIS), and ISO 9542 End System to Intermediate System Routing Information Exchange Protocol (ESIS) frames on this FR/ATM IWF.

39 SONET Error Collection

Synchronous Optical Network (SONET) is the North American (and Japanese) standard for telecommunications transmission using fiber optic cable. Synchronous Digital Hierarchy (SDH) is its European equivalent and has only slight differences. SONET defines the interface standards at the physical layer of the seven-layer OSI model that enable connection of fiber optic transmission systems and management of high bandwidth services. SONET is now an ANSI standard (ANSI T1.105, ANSI T1.106, and ANSI T1.117) and SDH is a UTI-T standard (G.707, G.708, G.709, and G.783).

One of the primary advantages of SONET is that it allows many different transmission formats (e.g., DS1, DS3, E3, video) to be transmitted on a single line. Basically, separate, slower signals can be multiplexed directly onto higher speed SONET signals without intermediate stages of multiplexing.

Transmission Rates and Signals

Synchronous Transport Signal 1 (STS-1) is the SONET standard for transmission over Optical Carrier 1 (OC-1) optical fiber at 51.84 Mbps. Higher-level signals are multiples of this basic rate. For example, STS-3/OC-3 (155.52 Mbps) is three times STS-1 and STS-12/OC-12 (622.08 Mbps) is 12 times the STS-1 rate. In SONET, 28 DS1 signals operating at 1.544 Mbps can be multiplexed into one STS-1 signal. (A small amount of the bandwidth is used for overhead.) In SDH, the standard Synchronous Transport Module 1 (STM-1) is the SDH standard for transmission over OC-3 optical fiber at 155.52 Mbps.

The STS signal consists of two parts: the STS payload (i.e., data) and the STS overhead. The overhead bytes manage the payload bytes and perform centralized fault management.

User Interface Commands

You can monitor the performance of SONET ATM ports and troubleshoot problems on these ports with SONET error collection. You can enable, configure, and monitor SONET error collection through User Interface (UI) commands. Descriptions of these commands begin on page 39-6.

◆ Note ◆

You *must* install the **sonet.img** image file to run the SONET error collection commands.

SONET error collection is supported on OmniSwitch Cell Switching Modules (CSMs) and ATM access modules (ASMs and ASM2s on the OmniSwitch and ASXs on the Omni Switch/Router). In addition, SONET error collection is not supported on the FCSM or FCSM II. Also, it is not supported on Ethernet or Token Ring modules.

◆ Important Notes ◆

For Release 4.4 and later, the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. Because SONET error collection is supported only in UI mode, you *must* change from CLI mode to UI mode. See Chapter 8, “The User Interface” for information on changing from CLI mode to UI mode.

SONET Error Collection and Switch Performance

When SONET collection is enabled, there is a small impact upon switch performance depending on the number of ports on which SONET is enabled and the number of intervals (see *SONET Error Collection Intervals* on page 39-3) of error collection that have been configured. However, under normal operating conditions, SONET error collection will not add more than 10% CPU overhead.

SONET Overview

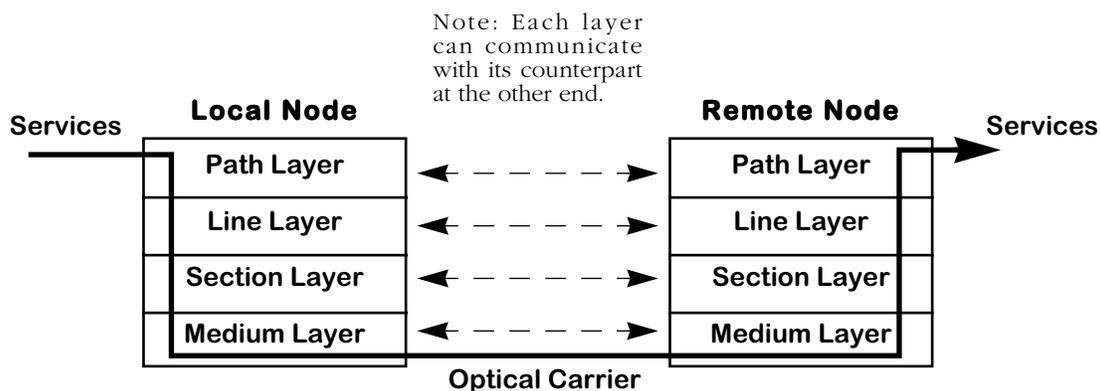
The following sections provide a brief overview of SONET/SDH topics that are important to SONET error collection.

SONET Error Collection Intervals

Once SONET error collection is enabled, the ATM timer invokes the physical level every second to read the hardware registers and send any physical-level errors to the statistics update module. Information about the physical medium is also sent to the statistics update module. This module calculates RFC 1595 errors and then updates the current table data structure. Every 15 minutes, the current samples are moved to a list of previous samples. Each 15-minute period is referred to as an *interval*.

SONET Protocol Layers

The SONET protocol stack consists of the medium, section, line, and path layers. The figure below illustrates four levels of hierarchy. Each layer can communicate with the layers above and below it. In addition, each layer can communicate with its counterpart on the far end. All of these layers are described in the subsections below.



Hierarchy of SONET Protocol Layers

Path Layer

Path Terminating Equipment (PTE) multiplexes/demultiplexes the STS payload and inserts STS path overhead, which consists of signaling and protocol information. The path layer maps services onto STS frames and transports them between the PTE. These services can be DS1, DS3, and video.

The main function of the path layer is to map signals into the format required by the line layer. The path layer reads, interprets, and modifies path overhead for performance and automatic protection switching. See *Viewing SONET Error Statistics Tables* on page 39-11 for displaying detailed statistics and *Viewing the Summary of SONET Error Statistics* on page 39-24 for displaying a summary of error statistics for this level.

Line Layer

A *line* is defined as the medium required to transmit data from the originating line equipment to the Line Terminating Equipment (LTE). The main function of the line layer is to provide synchronization and multiplexing for the path layer (described on the previous page). See *Viewing SONET Error Statistics Tables* on page 39-11 for displaying detailed statistics and *Viewing the Summary of SONET Error Statistics* on page 39-24 for displaying a summary of error statistics for this level.

Section Layer

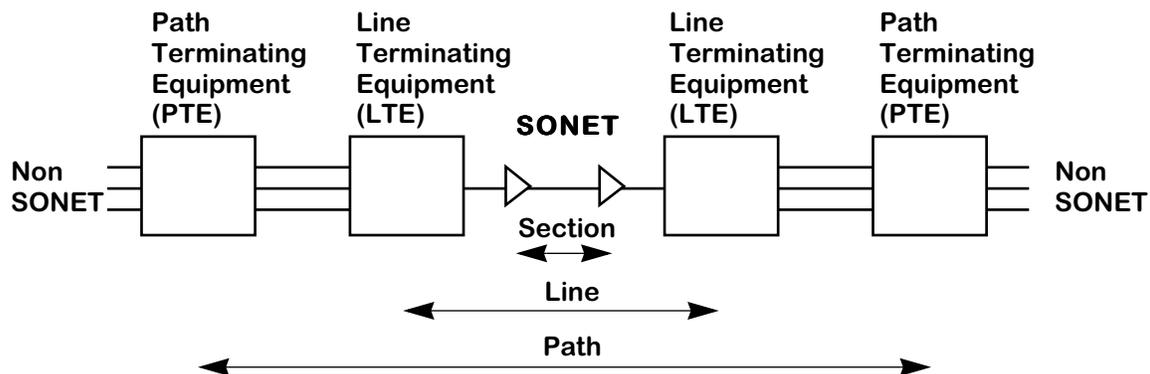
The section layer deals with the transport of STS frames across the physical medium. Section layer functions include framing, scrambling, section error monitoring, and insertion/termination of the section layer overhead. See *Viewing SONET Error Statistics Tables* on page 39-11 for displaying detailed statistics and *Viewing the Summary of SONET Error Statistics* on page 39-24 for displaying a summary of error statistics for this level.

Medium Layer

The medium layer, also known as the photonic layer, deals with the transport of bits across the physical medium. Its main function is the conversion between the electrical STS signal and optical OC signal. This layer is concerned with wavelength, pulse shape, and power level. See *Viewing the SONET Medium Table* on page 39-9 for documentation on displaying statistics for this layer.

SONET Connections

The figure below shows a simple SONET end-to-end connection. A non SONET signal is converted to an STS signal by the local Path Terminating Equipment (PTE). The PTE multiplexes the STS signal and adds path overhead. The PTE passes the STS signal to the Line Terminating Equipment (LTE), which provides reliable transport of the path layer payload and its overhead across the physical medium. The LTE passes the STS payload to the Section Terminating Equipment (STE). Basically, an STE is any two adjacent SONET network elements (e.g., a regenerator).



Simple SONET End-to-End Connection

Enabling and Disabling SONET Error Collection

You enable and disable the SONET error collection with the **smon** command. When the **smon** command is executed for the first time, the **sec.img** file is loaded and the SONET error collection commands (described in *The SONET Error Collection Menu* on page 39-6) are loaded. In addition, you can also display whether the SONET error collection has been enabled.

The syntax for the **smon** command is as follows:

```
smon [on | off]
```

The subsections below describe the three ways the **smon** command can be used.

Displaying SONET Error Collection Status

To display whether the SONET error collection has been enabled, enter

```
smon
```

at the system prompt. If SONET error collection has enabled, then the following will be displayed.

```
Sonet Monitoring is ON  
Usage: smon status  
status "on" - To Start Sonet Monitoring  
      "off" - To Stop Sonet Monitoring
```

If the SONET error collection has been disabled, then the following will be displayed.

```
Sonet Monitoring is OFF  
Usage: smon status  
status "on" - To Start Sonet Monitoring  
      "off" - To Stop Sonet Monitoring
```

Enabling SONET Error Collection

To enable the SONET error collection, enter

```
smon on
```

at the system prompt. After a few seconds, a screen similar to the following will be displayed.

```
Restoring SEC on 3/1, 3/2, 3/3, 3/4, 3/5, 3/6, 3/7, 3/8  
Config Restore of SEC over.
```

If you have installed the **sec.img** image file, you can now run the SONET error collection commands. Descriptions of these commands begin on page 39-6.

Disabling SONET Error Collection

To disable the SONET error collection, enter

```
smon off
```

The SONET Error Collection Menu

Before you can use the SONET error collection commands, you *must* perform the following steps:

- Load the **sec.img** file, which contains the software for these commands, onto your switch. (See Chapter 9, “Installing Switch Software,” for more information on installing image files.)
- Enable the commands with the **smon** command, which is described in *Enabling SONET Error Collection* on page 39-5.

After you have accomplished these steps, the SONET submenu will be displayed in the Interface menu, as shown below.

Command	Physical Interface Menu
slipc	Configure SLIP (Serial Line IP) on a TTY Port
eth100	Enter the 100BaseT sub-menu
10/100	Enter the 10/100BaseT sub-menu
sonet	Enter Sonet Sub-Menu
atm	Enter the ATM Management sub-menu

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

To enter the SONET submenu, enter

sonet

at the system prompt. Enter a question mark (?) to display the SONET submenu commands, as shown below.

Command	Sonet Error Statistics Menu
ses	Enable SONET Error Collection on Slot/Intf
sedm	Display SONET Medium Table
sest	Display Error Statistics Tables
secs	Clear Error Statistics Tables
sess	Display Summary of Error Statistics Collected

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

The **ses** command is described in *Enabling SONET Error Collection on ATM Ports* on page 39-7. The **sedm** command is described in *Viewing the SONET Medium Table* on page 39-9. The **sest** command is described in *Viewing SONET Error Statistics Tables* on page 39-11. The **secs** command is described in *Clearing SONET Error Statistics Tables for the Current Interval* on page 39-22. And the **sess** command is described in *Viewing the Summary of SONET Error Statistics* on page 39-24.

Enabling SONET Error Collection on ATM Ports

You can enable SONET error collection on a single ATM port, on all ATM ports on a switching module, or on every ATM port in a switch with the **ses** command. The syntax for the **ses** command is as follows:

```
ses <slot/port> | <slot> | all
```

The subsections that follow describe the three different ways you can enable SONET error collection.

Enabling SONET Error Collection on a Single Port

To enable SONET error collection on a single ATM port, enter **ses** followed by the slot number of the module, a slash (*/*), and the port number. For example, to enable SONET error collection on ATM port 3/6, enter

```
ses 3/6
```

at the system prompt. A screen similar to the following will be displayed.

SONET Error Statistics Collection

```
1) S/UNI Error Collection {Enable(1), Disable(2)} : Enable  
2) Number of 15 minutes samples to be stored (4..96) : 32
```

```
Enter (option=value/save/cancel) :
```

Select the number of the item you want to change. To change any of the values listed above, enter the line number, followed by an equal sign, and then the new value. For example, to set the number of 15-minute samples collected to 5, enter

```
2=5
```

at the prompt. To update the values you have changed, enter **save**. If you do not want to save the changes enter **quit** or **cancel**, or press **Ctrl-D**. If your changes have been successfully made, the following confirmation message will be displayed.

```
saving...
```

The configurable parameters in the **ses** command are described below.

1) S/UNI Error Collection

Enter **1** to enable SONET error collection or **2** to disable it.

2) Number of 15 minutes samples to be stored

Enter the number of 15-minute samples to be collected. The valid range is **4** to **96**. (Setting this value to **96** will set up collection for a 24-hour period.)

Enabling SONET Error Collection on all ATM Ports on a Switching Module

To enable SONET error collection on all ATM ports on a switching module, enter **ses** followed by the slot number. For example, to enable SONET error collection on all ATM ports on slot 3, enter

```
ses 3
```

A screen similar to the following will be displayed.

SONET Error Statistics Collection on All Ports in Slot 3

- 1) S/UNI Error Collection {Enable(1), Disable(2)} : -
- 2) Number of 15 minutes samples to be stored (4..96) : -

Enter (option=value/save/cancel) :

Select the number of the item you want to change. See *Enabling SONET Error Collection on a Single Port* on page 39-7 for documentation on configuring these items.

Enabling SONET Error Collection on all ATM Ports in a Switch

To enable SONET error collection on all ATM ports, enter

```
ses all
```

at the system prompt. A screen similar to the following will be displayed.

SONET Error Statistics Collection on All Slots and Ports

- 1) S/UNI Error Collection {Enable(1), Disable(2)} : -
- 2) Number of 15 minutes samples to be stored (4..96) : -

Select the number of the item you want to change. See *Enabling SONET Error Collection on a Single Port* on page 39-7 for documentation on configuring these items.

Viewing the SONET Medium Table

You use the **sedm** command to display physical media statistics for a single ATM port, all ATM ports on a switching module, or all ATM ports in a switch. The syntax for the **sedm** command is as follows:

```
sedm <slot/port> | <slot> | all
```

See the subsection below for documentation on viewing physical media statistics on a single port; see *Viewing the SONET Medium Table for All ATM Ports on a Switching Module* on page 39-10 for documentation on viewing physical media statistics on all ATM ports on a switching module; and see *Viewing the SONET Medium Table for all ATM Ports* on page 39-10 for documentation on viewing physical media statistics on all ATM ports in a switch.

Viewing the SONET Medium Table for a Single ATM Port

To display the physical media statistics for a single ATM port, enter **sedm** followed by the slot number of the port, a slash (/), and the port number. For example to display the physical media statistics for port 3/1, enter

```
sedm 3/1
```

at the system prompt. A screen similar to the following will be displayed.

```
SONET Medium Table for 3/1
=====
Medium Type           SONET
Time Elapsed         16 sec
Number of samples     10
Line Coding           NRZ
Line Type             Multi Mode
Circuit Identifier    PMC SUNI
```

The fields displayed by the **sedm** command are described below.

Medium Type. This field identifies whether a North American SONET signal or a European SDH signal is used on this port.

Time Elapsed. The number of seconds, including partial seconds, that have elapsed since the current error-measuring period.

Number of samples. The number of previous intervals for which valid data has been stored.

Line Coding. The type of line coding used on this port. The types of line coding include B3Zs and CMI, which are used for electrical SONET/SDH signals (STS-1 and STS-3), and Non-Return to Zero (NRZ) and Return to Zero (RZ), which are used for optical SONET/SDH signals. If the type of line coding is unknown, then **Other** will be displayed.

Line Type. The line type used on this port. The line types include Short Single Mode, Long Single Mode, and Multi Mode used on fiber interfaces, and Coax and UTP used on electrical interfaces. If the line type is unknown, then **Other** will be displayed.

Circuit Identifier. This field displays the transmission vendor's circuit identifier. This information can be used to aid troubleshooting.

Viewing the SONET Medium Table for All ATM Ports on a Switching Module

To display the physical media statistics for all ATM ports on a switching module, enter **sedm** followed by the slot number. For example, to display the physical media statistics for all ATM ports, enter

sedm 3

at the system prompt. See *Viewing the SONET Medium Table for a Single ATM Port* on page 39-9 for a sample display and descriptions of statistics.

Viewing the SONET Medium Table for all ATM Ports

To display the physical media statistics for all ATM ports on a switch, enter **sedm** followed by **all**. For example, to display the physical media statistics for all ATM ports, enter

sedm all

at the system prompt. See *Viewing the SONET Medium Table for a Single ATM Port* on page 39-9 for a sample display and descriptions of statistics.

Viewing SONET Error Statistics Tables

You use the **sed**s command to view the SONET error statistics tables. The syntax for the **sed**s command is as follows:

```
seds <slot/port> [<interval>] [<table>]
```

The **<interval>** option lets you display a specific interval (described in *Viewing SONET Error Statistics for a Single Interval* on page 39-17) or all intervals (described in *Viewing SONET Error Statistics for All Intervals* on page 39-19). If you do not use this option, then the current interval will be displayed (described in the subsection below).

The **<table>** option lets you display a specific table for a single interval, the current interval, or all intervals. See *Viewing Individual SONET Error Statistics Tables* on page 39-21 for a description of this option.

Viewing SONET Error Statistics for the Current Interval

To view the SONET error statistics table for the current interval, enter **sed**s followed by the slot number of the module, a slash (/), and the port number. (You can also view just one table with the **<table>** option, which is described in *Viewing Individual SONET Error Statistics Tables* on page 39-21.) For example, to view the error statistics for ATM port 3/4, enter

```
seds 3/4
```

at the system prompt. A screen similar to the one on following page will be displayed.

SONET Section Table
=====

Interval Number	Current Interval
Interval Start Time	THU SEP 16 16:25:40 1999
Line Status	LOS and LOF
Coding Violations	2165901
Errored Seconds	44
Severely Errored Seconds	44
Severely Errored Framing Seconds	44

SONET Line Table
=====

Interval Number	Current Interval	
Interval Start Time	THU SEP 16 16:25:40 1999	
Errors	Line	Far End Line
=====	====	=====
Line Status	AIS	NA
Coding Violations	0	0
Errored Seconds	9	0
Severely Errored Seconds	0	0
Unavailable Seconds	44	0

SONET Path Table
=====

Interval Number	Current Interval	
Interval Start Time	THU SEP 16 16:25:40 1999	
Errors	Path	Far End Path
=====	====	=====
Line Status	STS AIS, STS RDI, LabelMismatch	
Coding Violations	0	0
Errored Seconds	9	0
Severely Errored Seconds	0	0
Unavailable Seconds	46	0

The fields displayed by the **sed**s command are grouped into statistics for the section, line, and path tables. In addition, the line and path interval tables are divided into local and far-end groups for most statistics. See the subsections on the following pages for descriptions of these statistics for the current interval.

Section Table Statistics

The section table statistics displayed by the **seds** command for the current interval are described below.

Interval Number. This field displays the text **Current Interval**.

Interval Start Time. The start time of the current interval.

◆ Note ◆

The following field, **Line Status**, only displays when you select the current interval.

Line Status. This field displays the current status of the interface for this interval. The following lists the possible values:

NoDefect. The interface is operating properly.

LOS. The interface is experiencing a Loss of Signal (LOS) failure.

LOF. The interface is experiencing a Loss of Frame (LOF) failure. An LOF defect is declared when an Out of Frame/Severely Errored Frame (OOF/SEF) defect persists for a period of 3 milliseconds. An LOF failure is declared when the LOF defect persists for a period of 2.5 (+/- 0.5) seconds (except when the LOS failure or defect is present).

Coding Violations. The number of coding violations encountered by the SONET/SDH section layer in this 15-minute interval. Coding violations are Bit Interleaved Parity (BIP) errors detected in the incoming signal. Section level coding violations are collected using BIP-8 in the B1 byte located in the section overhead of STS-1 No. 1.

Errored Seconds. The number of errored seconds encountered by the SONET/SDH section layer in this 15-minute interval. An errored second is a second with one or more coding violations at this layer or one or more incoming defects (e.g., a Severely Errored Frame (SEF), a Loss of Signal (LOS), an Alarm Indication Signal (AIS), or a Loss of Pointer(LOP)) has occurred.

Severely Errored Seconds. The number of severely-errored seconds encountered by the SONET/SDH section layer in this 15-minute interval. A severely errored second is a second with a rate of x or more coding violations at this layer (depending on the data rate, as shown in the table below), or a second during which at least one or more incoming defects at this layer has occurred.

Severely Errored Second Values for the Section Layer

Rate	Number of Coding Violations (x)	Min. Bit error rate
OC-1	9	1.5×10^{-7}
OC-3	16	1.0×10^{-7}
OC-9	47	1.0×10^{-7}
OC-12	63	1.0×10^{-7}

Severely Errored Framing Seconds. The number of Severely Errored Framing Seconds (SEFS) encountered by the SONET/SDH section layer in this 15-minute interval. An SEFS is a second containing one or more Out of Frame (OOF) errors.

Line Table Statistics

The line table statistics displayed by the **sed**s command for the current interval are described below.

Interval Number. This field displays the text **Current Interval**.

Interval Start Time. The start time of the current interval.

Local Line Table Statistics

◆ Note ◆

The following field, **Line Status**, only displays when you select the current interval.

Line Status (Line). This field displays the current status of the interface for this interval. The following lists the possible values:

NoDefect. The interface is operating properly.

AIS. The interface is experiencing an Alarm Indication Signal (AIS) failure. A line AIS defect is detected as a “111” pattern in bits 6, 7, and 8 of the K2 byte, which is used for Automatic Protection Switching (APS) signaling, in five (5) consecutive frames. A line AIS failure is declared when the Line AIS defect persists for 20.5 (+/- 0.5) seconds.

RDI. The interface is experiencing a Remote Defect Indication (RDI). A line RDI defect is a “110” code in bits 6, 7, and 8 of the K2 byte, which is used for Automatic Protection Switching (APS) signaling, of STS-1 No. 1 in five (5) consecutive frames.

Coding Violations. The number of coding violations encountered by the SONET/SDH line layer in this 15-minute interval. Coding violations are Bit Interleaved Parity (BIP) errors detected in the incoming signal. Line level coding violations are collected using BIP-8s in B2 bytes located in the line overhead of each STS-1.

Errored Seconds. The number of errored seconds encountered by the SONET/SDH line layer in this 15-minute interval. An errored second is a second with one or more coding violations at this layer or one or more incoming defects (e.g., a Severely Errored Frame (SEF), a Loss of Signal (LOS), an Alarm Indication Signal (AIS), or a Loss of Pointer (LOP)) has occurred.

Severely Errored Seconds. The number of severely errored seconds encountered by the SONET/SDH line layer in this 15-minute interval. A severely errored second is a second with a rate of x or more coding violations at this layer (depending on the data rate, as shown in the table below), or a second during which at least one or more incoming defects at this layer has occurred.

Severely Errored Second Values for the Line Layer

Rate	Number of Coding Violations (x)	Min. Bit error rate
OC-1	12	2.0×10^{-7}
OC-3	32	2.0×10^{-7}
OC-9	94	2.0×10^{-7}
OC-12	124	2.0×10^{-7}

Unavailable Seconds. The number of unavailable seconds encountered by the SONET/SDH line layer in this 15-minute interval. The SONET/SDH interface at this level becomes unavailable at the onset of 10 contiguous severely errored seconds.

Far End Line Statistics

Line Status (Far End Line). See the description for the **Line Status** field on the previous page.

Coding Violations (Far End Line). The number of far-end coding violations reported via the far-end block counter encountered by the SONET/SDH line layer in the current 15-minute interval. See the description for the **Coding Violations** field for the local line layer on the previous page for more information.

Errored Seconds (Far End Line). The number of far-end errored seconds encountered by the SONET/SDH line layer in the current 15-minute interval. See the description for the **Errored Seconds** field for the local line layer on the previous page for more information.

Severely Errored Seconds (Far End Line). The number of far-end severely-errored seconds encountered by the SONET/SDH line layer in the current 15-minute interval. See the description for the **Severely Errored Seconds** field for the local line layer on the previous page for more information.

Unavailable Seconds (Far End Line). The number of far-end unavailable seconds encountered by the SONET/SDH line layer in the current 15-minute interval. See the description for the **Unavailable Seconds** field for the local line layer above for more information.

Path Table Statistics

The path table statistics displayed by the **se** command for the current interval are described below.

Interval Number. This field displays the text **Current Interval**.

Interval Start Time. The start time of the current interval.

Local Path Table Statistics

◆ Note ◆

The following field, **Line Status**, only displays when you select the current interval.

Line Status. This field displays the current status of the interface. The following lists the possible values:

NoDefect. The interface is operating properly.

STS LOP. The interface is experiencing an STS Loss of Pointer (LOP) failure. An LOP defect is declared when either a valid pointer is not detected in eight (8) consecutive frames, or when eight (8) consecutive frames are detected with the New Data Flag (NDF) set to "1001" with a valid concatenation indicator.

An STS Path LOP failure is declared when the STS Path LOP defect period persists for a period of 2.5 (+/- 0.5) seconds.

STS AIS. The interface is experiencing an STS Alarm Indication Signal (AIS) failure. The STS Path defect is detected as all ones in bytes H1 and H2, which are used to indicate the offset between the pointer and the first byte of the STS-1 SONET Payload Envelope (SPE), in three (3) consecutive frames. An STS Path AIS failure is declared when the STS Path AIS defect persists for 2.5 (+/- 0.5 seconds).

STS RDI. The interface is experiencing an STS Remote Defect Indication (RDI). STS path RDI is detected by the upstream STS Path Terminating Equipment (PTE) as a “1” in bit 5 of the Path Status Byte (G1) for five (5) contiguous frames.

Unequipped. The interface is currently idle.

LabelMismatch. The interface is detecting a signal label mismatch.

Coding Violations. The number of coding violations encountered by the SONET/SDH path layer in this 15-minute interval. Path level coding violations are collected using the BIP-8 in the B3 byte of the STS Path overhead of the Path Terminating Equipment (PTE).

Errored Seconds. The number of errored seconds encountered by the SONET/SDH path layer in this 15-minute interval.

Severely Errored Seconds. The number of severely-errored seconds encountered by the SONET/SDH path layer in this 15-minute interval. A severely errored second is a second with a rate of x or more coding violations at this layer (depending on the data rate, as shown in the table below), or a second during which at least one or more incoming defects at this layer has occurred.

Severely Errored Second Values for the Path Layer

Rate	Number of Coding Violations (x)	Min. Bit Error Rate
STS-1	9	1.5×10^{-7}
STS-3	16	1.0×10^{-7}

Unavailable Seconds. The number of unavailable seconds encountered by the SONET/SDH path layer in this 15-minute interval. The SONET/SDH interface at this level becomes unavailable at the onset of 10 contiguous severely errored seconds.

Far-End Path Table Statistics

Line Status (Far End Path). See the description for the **Line Status (Path)** field on the previous page.

Coding Violations (Far End Path). The number of far-end coding violations reported by the far-end block count encountered via the SONET/SDH line layer in this 15-minute interval. See the description for the **Coding Violations** field for the local path layer on the previous page for more information.

Errored Seconds (Far End Path). The number of far-end errored seconds encountered by the SONET/SDH path layer in this 15-minute interval. See the description for the **Errored Seconds** field for the local path layer above for more information.

Severely Errored Seconds (Far End Path). The number of far-end severely-errored seconds encountered by the SONET/SDH path layer in this 15-minute interval. See the description for the **Severely Errored Seconds** field for the local path layer above for more information.

Unavailable Seconds (Far End Path). The number of unavailable seconds encountered by the SONET/SDH path layer in this 15-minute interval you selected. See the description for the **Unavailable Seconds** field for the local path layer above for more information.

Viewing SONET Error Statistics for a Single Interval

To view the SONET error statistics table for a single interval, enter **sed**s followed by the slot and port number of the ATM port, and followed by the interval number, which *must* be a value between 1 and 96. (You can also view just one table with the **<table>** option, which is described in *Viewing Individual SONET Error Statistics Tables* on page 39-21.) For example, to view the SONET error statistics for ATM port 3/4 for the fifth interval, enter

seds 3/4 5

at the system prompt. A screen similar to the following will be displayed.

SONET Section Table

=====

Interval Number	Previous Interval #5
Interval Start Time	WED SEP 22 12:06:11 1999
Coding Violations	43930404
Errored Seconds	900
Severely Errored Seconds	900
Severely Errored Framing Seconds	900

SONET Line Table

=====

Interval Number	Previous Interval #5	
Interval Start Time	WED SEP 22 12:06:11 1999	
Errors	Line	Far End Line
=====	=====	=====
Coding Violations	0	0
Errored Seconds	0	0
Severely Errored Seconds	0	0
Unavailable Seconds	900	0

SONET Path Table

=====

Interval Number	Previous Interval #5	
Interval Start Time	WED SEP 22 12:06:11 1999	
Errors	Path	Far End Path
=====	=====	=====
Coding Violations	0	0
Errored Seconds	0	0
Severely Errored Seconds	0	0
Unavailable Seconds	900	0

Viewing SONEt Error Statistics Tables

The fields displayed by the **sed**s command are grouped into statistics for the section, line, and path tables. See *Viewing SONEt Error Statistics for the Current Interval* on page 39-11 for descriptions of all statistics except for **Interval Number** and **Interval Start Time**, which are described below.

Interval Number. This field displays the interval number you selected. The interval must be between 1 and 96.

Interval Start Time. The start time of the 15-minute interval you selected.

Viewing SONET Error Statistics for All Intervals

To view the SONET error statistics table for all intervals, enter **se**ds followed by the slot number of the module, a slash (/), the port number, and **all**. (You can also view just one table with the **<table>** option, which is described in *Viewing Individual SONET Error Statistics Tables* on page 39-21.) For example, to view the error statistics for all intervals on ATM port 3/4, enter

```
se
```

ds 3/5 all

at the system prompt. A screen similar to the following will be displayed.

SONET Section Interval Table				
Interval Number	Coding Violation	Errored Seconds	Severely Errored Seconds	Severely Errored Framing Seconds
1	43931988	900	900	900
2	43930434	900	900	900
3	43929612	900	900	900
4	43934406	900	900	900
5	43930404	900	900	900
6	43929618	900	900	900
7	43932786	900	900	900
8	43930416	900	900	900
9	43937622	900	900	900
10	43938396	900	900	900

SONET Line Interval Table				
Interval Number	Coding Violation	Errored Seconds	Severely Errored Seconds	Unavailable Seconds
1	0	0	0	900
2	0	0	0	900
3	0	0	0	900
4	0	0	0	900
5	0	0	0	900
6	0	0	0	900
7	0	0	0	900
8	0	0	0	900
9	0	0	0	900
10	0	0	0	900

SONET Far End Line Interval Table				
Interval Number	Coding Violation	Errored Seconds	Severely Errored Seconds	Unavailable Seconds
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

— Output continues on next page —

SONET Path Interval Table

Interval Number	Coding Violation	Errored Seconds	Severely Errored Seconds	Unavailable Seconds
1	0	0	0	900
2	0	0	0	900
3	0	0	0	900
4	0	0	0	900
5	0	0	0	900
6	0	0	0	900
7	0	0	0	900
8	0	0	0	900
9	0	0	0	900
10	0	0	0	900

SONET Far End Path Interval Table

Interval Number	Coding Violation	Errored Seconds	Severely Errored Seconds	Unavailable Seconds
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

The fields displayed by the **sed**s command are grouped into statistics for the section, line, and path tables. See *Viewing SONET Error Statistics for the Current Interval* on page 39-11 for descriptions of all statistics except for **Interval Number**, which is described below.

Interval Number. The interval number for this instance.

Viewing Individual SONET Error Statistics Tables

You can use the **<table>** option with the **sed**s command to view individual SONET error statistics tables on a single ATM port, on all ATM ports on a switching module, or on all ATM ports. The following lists the valid **<table>** option:

- s** or **S**. Use this option to view the section table.
- l** or **L**. Use this option to view the local and far-end line tables.
- p** or **P**. Use this option view the local and far-end path tables.

For example, to display the local and far-end path table statistics for the fifth interval on port 3/4, enter

```
sed s 3/4 5 p
```

at the system prompt. A screen similar to the following will be displayed.

```

SONET Path Table
=====

Interval Number          Previous Interval #5
Interval Start Time      WED SEP 22 14:23:28 1999

Errors
=====
Coding Violations        Path          Far End Path
Errored Seconds          0             0
Severely Errored Seconds 0             0
Unavailable Seconds      900          0

```

See *Viewing SONET Error Statistics for the Current Interval* on page 39-11 for descriptions of parameters if you use the **<table>** option for the current interval, see *Viewing SONET Error Statistics for a Single Interval* on page 39-17 for a specific interval, or see *Viewing SONET Error Statistics for All Intervals* on page 39-19 for descriptions of parameters if you use the **<table>** option for all intervals.

Clearing SONET Error Statistics Tables for the Current Interval

You use the **secs** command to clear one or all statistics tables for the current interval on one ATM port, all ATM ports on a switching module, or all ATM ports on your switch. The syntax for the **secs** command is as follows:

```
secs <slot/port> | <slot> | all [<table>]
```

The **<table>** option lets you clear the error statistics for a single table. If you do not use this option, then the statistics will be cleared for all tables. See *Clearing Error Statistics for a Single Table* on page 39-23 for more information on this option. To clear the statistics for all tables, see the subsection below.

◆ Important Note ◆

The **secs** command only clears statistics for the current interval and does *not* affect previous intervals.

Clearing Error Statistics for All Tables

To clear all SONET error statistic tables for the current interval on all ATM ports in your switch, enter

```
secs all
```

at the system prompt. To clear all the SONET error statistics on all ATM ports on a switching module, enter **secs** followed by the slot number. For example, to clear the SONET error statistics for all fiber ports on Slot 3 for the current interval, enter

```
secs 3
```

at the system prompt. To clear all the SONET error statistic tables on a single ATM port, enter **secs** followed by the slot number of the port, a slash (/), and the port number. For example, to clear the SONET error statistic tables for port 3/2 for the current interval, enter

```
secs 3/2
```

at the system prompt.

Clearing Error Statistics for a Single Table

You can use the **<table>** option with the **secs** command to clear the statistics (for the current interval) for a single table on all ATM ports in a switch, all ATM ports on a switching module, or a single ATM port. The following lists the valid **<table>** option:

- s** or **S**. Use this option to clear the section table.
- l** or **L**. use this option to clear the near-end line table.
- fl** or **FL**. use this option to clear the far-end line table.
- p** or **P**. Use this option clear the path table.
- fp** or **FP**. Use this option to clear the far-end path table.

For example, to clear the far-end path table statistics on a ATM port 3/4, enter

```
secs 3/4 fp
```

at the system prompt.

◆ Note ◆

When using the **<table>** option, do *not* mix upper- and lower-case letters. While the **FL** or **fl** options will clear the far-end line table statistics, **fL** or **Fl** will just produce an error message.

You must clear the statistics for one table or all of the tables (see *Clearing Error Statistics for All Tables* on page 39-22). You cannot select more than one **<table>** option.

Viewing the Summary of SONET Error Statistics

You can display a summary of SONET error statistics for one ATM port, all ATM ports on a switching module, or all ATM ports on a switch with the **sess** command. The syntax for the **sess** command is as follows:

```
sess <slot/port> | <slot> | all
```

For example, to display the SONET error statistics for all ATM ports on the switching module in slot 3, enter

```
sess 3
```

at the system prompt. A screen similar to the following will be displayed.

```
SONET Error Statistics Summary for Slot 3

Slot/Port      Layer      Errored Interval
=====      =====
3/1            Section    Current, Previous - 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50,
51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70,
71, 72, 73, 74, 75, 76, 77
3/1            Line       Previous - 77
3/1            Path       Previous - 77
3/2            Section    Current, Previous - 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50,
51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70,
71, 72, 73, 74, 75, 76, 77
3/2            Line       Previous - 77
3/2            Path       Previous - 77
3/3            Section    Current, Previous - 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50,
51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70,
71, 72, 73, 74, 75, 76, 77
3/3            Line       Previous - 77
3/3            Path       Previous - 77
3/4            Section    Current, Previous - 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50,
51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70,
71, 72, 73, 74, 75, 76, 77
3/4            Line       Previous - 77
3/4            Path       Previous - 77
3/5            Section    Current, Previous - 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50,
51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70,
71, 72, 73, 74, 75, 76, 77
3/5            Line       Previous - 77
3/5            FarEnd Line Previous - 77
3/5            Path       Previous - 77
3/5            FarEnd Path Previous - 77
```

— Output continues on next page —

```

3/6      Section      Current, Previous - 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50,
51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70,
71, 72, 73, 74, 75, 76, 77
3/6      Line          Previous - 77
3/6      FarEnd Line Previous - 77
3/6      Path          Previous - 77
3/6      FarEnd Path Previous - 77
3/7      Section      Current, Previous - 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50,
51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70,
71, 72, 73, 74, 75, 76, 77
3/7      Line          Previous - 77
3/7      FarEnd Line Previous - 77
3/7      Path          Previous - 77, 78
3/7      FarEnd Path Previous - 78
3/8      Section      Current, Previous - 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50,
51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70,
71, 72, 73, 74, 75, 76, 77, 78
3/8      Line          Previous - 78
3/8      FarEnd Line Previous - 78
3/8      Path          Previous - 78
3/8      FarEnd Path Previous - 78

```

The fields displayed by the `sess` command are described below.

Slot/Port. The port number for this instance

Layer. The layer where the error (or errors) occurred. This can be **Section** for the section layer, **Line** for the line layer, or **Path** for the path layer.

Errored Interval. The intervals that the error (or errors) occurred in.

40 Cell Switching Modules (CSMs)

The OmniSwitch provides the flexibility to start as a pure LAN switch, gradually migrate to a hybrid LAN/ATM switch, and finally transform into a pure ATM switch capable of supporting multiple Classes of Service and robust traffic management. Making the transition from a LAN switch to an ATM switch requires only a change of interface modules; no backplane upgrade is necessary.

The OmniSwitch with ATM switching functionality comes in 3-slot, 5-slot, and 9-slot versions. Each version supports the same management, frame switching, and cell switching modules. Each version also supports the same bus architecture. OmniSwitch chassis types are described in Chapter 4, “The OmniSwitch Chassis.”

Using a distributed architecture, the OmniSwitch enables you to increase the switching capacity as you add Cell Switching Modules (CSMs). Each CSM provides enough capacity to handle the non-blocking load of its own ports. In this way, the OmniSwitch scales cost-effectively with the growth requirements of your ATM network.

This chapter provides a reference to the OmniSwitch ATM cell matrix, the frame-to-cell switching module, and cell switching modules. In addition, it provides application examples to show typical implementations of the OmniSwitch’s ATM switching technology. More detailed information on Quality of Service (QoS) support, traffic management, and virtual circuit configuration is in Chapter 41, “Managing Cell Switching Modules (CSMs).” Information on using the PNNI protocol with the OmniSwitch can be found in Chapter 46, “Configuring and Monitoring PNNI.”

◆ Special Note ◆

The chapter assumes familiarity with ATM concepts. The focus of the chapter is not to explain ATM concepts, but to describe the OmniSwitch implementation of various ATM switch features.

Virtual Circuits

Console and Network Management Software allow you to configure and monitor Permanent Virtual Circuits (PVCs) and “soft PVCs.” Switched Virtual Circuits (SVCs) are only monitored. Statistics are provided for all types of virtual circuits. Virtual circuits may be either Virtual Path Connections (VPCs) or Virtual Channel Connections (VCCs).

A variety of statistics are available at the port and virtual connection level. These statistics provide information on Cell Loss Priority (CLP) cell flows, cell discards, and actions taken as a result of leaky bucket algorithms.

Dynamic Input Buffering With Output Control

The OmniSwitch uses a unique buffer management system that combines the scalability of input buffers and the control of output buffers. Cell buffers are located on input ports, but these buffers are actually controlled by output ports. Each output port sees the traffic destined for it and uses this knowledge to schedule traffic flow across the fabric.

To effectively interconnect ATM networks with the bursty nature of LANs, the OmniSwitch uses very large cell buffers that can withstand massive inflows of LAN traffic.

Quality of Service (QoS)

The OmniSwitch's buffer management supports six (6) different Class of Service levels that are compatible and expand upon ATM Forum QoS specifications. Each QoS level supports a different ATM traffic type (CBR, rt-VBR, nrt-VBR, ABR, or UBR) and supports different Generic Cell Rate Algorithms (GCRAs). The levels are organized by priority with additional granularity provided by sixteen (16) different user priority levels assignable at the virtual circuit level.

Partial Packet Discard (PPD) and Early Packet Discard (EPD)

When either Partial Packet Discard (PPD) or Early Packet Discard (EPD) is enabled, the switch can intelligently discard cells associated with AAL5 PDU during congestion conditions. This feature reduces the bandwidth used along the remaining downstream path. PPD or EPD can be enabled for a specific virtual circuit through the **cvc** command. See Chapter 41, "Managing Cell Switching Modules (CSMs)," for more information on enabling PPD or EPD.

Dual Leaky Buckets

Dual leaky buckets are set up on each virtual circuit and policing algorithms can check for Peak Cell Rate (PCR), Sustained Cell Rate (SCR), and Maximum Burst Size (MBS). Options for enforcement of the traffic contract can be static—dropping all cells in excess of the contract regardless of congestion conditions—or congestion-based. Congestion-based enforcement will tag or discard cells depending on the level of congestion on the connection and a cell's Cell Loss Priority (CLP). The enforcement method is defaulted based on traffic descriptors and is not user-selectable in this release.

Available Bit Rate Traffic

The OmniSwitch supports Explicit Rate flow control for ABR traffic. Resource Management (RM) cells are forwarded along virtual connections. In addition, the Explicit Forward Congestion Indicator (EFCI) is supported for all traffic types. Currently SARs do not support ABR resource management. Therefore, ATM End Systems supporting resource management are not available to test at this time, and this feature is not fully operational in this release.

MPM-C and MPM-III Signaling Performance

Large numbers of calls to other switches (e.g., 250 per second) can cause excessive CPU utilization on an MPM-C or an MPM-III, which degrades signaling performance. Therefore, to improve signalling performance, add the following line to the switch's command file (**mpmc.cmd** on the MPM-C and **mpm3.cmd** on the MPM-III):

```
atm_use_mbus=0
```

This line *must* be placed before the **cmInIt** line. See Chapter 11, "Managing Files," for more information on editing the command file.

◆ Note ◆

The default MPM-C command file (**mpmc.cmd**) includes the **atm_use_mbus=0** line.

Required Image Files

See the table below for the required images files for the MPM-C, FCSM-I, FCSM-II, and CSM Modules. (See Chapter 7, “OmniSwitch Switching Modules,” for the MPM, MPM-III, and frame-based switching modules.) You *must* load the image file (or files) listed for the corresponding module or it will not run.

If you are running the multiple-peer group version of PNNI, you *must* use the image file listed within parentheses instead of the one listed to the left. (For example, you would use the **cell_mpg.img** image file instead of the **cell.img** image file.) If you are running the single-peer group version of PNNI, do *not* use the files listed within parentheses. See Chapter 46, “Configuring and Monitoring PNNI,” for more information.

◆ Note ◆

On CSM modules, the **sonet.img** file is a required image file. On ATM access modules (ASM and ASM2 modules), you must load the **sonet.img** file to run SONET error collection. However, this image file is not required to run these modules.

Required Image Files

Module	Image File(s)
MPM-C	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), mpmc.img, sonet.img
FCSM I	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), sonet.img
FCSM II	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-A25-12 (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-A25-12 (MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-A25-24W (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-A25-24W (MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), sonet.img

continued on next page...

Required Image Files (continued)

Module	Image File(s)
CSM-155-8 (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-155-8 (with MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-155C-8 (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-155C-8 (MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-622 (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-622 (with MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-U (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-U (with MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-U+ (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-U+ (with MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-AB-155C (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-AB-155C (with MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-AB-155FM/FS/FH (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-AB-155FM/FS/FH (with MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), sonet.img
CSM-AB-DS3 (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), ds3e3drv.img
CSM-AB-DS3 (with MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), ds3e3drv.img
CSM-AB-E3 (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), ds3e3drv.img, sonet.img
CSM-AB-E3 (with MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), ds3e3drv.img, sonet.img

continued on next page...

Required Image Files (continued)

Module	Image File(s)
CSM-AB-DS1 (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), sonet.img, t1e1drv.img
CSM-AB-DS1 (with MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), sonet.img, t1e1drv.img
CSM-AB-E1 (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), sonet.img, t1e1drv.img
CSM-AB-E1 (with MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), sonet.img, t1e1drv.img
CSM-AB-CE-T1 (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), asmce.img, asmcedrv.img, cell.img (or cell_mpg.img), sonet.img, t1e1drv.img
CSM-AB-CE-T1 (with MPM-C)	asmc.img (or asmc_mpg.img), asmce.img, asmcedrv.img, cell.img (or cell_mpg.img), sonet.img, t1e1drv.img
CSM-AB-CE-E1 (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), asmce.img, asmcedrv.img, cell.img (or cell_mpg.img), sonet.img, t1e1drv.img
CSM-AB-CE-E1 (with MPM-C)	asmc.img (or asmc_mpg.img), asmce.img, asmcedrv.img, cell.img (or cell_mpg.img), sonet.img, t1e1drv.img
CSM-AB-IMA-DS1 (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), ima.img, sonet.img, t1e1drv.img
CSM-AB-IMA-DS1 (with MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), ima.img, sonet.img, t1e1drv.img
CSM-AB-IMA-E1 (MPM-1G or MPM-III)	asm.img (or asm_mpg.img), cell.img (or cell_mpg.img), ima.img, sonet.img, t1e1drv.img
CSM-AB-IMA-E1 (with MPM-C)	asmc.img (or asmc_mpg.img), cell.img (or cell_mpg.img), ima.img, sonet.img, t1e1drv.img
CSM-ABT-155F (MPM-1G or MPM-III)	asm_mpg.img (or asm_mpg.img), cell_mpg.img (or cell_mpg.img), sonet.img, text_cfg.img, pm_ctm.eexe
CSM-ABT-155F (with MPM-C)	asmc_mpg.img (or asmc_mpg.img), cell_mpg.img (or cell_mpg.img), sonet.img, text_cfg.img, pm_ctm.eexe

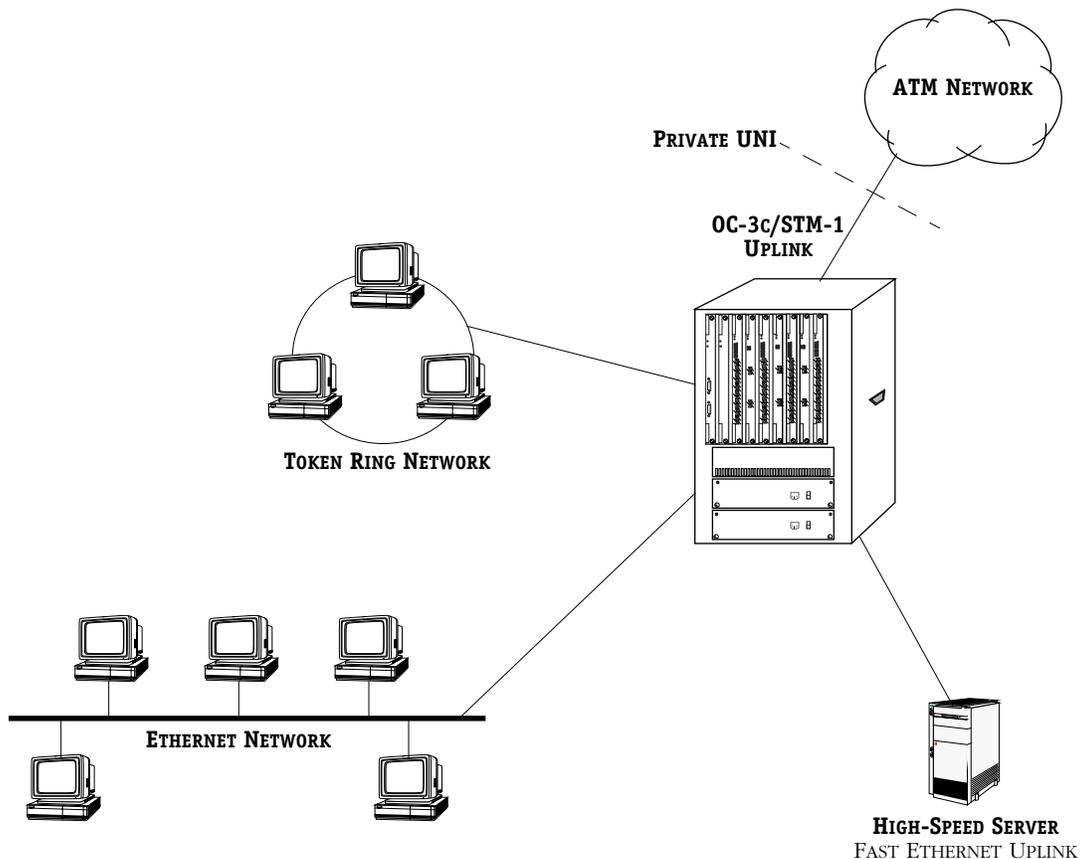
ATM Switching Applications and Configurations

With its embedded frame bus and cell matrix, the OmniSwitch is an ideal system for migrating from frame-based LAN interfaces, such as Ethernet and Token Ring, to cell-based ATM networks. It provides all the advanced LAN switching of an OmniSwitch and can be transformed into a pure ATM switch capable of supporting OC-3c/STM-1 and OC-12c/STM-4c connections that are compliant with current ATM standards. The following sections provide examples of OmniSwitch ATM switching applications.

Frame-Based LAN Switch With ATM Uplinks

The OmniSwitch can start as a pure LAN switch, switching frames from LAN interfaces such as Ethernet and Token Ring. It can also support ATM uplink connections that are compatible with User-to-Network (UNI) versions 4.0, 3.1, and 3.0 to provide comprehensive LAN-to-ATM internetworking. These ATM uplink connections provide connectivity to the native ATM network. When you want to add cell switching modules that provide OC-3c/STM-1 and OC-12c/STM-4c connections, you can add them at any time—the cell switching backplane is already in place.

The network in the illustration below shows an OmniSwitch switching traffic for Ethernet, Token Ring, Fast Ethernet, and ATM uplink interfaces. It serves as a LAN switch while having an uplink to the ATM network. At any time, it could be turned into an ATM switch. For a close-up view and the module mix of the OmniSwitch as a LAN switch, see *Pure LAN Switch* on page 40-12.



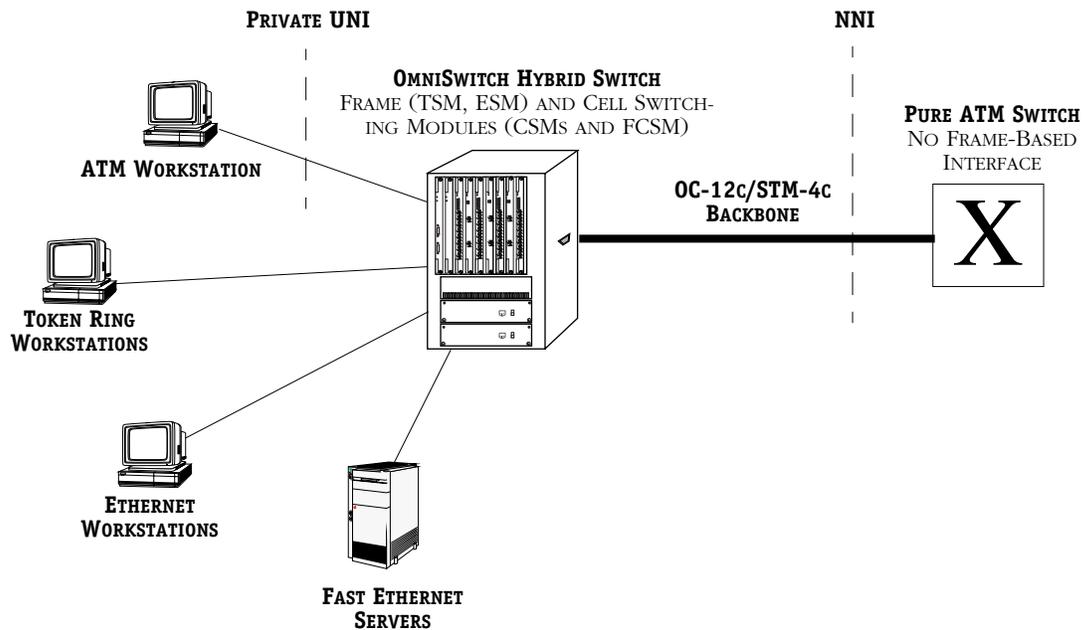
OmniSwitch as a Frame-Based LAN Switch

Hybrid LAN/ATM Switch

An intermediate step in the migration to an ATM network might require the OmniSwitch to support LAN and ATM switching in one chassis. This dual-functionality is possible since cell switching modules and frame switching modules can be installed in the same OmniSwitch chassis. LAN devices and networks can be connected to Ethernet, Token Ring, Fast Ethernet, and WAN modules and enjoy the benefits of high-speed, VLAN-capable any-to-any switching. At the same time, these LAN devices have access to the ATM network via the CSM modules installed in the same chassis.

In the network illustration below, the OmniSwitch chassis contains both cell and frame switching modules. (For a close-up view of this configuration and its module mix, see *Hybrid LAN/ATM Switch* on page 40-13.) It can switch LAN traffic among the Token Ring workstations, Ethernet workstations, and the Fast Ethernet server. All of these LAN devices are connected to frame switching modules, such as TSMs and ESMs.

In addition, the OmniSwitch provides ATM switching to the desktop for the ATM End Station (ES), which is connected directly to a CSM port. Another CSM port connects to an OC-12c/STM-4c backbone that links to a pure ATM switch.

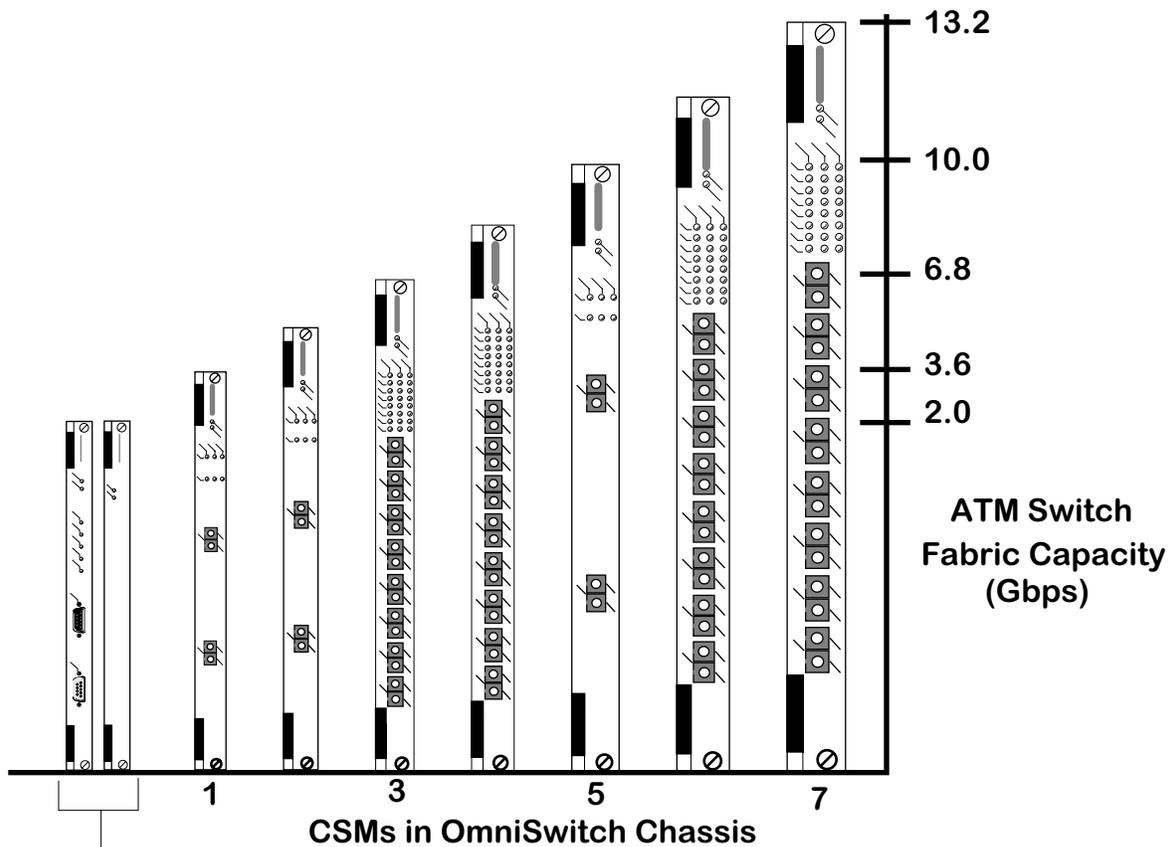


OmniSwitch as a Hybrid Frame and Cell Switch

Distributed Cell Switching Fabric

The OmniSwitch ATM cell matrix is fully distributed with no central switch component and no single point of failure. One advantage of this distributed fabric is that it can grow cost-effectively as your ATM network requirements grow; the aggregate 13.2 Gbps of switch fabric is distributed across all Cell Switching Modules (CSMs). As an ATM switch, the OmniSwitch can be scaled from 2.0 Gbps to 13.2 Gbps, in 1.6 Gbps increments.

Each CSM added to the switch provides an additional 1.6 Gbps of backplane capacity. Each CSM adds exactly as much capacity and buffers to the overall fabric as is required by its ports. A CSM module may contain eight (8) OC-3c/STM-1 ports or two (2) OC-12c/STM-4c ports. The chart below provides an idea of how the fabric capacity of the OmniSwitch scales with each new CSM module installed.



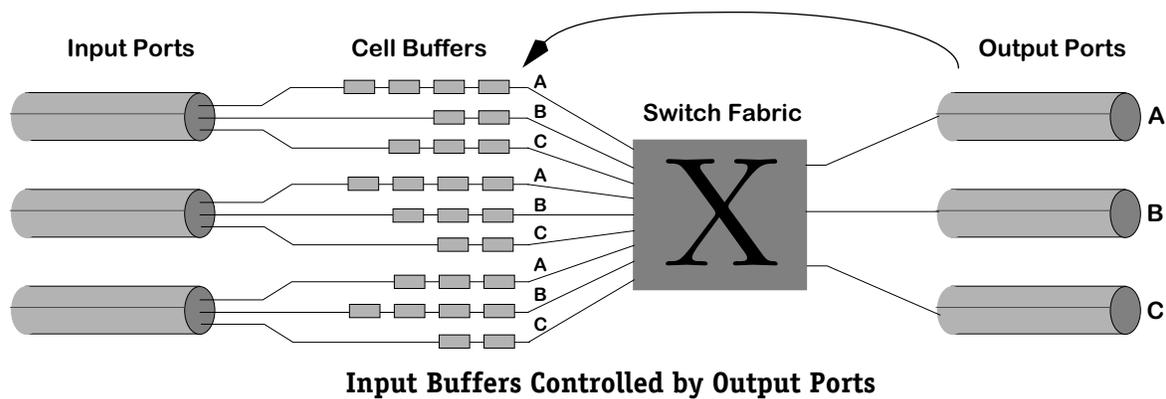
The MPM and FCSM modules are the base requirement in most cell switching configurations (PVC-only configurations do not require an FCSM). The MPM module is on the left and the FCSM is on the right.

Buffer Management

Cells enter the cell switching fabric on input ports and are switched to output ports. Sometimes collisions take place between cells when cells come in on two or more input ports that are destined for the same output port. This competition for output bandwidth may cause momentary input buffering or it could lead to sustained congestion.

Collisions on the cell fabric create the need for queueing, or buffering, where one or more cells must wait in line before being delivered to the output port. The queueing or buffer management scheme determines the throughput seen by the user. The OmniSwitch uses a dynamic input buffering with output control scheme. The buffers are physically located on the input ports but they are controlled by the destination output port.

Buffers are dynamically allocated based on a connection's Class of Service and the output port. Essentially, *the output port controls the input port buffers*. Each output port can see all traffic destined for it, and can determine how to schedule the release of this traffic based on Class of Service and fairness algorithms. The illustration below shows how cell buffers lie on input ports, but are actually managed by output ports.

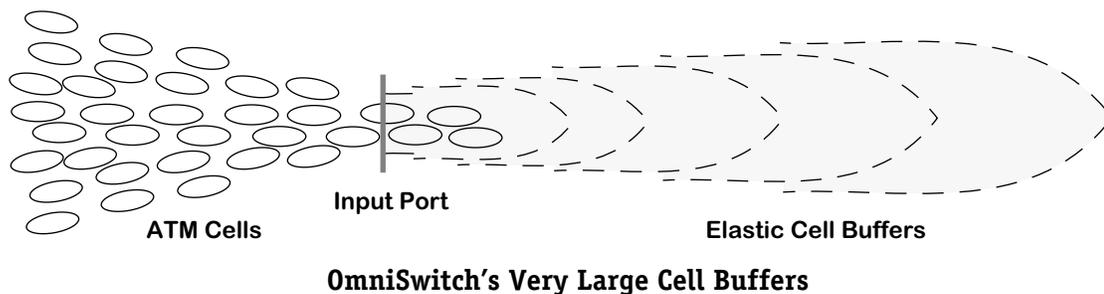


This method of buffer management provides completely non-blocking performance while cost effectively scaling buffer requirements as the system grows.

Cell Buffers

In campus and enterprise networks, about 95% of the traffic is bursty LAN-based data traffic. Buffer management must be designed knowing that networks will be characterized by massive, but momentary, traffic bursts. At other times, traffic activity may be quiet or may be mixed with isochronous voice and video traffic.

LAN-based traffic has been shown to respond poorly to cell loss due to congestion. In order to operate effectively in such a network environment, the OmniSwitch was designed with very large, efficiently managed cell buffers. Cell buffers need to be elastic enough to withstand massive bursts of data from large numbers of sources without resorting to congestion control or discarding cells. On CSMs, each OC-3c/STM-1 port has 8192 cell buffers and each OC-12c/STM-4c port has 131,072 cell buffers.

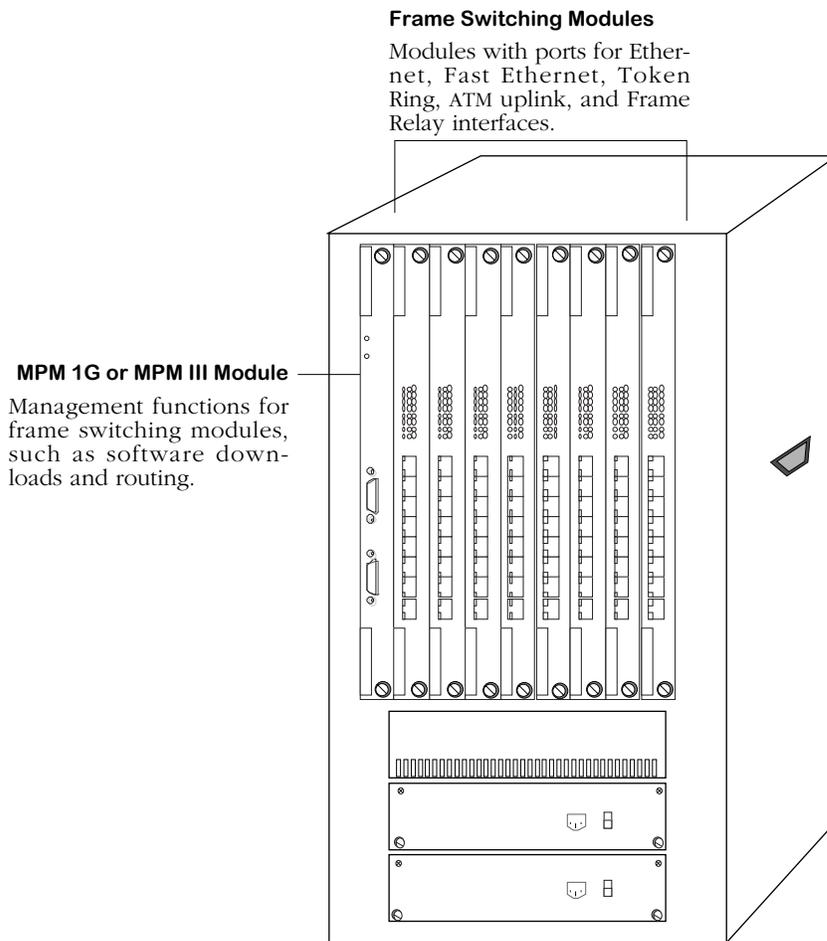


Module Mix for OmniSwitch Configurations

The mix of modules in your OmniSwitch chassis will vary depending upon whether you configure it as a pure LAN switch, a hybrid LAN/ATM switch, or a pure ATM switch. All configurations require an MPM 1G, MPM II, or MPM-C module, but not all require an FCSM module. The following sections and illustrations describe the differences between the three main OmniSwitch configurations.

Pure LAN Switch

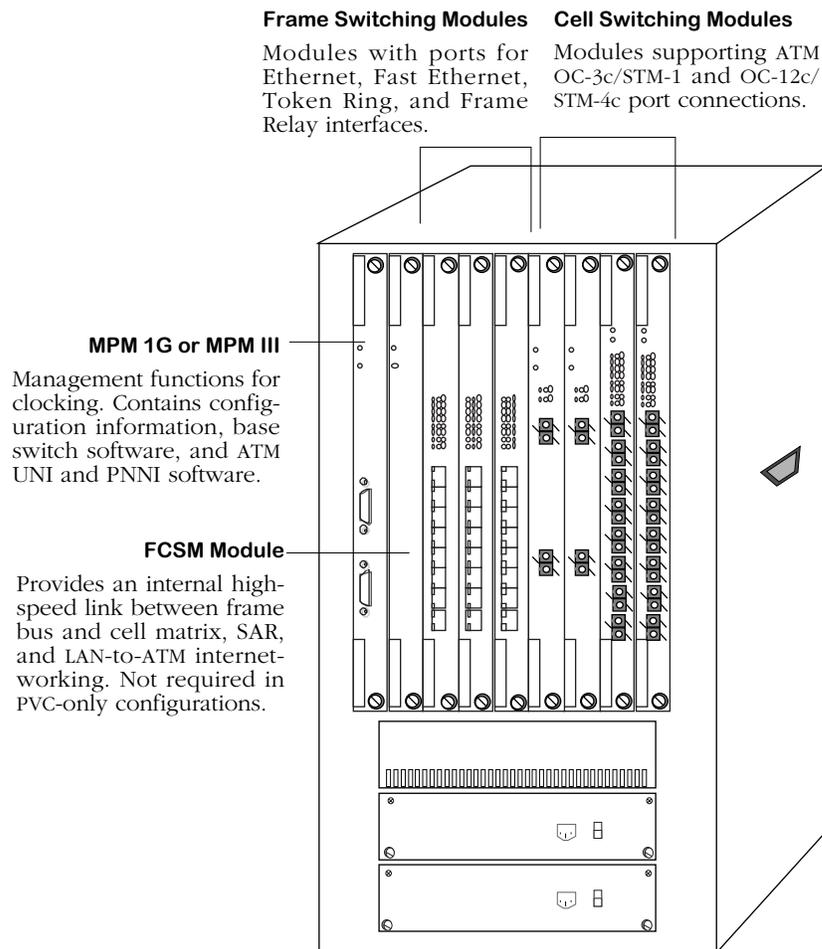
When the OmniSwitch is configured as a LAN switch it requires an MPM 1G or MPM III module and frame switching modules, such as Ethernet (ESM), Token Ring (TSM), and WAN (WSM) modules. (An MPM-C *cannot* be used in a pure LAN switch configuration.) In addition, you could also install ATM uplink (ASM) modules into this pure LAN switch. The illustration below points out the parts of a pure LAN switch configuration:



OmniSwitch as a Pure LAN Switch

Hybrid LAN/ATM Switch

When the OmniSwitch is configured as a hybrid LAN/ATM switch, it requires an MPM 1G or MPM III module, an FCSM module, frame switching modules, and Cell Switching Modules (CSMs). (An MPM-C *cannot* be used in a hybrid LAN/ATM switch configuration.) The MPM module must contain at least 16 MB of system memory. Both the frame switching modules and cell switching modules are supported by the OmniSwitch backplane. The FCSM module serves as an internal link between the cell and frame backplanes and provides complete LAN-to-ATM internetworking functions. In addition, the FCSM provides the SAR functionality on behalf of the MPM for call processing. The illustration below points out the major parts of a hybrid switch.



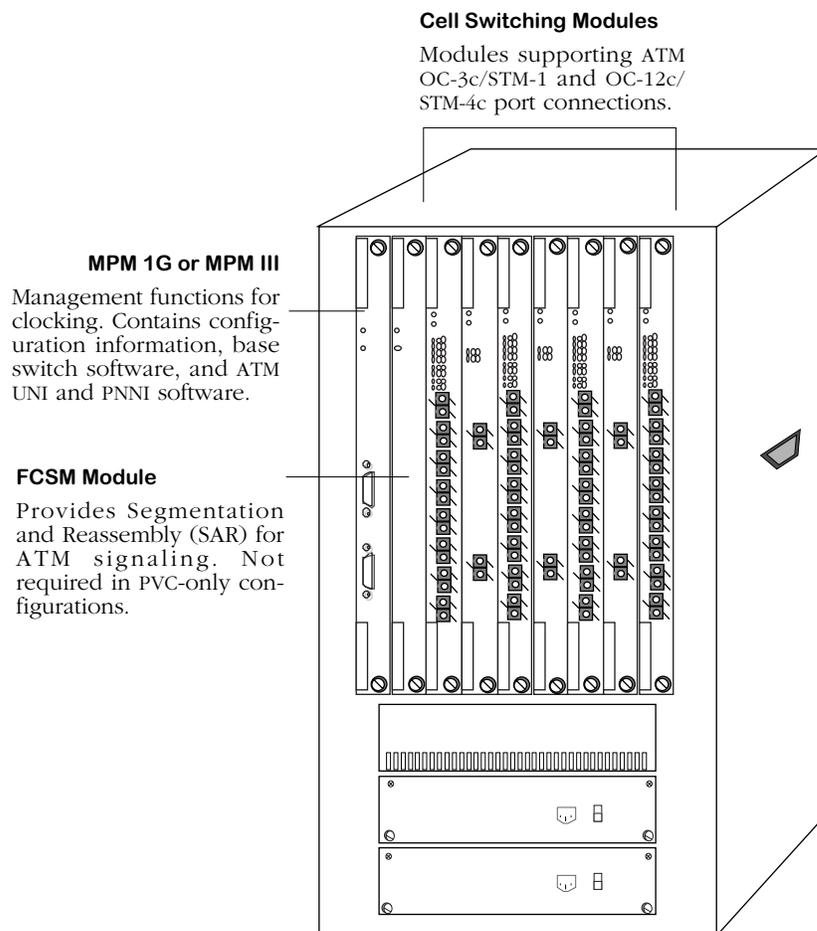
OmniSwitch as a Hybrid LAN/ATM Switch

Pure ATM Switch

When the OmniSwitch is configured as a pure ATM switch, it must have one of the following configurations:

- An MPM 1G or MPM III module, an FCSM module, and Cell Switching Modules (CSMs)
- An MPM-C and CSMs.

The MPM module must contain at least 16 MB of system memory. The FCSM and MPM-C provide call processing Segmentation and Reassembly (SAR) for the cell switching backplane. The illustration below points out the major parts of a pure ATM switch using an MPM and an FCSM. See *Omni-3ux with an MPM-C and Two CSMs* on page 40-23 for an illustration of a pure ATM switch with an MPM-C.



OmniSwitch as a Pure ATM Switch

Cell Switching Modules

The OmniSwitch Cell Switching Modules support ATM UNI 4.0, 3.1, and 3.0 and NNI (PNNI 1.0 or IISP) interfaces via OC-3c/STM-1 or OC-12c/STM-4c ports. Most CSMs are equipped with four (4) Input Output Processor (IOP) ASICs and one ATM fabric ASIC. (The FCSM I has one IOP, the FCSM II has two IOPs, and the CSM-U and CSM-U+ have three IOPs.) All port types support point-to-point and point-to-multipoint connections. Both Virtual Path Connections (VPCs) and Virtual Channel Connections (VCCs) are supported. VPI and VPI/VCI label assignment and management is supported for VPCs and VCCs, respectively.

The OmniSwitch supports Permanent Virtual Circuits (PVCs), Switched Virtual Circuits (SVCs), and soft PVCs. PVCs and soft PVCs are configurable through ATM menu software commands. SVCs are automatically set up by the network via PNNI. The configuration of PVCs is described in Chapter 41, “Managing Cell Switching Modules (CSMs),” and the configuration of soft PVCs is described in Chapter 42, “Advanced CSM Management.”

Each OC-3c/STM-1 port, in hardware, supports up to 4096 connections and each OC-12c/STM-4c port supports 65,536 connections. All ports support very large cell buffers. Each OC-3c/STM-1 port has enough capacity for 8192 cell buffers, and each OC-12c/STM-4c port has enough capacity for 131,072 cell buffers.

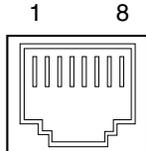
You may remove and insert CSM modules while the switch is running. This technique is referred to as “hot swapping.” When you hot swap, you must replace the CSM module with the same module type as the one you removed. See Chapter 7, “OmniSwitch Switching Modules,” for more information on hot swapping CSM modules.

CSMs cannot be installed in Slot 1 of an OmniSwitch chassis; they can only be installed in slots 2 and above. The Cell Switching Modules are as follows:

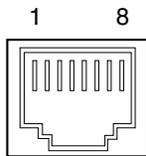
- FCSM I Frame-to-Cell Switching Module. Required in all OmniSwitch ATM switch configurations that use an MPM. Works in conjunction with the MPM to provide call processing Segmentation and Reassembly (SAR) and LAN-to-ATM internetworking.
- FCSM II The OC-12c/STM-4c version of the original FCSM.
- MPM-C Management Processing Module with cell switching matrix. In a wide-format chassis, the MPM-C can be used in place of an MPM and FCSM.
- CSM-155F Eight-port 155 Mbps cell switching module. Each port supports an OC-3c/STM-1 connection and can be factory-configured to support single mode or multimode fiber.
- CSM-622 Two-port 622 Mbps cell switching module. Each port supports an OC-12c/STM-4c connection and can be factory-configured to support single mode or multimode fiber.
- CSM-155C Eight-port 155 Mbps cell switching module. Each port supports an OC-3c/STM-1 connection on UTP cable.
- CSM-A25-12 Twelve-port ATM 25 Mbps cell switching module.
- CSM-A25-24 Twenty-four port ATM 25 Mbps cell switching module.
- CSM-U Universal cell switching module with three adapter board positions. Adapter boards include support for OC-3 fiber and copper ports, T1/E1 ports, DS3/E3 ports, T1/E1 circuit emulation ports, Stratum-3 hardware clocking, and Inverse Multiplexing over ATM (IMA).
- CSM-U+ An advanced version of the CSM-U that supports 0 to 7 bits for VPIs (the default is 4) and 8 to 14 for VCIs (the default is 10).

CSM Pinouts

The following figures and table illustrate the pinouts for copper-based connector ports.



CSM RJ-45 Specifications	
Pin Number	Standard Signal Name
1	Xmit Data +
2	Xmit Data -
3	
4	
5	
6	
7	Receive Data +
8	Receive Data -



CSM-CE RJ-48C Specifications	
Pin Number	Standard Signal Name
1	Tx_Ring
2	Tx_Tip
3	Chassis GND
4	Rx_Ring
5	Rx_Tip
6	Chassis GND
7	Chassis GND (A jumper is provided for connecting Pins 7 and 8 to the chassis ground, if required.)
8	Chassis GND (A jumper is provided for connecting Pins 7 and 8 to the chassis ground, if required.)

Frame-to-Cell Switching Module (FCSM)

The Frame-to-Cell Switching Module (FCSM) provides an internal link between the OmniSwitch backplane's frame bus and cell matrix. Since the MPM is not directly attached to the OmniSwitch cell switching fabric, the FCSM provides the Segmentation and Reassembly (SAR) functionality required for the cell backplane as well as LAN-to-ATM interworking. There are two versions of the FCSM. The FCSM I (also known as the FCSM-155) supports OC-3c/STM-1 connections and the FCSM II supports OC-12c/STM-4c connections.

The FCSM is required when the OmniSwitch is configured as a hybrid ATM-to-LAN interface switch. (It is not required for a pure frame switch configuration). In a hybrid configuration, the FCSM provides frame switching modules with a "link" to the cell matrix. In a pure ATM switch configuration, the FCSM provides call processing SAR functionality for the MPM module. The FCSM can be installed in any chassis slot except Slot 1.

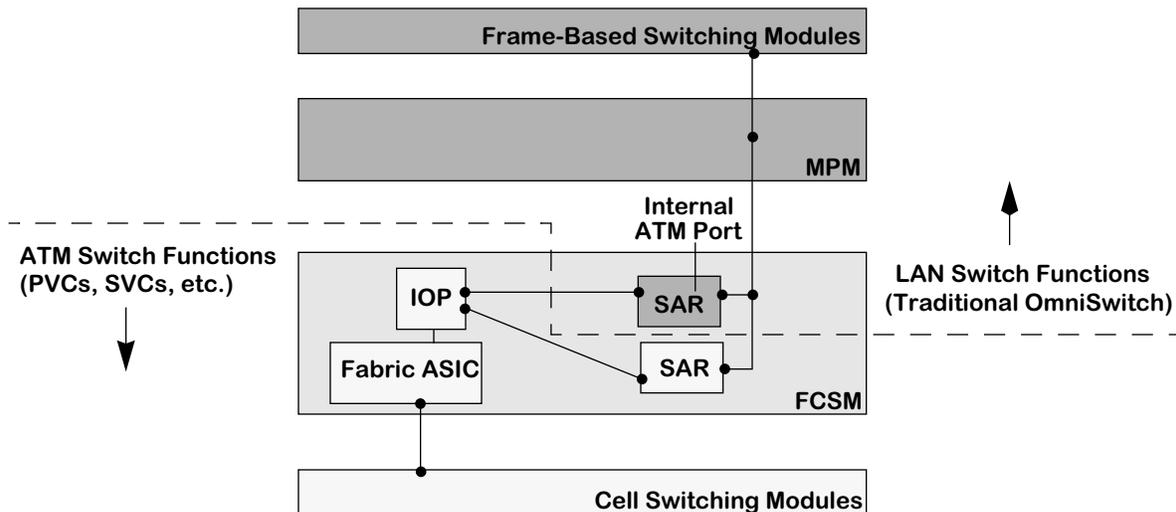
◆ Important Note ◆

The FCSM module *must* be installed before any Cell Switching Module (CSM); i.e., the FCSM must have a lower slot number than any CSM in the same chassis.

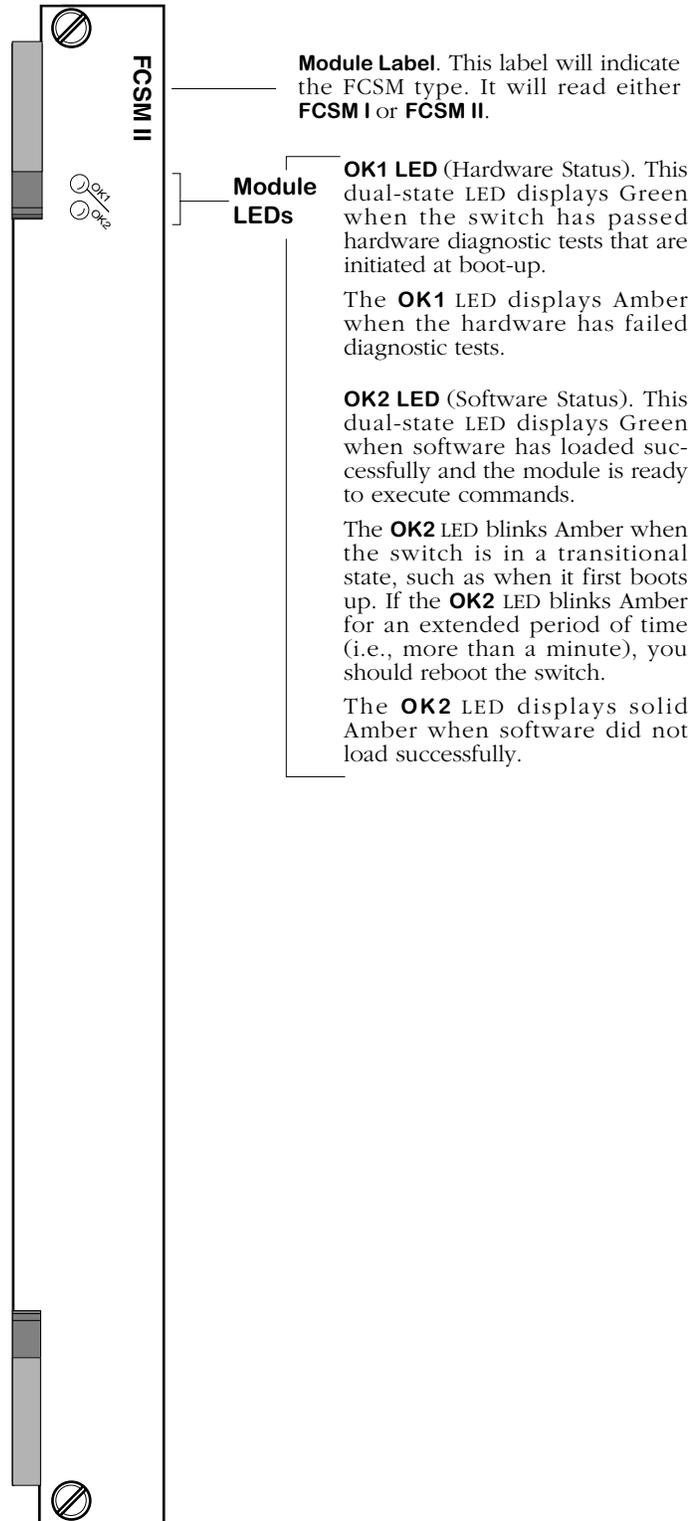
Although the FCSM does not contain any physical ports, it does contain an internal ATM port that can be viewed and configured through switch software. This port is functionally the same as an ASM module port. However, instead of connecting to an ATM switch through fiber cable, this logical port is hardwired into the ATM cell matrix. You can view statistics and configure ATM services, such as LAN Emulation and Classical IP and Trunking, on this internal port. By creating ATM services on this port, you provide a bridge between devices on LAN interfaces (Ethernet, Token Ring) and those connected to the native ATM network.

This internal ATM access port is directly connected to an OC-3c/STM-1 or OC-12c/STM-4c port that is functionally the same as a CSM port. Logically, these two ports are two halves of the same port; User Interface software displays them as part of the same port. The FCSM I also contains a second internal port that also contains an ATM access half and a CSM half. This second port is used to pass management cells for signaling, ILMI, and PNNI.

The illustration below shows the parts of an FCSM and how the FCSM interacts with other modules in an OmniSwitch chassis:



FCSM Provides the Link Between Frame Bus and Cell Matrix



The Frame-to-Cell Switching Module

FCSM I (FCSM-155)

The FCSM I contains two RISC processors used for LAN-to-ATM internetworking (i.e., MAC layer translations). These processors provide the same function as the OmniSwitch ASM uplink modules. The FCSM also contains two OC-3c/STM-1 SARs. One SAR has 0.5 MB for signalling functions and one has 2 MB for data. Finally, the FCSM I contains an Input Output Processor (IOP) ASIC and an ATM fabric ASIC.

◆ Note ◆

You *cannot* use an FCSM I with an MPM-C.

FCSM I Redundancy

Release 3.3 and later software supports redundant FCSM I (also referred to as the FCSM-155) module configurations. This feature will automatically switch control to a secondary FCSM I if the primary FCSM I fails. Redundant FCSM II configurations are not currently supported.

By default, the FCSM I inserted into the lowest slot number will be the primary FCSM I. An FCSM I should *not* be installed in Slot 1. Both FCSMs should be inserted before any CSMs (i.e., the FCSMs must have a lower slot number than any CSM in the same chassis).

For example, you could install the primary FCSM I in Slot 2 and the secondary FCSM I in Slot 4 as long as you did not install a CSM module in Slot 3. In this setup, you could install an Ethernet or other non-CSM module in Slot 3.

There are two methods for setting up redundant FCSMs. Both methods require you to set up identical ATM services (if applicable) on each FCSM.

The first method is recommended, but requires two power cycles. The second method requires only one power cycle, uses hot swapping, and exercises the redundant FCSM configuration. Alcatel recommends the first method as long as your network environment can tolerate two power cycles. If you want to avoid the second power cycle, then use the second method.

Redundancy Configuration Method 1: Two Power Cycles

This procedure requires you to power up and power down the switch twice. Make sure you perform this procedure during a time when these power cycles will not disrupt network use.

Begin this procedure with the primary FCSM installed in the chassis. By default, the FCSM inserted into the slot with the lowest number will be the primary FCSM. An FCSM should not be installed in Slot 1 and FCSMs must be inserted before any CSMs (i.e., the FCSMs must have a lower slot number than any CSM in the same chassis).

If your switch is powered down, begin by installing the primary FCSM in the appropriate slot. If your switch is already operational, issue the following command before inserting the FCSM:

```
swap on
```

This command allows you to hot swap modules in the chassis; it is explained in more detail in Chapter 10, "Configuring Management Processor Modules."

1. Configure all required ATM services, such as LAN Emulation (LANE), on the primary FCSM. (If this is an existing FCSM I, you may have already configured these services.) Keep good records of all configuration parameters because you will need to re-enter them on the secondary FCSM I.
2. Power down the switch.

3. Pull the primary FCSM away from the backplane of the switch chassis. You do not need to remove the module from the chassis, but it should not be connected to the backplane.
4. Insert the secondary FCSM into the slot where it will reside. This slot number should be higher than the slot number used for the primary FCSM. However, the secondary FCSM should be inserted before any CSM modules in the same switch chassis.
5. Power up the switch.
6. Configure all ATM services on the secondary FCSM that you configured during Step 2 for the primary FCSM. It is important that the configurations match so that, in case of a switch-over, the same services will be supported once the secondary FCSM takes over.
7. Power down the switch.
8. Re-insert the primary FCSM into the same slot where it resided when you configured services in Step 1. The secondary FCSM should still be installed in the switch.
9. Power up the switch. Your redundant FCSM configuration is now operational.

Redundancy Configuration Method 2: One Power Cycle

The procedure requires you to power down and power up the switch once. Use this procedure if your network cannot tolerate the two power cycles required by Method 1.

Begin this procedure with both the primary and secondary FCSMs installed in the chassis. By default, the FCSM inserted into the slot with the lowest number will be the primary FCSM. Neither FCSM should be installed in Slot 1 and both FCSMs should be inserted before any CSMs (i.e., the FCSMs must have a lower slot number than any CSM in the same chassis).

If your switch is powered down, begin by installing the two FCSMs in the appropriate slots. If your switch is already operational, issue the following command before inserting an FCSM:

```
swap on
```

This command allows you to hot swap modules in the chassis; it is explained in more detail in Chapter 10, "Configuring Management Processor Modules."

1. Configure all needed ATM services, such as LAN Emulation (LANE), on the primary FCSM. Keep good records of all configuration parameters because you will need to re-enter them on the secondary FCSM.
2. Enter the following command:

```
swap on
```

The following message will display:

```
Swap is ON for 5 minutes
```

3. Pull the primary FCSM away from the backplane of the switch chassis. You do not need to remove the module from the chassis. Messages similar to the following will display:

```
Module removed from slot 3  
Bringing down primary FCSM on slot 3.....  
Bringing up secondary FCSM on slot 4.  
Initializing slot 4, iop 0, Initializing Fabric.  
complete
```

These messages indicate that the secondary FCSM took over once the primary FCSM was removed from the switch backplane.

4. Configure all ATM services on the secondary FCSM that you configured during Step 2 for the primary FCSM. It is important that the configurations match so that, in case of a switch-over, the same services will be supported once the secondary FCSM takes over.
5. Power down the switch.
6. Re-install the primary FCSM into the same slot from which you removed it in Step 3.
7. Power up the switch. Once the switch comes back up, your redundant FCSM configuration will be operational.

What Happens When an FCSM Fails

Before a primary FCSM I fails the switch will attempt to ping it before bringing it down. Messages similar to the following display during the failure of a primary FCSM and the switch-over to the secondary FCSM:

```
Pinging module 3
Pinging module 3
Pinging module 3
Pinging module 3
Bringing down primary FCSM on slot 3.....
Bringing up secondary FCSM on slot 4.
Initializing slot 4, iop 0, Initializing Fabric.
complete
```

After a primary FCSM I fails, its LEDs will be off and its status will read **Disabled** in the **slot** command. The following screen shows a **slot** command display with a primary FCSM, which has just failed, in slot 3 and a secondary FCSM, which just took over, in slot 4:

Slot	Module-Type Part-Number	Adm-Status Oper-Status	HW Rev	Board Serial #	Mfg Date	Firmware-Version Base-MAC-Address
1*	MPM-II 5012013	Enabled Operational	A	70201177	01/08/97	3.3 00:20:da:04:21:f0
2	Empty					
3	FCSM 5012906	Disabled Problem	A2	71750011	04/25/97	3.3 00:20:da:7e:fe:50
4	FCSM 5012906	Enabled Operational	A2	71337442	03/29/97	3.3 00:20:da:7b:1e:30
5	Empty					
6	Empty					
7	Ether/8 50000014	Enabled Operational	B	192	01/25/95	3.3 00:20:da:03:06:30
8	CSM-OC12-S 5013306	Enabled Operational	A1	1	06/24/97	3.3 None
9	Empty					

After a primary FCSM goes down and the secondary FCSM takes over, you must first power down the switch before replacing the failed primary FCSM with a new primary FCSM.

FCSM II

The FCSM II contains a custom ASIC for LAN-to-ATM internetworking (i.e., MAC layer translations). This processor provides the same function as an OmniSwitch ASM uplink module. The FCSM also contains one OC-12c/STM-4c SAR. Finally, the FCSM contains two Input Output Processor (IOP) ASICs and an ATM fabric ASIC. It is recommended that the FCSM II be installed in a chassis slot, except Slot 1, with a lower number than any installed CSM modules.

The FCSM II differs from the FCSM I in that it contains only one internal port that is visible to the user through software. The FCSM I contains two internal ports, one of which handles management signaling while the other handles data transmission. On the FCSM II, all management signaling and data transmission occur over the same internal port.

◆ Important Note ◆

Signaling is not supported on non zero VPIs on the FCSM II.

In Release 4.3 and later the FCSM II can be reset with the **reset** command without rebooting the switch. See Chapter 58, "Running Hardware Diagnostics," for more information on the **reset** command.

FCSM II Technical Specifications	
Standards Supported	ATM Forum User-to-Network Interface 4.0, 3.1, and 3.0 ISO Q.2931 ATM LAN Emulation Client V1.0 ITU-T I.432 and G.957 Bellcore TR-NWT-000253 Private Network-to-Network Interface (PNND) 1.0 Interim Interswitch Protocol (IISP)
Data Rate	Up to 500 Mbps
Maximum Frame Size	8,000 bytes (ASM half)

◆ Note ◆

The FCSM II requires an MPM III or an MPM 1G, Revision B16 or later. You *cannot* use an FCSM II with an MPM II or an MPM-C.

The Cell Switching Management Processor Module (MPM-C)

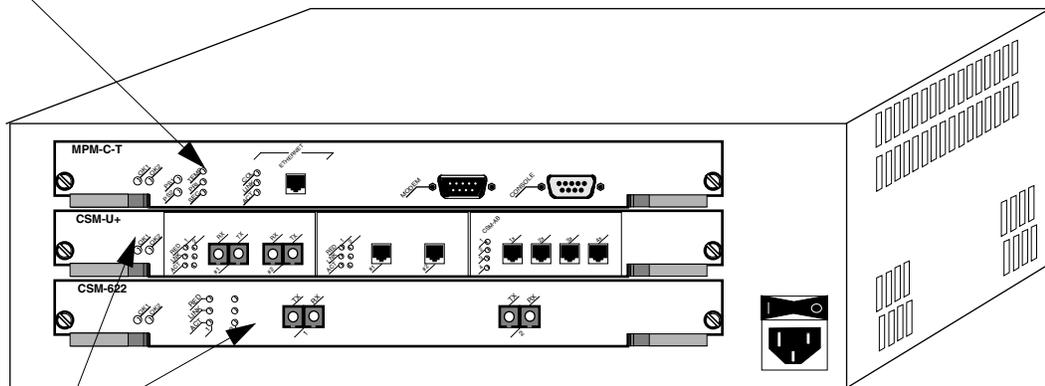
The MPM-C combines the management functions of an MPM 1G and the connection to the cell matrix provided by an FCSM. As a management module, the MPM-C provides such system services as maintenance of user configuration information, downloading of switching module software, basic bridge management functions, the SNMP management agent, and access to the User Interface software.

The MPM-C can only be used with Cell Switching Modules (CSMs). You cannot install an MPM-C with frame-based switching modules (e.g., ESMs, TSMs, FSMs).

◆ **Note** ◆

The MPM-C can be installed in a wide-format chassis (Omni-3wx, Omni-5wx, or Omni-9wx) only.

Cell Switching Management Processor Module (MPM-C)



Cell Switching Modules (CSMs)

Omni-3wx with an MPM-C and Two CSMs

The MPM-C contains one OC-3c/STM-1 Segmentation and Reassembly (SAR), which provides call processing SAR functions (i.e., “FCSM” functionality). In addition, the MPM-C has one Input Output Processor (IOP) ASIC, which communicates with the cell switching fabric. In a fully loaded Omni-9wx, the MPM-C has a 13.2 Gbps cell fabric matrix. It supports OC-3c/STM-1 and OC-12c/STM-4c connections, integrated call setup, and PNNI processing.

Although the MPM-C does not have any physical ATM ports, it does have a single *logical* port that can be used for management purposes. See *ATM Services on the MPM-C* on page 40-29 for more information.

MPM-C Technical Specifications	
Flash Memory	8 MB (expandable to 32 MB)
SIMM (DRAM) Memory	32 MB (expandable to 128 MB)
SDRAM Memory	64 MB
Cell Switching Fabric	Up to 13.2 Gbps (aggregate)
Serial Ports	2 (1 male DB9 modem connector and 1 female DB9 console connector)
Ethernet (10 Mbps) Switch Management Ports	1 copper RJ-45 or fiber (ST) port for switch management functions.
Standards Supported	ATM Forum User-to-Network Interface 4.0, 3.1, and 3.0 ISO Q.2931 ATM LAN Emulation Client V1.0 ITU-T I.432 and G.957 Bellcore TR-NWT-000253 Private Network-to-Network Interface (PNNI) 1.0 Interim Interswitch Protocol (IISP)
Maximum Frame Size	8,000 bytes ("FCSM" half)
Power Consumption	3.5 amps

In an Omni-3wx, you can install up to two (2) Cell Switching Modules (CSMs). In an Omni-5wx, you can install up to four (4) CSMs. And in an Omni-9wx, you can install up to eight (8) CSMs.

◆ **Note** ◆

The MPM-C *must* be installed in Slot 1 or Slot 2. In addition, you *cannot* install a CSM in Slot 1.

Warning Label. This label indicates that the module contains an optical transceiver (MPM-C-FL only).

OK1 (Hardware Status). This dual-state LED is on Green when the MPM-C has passed power-on hardware diagnostics successfully. On Amber when the hardware has failed diagnostic tests. If the **OK1** LED is alternating Green and Amber, then file system compaction is in progress.

Caution

Do not power down the OmniSwitch or insert any modules while the **OK1** LED is alternating Green and Amber. If you do, file corruption may result and you will not be able to restart the switch.

OK2 (Software Status). Blinking Green when the MPM-C has successfully loaded software to the switching modules. Blinking Amber when the MPM-C is in a transitional state, such as when it first boots up. If the **OK2** LED blinks Amber for an extended period of time (i.e., more than a minute), then you should reboot the switch.

Caution

Do not insert or remove any modules while the MPM-C **OK2** LED is blinking Amber. If you do, file corruption may result and you will not be able to restart the switch.



Label. This label will indicate the Ethernet management port type. It will read either **MPM-C-FL** (multimode fiber Ethernet port) or **MPM-C-T** (copper RJ-45 Ethernet port).

PS1 (Power Supply 1 Status). This dual-state LED is on Green when the switch is receiving the proper voltage from Power Supply 1. It is on Amber when Power Supply 1 is on, but not supplying the correct amount of voltage to power the switch, or is installed and turned off. The **PS1** LED is Off when the Power Supply 1 is not present.

PS2 (Power Supply 2 Status). This dual-state LED is on Green when the OmniSwitch is receiving the proper voltage from Power Supply 2. It is on Amber when Power Supply 2 is on, but not supplying the correct amount of voltage to power the switch, or is installed and turned off. The **PS2** LED is Off when Power Supply 2 is not present.

TEMP (Temperature). On Yellow to warn that the internal switch temperature is approaching maximum operating limits. Note that this LED comes on *before* the temperature limit is reached.

PRI (Primary MPM-C). On Green when this MPM-C is the active, or controlling, MPM-C. It is also on Green when this is the only MPM-C installed in the switch.

SEC (Secondary MPM-C). On Green when this MPM-C is the secondary MPM-C in a redundant MPM-C configuration. As the secondary MPM-C, this module is in hot standby mode.

Cell-Switching Management Processor Module (MPM-C) Status LEDs

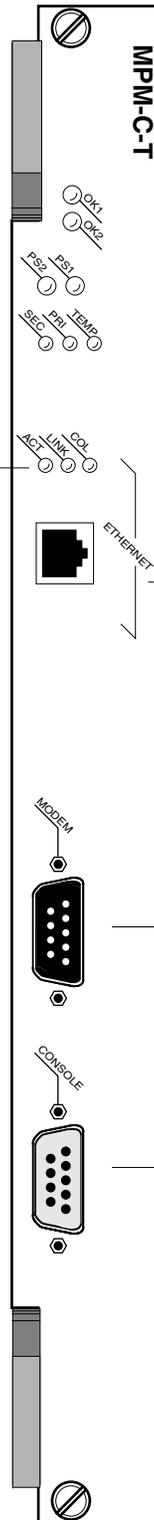
The MPM-C module includes one row of LEDs for the Ethernet management port.

ACT (Activity). On Green when data is transmitted or received on the Ethernet management port.

LINK (Link Status/Disabled). On Green continuously when a good cable connection exists. Off when a good connection does not exist.

COL (Collision). On Yellow when a collision has been detected on the port.

Port LEDs



Ethernet Management Port. Copper RJ-45 (shown here) and fiber ST ports are available for rapid switch file transfers and network management functions.

Modem Connector. A male serial DB-9 DTE connector for switch file transfers and network management functions.

Console Connector. A female serial DB-9 DCE connector for switch file transfers and network management functions.

MPM-C Management Connectors

MPM-C Serial and Ethernet Management Ports

You can gain access to switch management software through one of the two serial (RS-232) ports on the MPM-C or the Ethernet management port. The two serial ports are configured with 9-pin “D” connectors (DB-9) per the IBM AT serial port specification. One port, called the “modem” port, is male and the other, called the “console” port, is female. See (*MPM-C Management Connectors* on page 40-26) for illustrations of these ports.

The modem port is a Data Terminal Equipment (DTE) connector, which is typically connected to a modem. You can also connect directly from this port to a PC or terminal with a standard null-modem cable available in most computer equipment stores.

◆ **Note** ◆

The modem port is hard-wired for DTE communication; you do not need to set any jumpers.

The console port is a Data Communication Equipment (DCE) connector, which can be directly connected to a PC, terminal, or printer.

Ethernet Management Port

The MPM-C also supports an out-of-band Ethernet port for high-speed uploads and switch management functions. With this port, you can access the OmniSwitch over a network via Telnet or FTP. See the table below for available Ethernet management port types.

MPM-C Module	Ethernet Management Port Type (Cable Type)	Max. Cable Distance
MPM-C-T	RJ-45 (UTP)	100 meters
MPM-C-FL	ST (Multimode fiber)	2 kilometers

The Ethernet management port has a default IP address of 192.168.11.1, which can be used for initial connectivity. You can use the Boot prompt or the **ethernetc** command to change this address. See Chapter 10, “Configuring Management Processor Modules,” for more information on the **ethernetc** command and see Appendix A, “The Boot Line Prompt,” for documentation on configuring the Ethernet management port with the boot prompt.

Configuring MPM-C Serial Ports

The serial communications parameters for the two MPM-C serial ports are set by default to the following:

- 9600 bits per second (bps)
- 8 data bits
- 1 stop bit
- no parity
- no hardware flow control (Windows)

Each serial port supports serial data rates of 1200, 9600, 19200, and 38400 bps. However, you must remove the default baud rate shunt (E1), which fixes the baud rate at 9600 bps, before you can change the baud rate. This shunt is located near the front end of the MPM-C's circuit board, just to the right of the Ethernet management port.

To change the serial port configuration parameters, use the **ser** command, which is described in detail in Chapter 10, "Configuring Management Processor Modules."

Flash Memory and OmniSwitch Software

Flash memory on the MPM-C holds the OmniSwitch's executable images and configuration data. When a switching module comes online, the MPM-C downloads the appropriate image file for that module to that module's memory. Image files (those with the **img** extension) contain executable code for different switching modules and software features. See Chapter 6, "The Management Processor Module (MPM)," for more information on image files.

MPM-C Redundancy

You can configure an OmniSwitch with redundant MPM-Cs. For MPM functions (e.g., switch management), the MPM-C operates in the same manner as a standard MPM. For "FCSM" functionality (e.g., ATM services), the MPM-C functions in ways very similar to the FCSM I. See the subsections below for descriptions of these two types of redundancy.

Redundancy for MPM Functions

Each MPM-C in a redundant configuration stores information for the switch. If one MPM-C fails, the other MPM-C automatically assumes all management responsibilities. After initialization, the new MPM-C will read the configuration information from the existing MPM-C as long as you set automatic configuration synchronization to active. Any virtual paths and/or virtual circuits you created will be saved in the configuration files if automatic configuration synchronization is active. See Chapter 6, "The Management Processor Module (MPM)," for more information on redundancy for MPM functionality.

Redundancy for FCSM Functions

Follow the steps below to configure "FCSM" redundancy (i.e., configuring redundant ATM services) on the MPM-C.

1. Configure all required ATM services, such as LAN Emulation (LANE), on the primary MPM-C. Keep good records of all configuration parameters because you will need to re-enter them on the secondary MPM-C.
2. Configure all ATM services on the secondary MPM-C. It is important that the configurations match so that, in case of a switch-over, the same services will be supported once the secondary MPM-C takes over.

ATM Services on the MPM-C

Currently, you can configure a single LANE (Ethernet or Token Ring) client, Classical IP (CIP), or Point-to-Point (PTOP) services on an MPM-C; however, VLAN cluster, Alcatel-proprietary ATM trunking, and 1483 scaling services are *not* supported.

A single LANE Client (LEC) or PTOPT service can be used for switch management purposes. The service's IP address can be used to telnet, FTP, ping, SNMP, etc., to and from the switch. UI commands to create, view, modify, and delete ATM services (**cas**, **vas**, **mas**, and **das**, respectively) operate on an MPM-C. If you wanted to create a PTOPT service on an MPM-C in slot 1, for example, you would enter

```
cas 1/1
```

at the system prompt. See Chapter 36, "Configuring ATM Services," for more information on ATM services command.

CSM-155F

The CSM-155 Cell Switching Module (CSM) contains eight full-duplex SONET/SDH STS-3c ports that use fiber SC connectors. The ports support the OC-3c/STM-1 standard data rate of 155 Mbps. The CSM-155 can be factory configured with single mode or multimode fiber connectors. The single mode version is referred to as the CSM-155-8S; the multimode version is referred to as the CSM-155-8. There is also a version with six multimode and two single mode connectors referred to as the CSM-155-6M2SW. Multimode and single mode connectors are differentiated by color: multimode connectors are black, single mode connectors are blue.

Each of the eight OC-3c/STM-1 ports supports up to 4096 virtual circuits (either Virtual Paths or Virtual Channels). In addition, each CSM-155 supports a total of 8192 point-to-multipoint virtual circuits. The cell buffer size for each physical port is 8192 cells.

The CSM-155 is suited for either direct connections to ATM workstations, backbone connections, or as an NNI link to a larger backbone. High-performance ATM workstations, servers, LAN switches, and routers can connect directly to CSM-155 ports; the CSM-155 can then connect into an ATM network that might support a larger backbone.

CSM-155 Technical Specifications	
Number of ports	8 SONET/SDH
Connector Type	SC
Standards Supported	ATM Forum User-to-Network Interface 4.0, 3.1, and 3.0 ITU-T I.432 and G.957 ANSI T1.105 Bellcore TR-NWT-000253 ATM Forum Traffic Management 4.0 Private Network-to-Network Interface (PNNI) 1.0 Interim Interswitch Protocol (IISP)
Data Rate	155 Mbps
Virtual Circuits Supported	4096 point-to-point per port; 8192 point-to-multipoint per CSM-155
Cell Buffer Size	8192 per port
Connections Supported	OC-3c/STM-1 connections to ATM stations, backbones.
Optical output power	Multimode: -20 to -14 dBm Single mode: -15 to -8 dBm
Optical receiver sensitivity	Multimode: -29 to -14 dBm Single mode: -31 to -8 dBm
Cable Supported	Multimode: 62.5 micron multimode fiber Single mode: intermediate-reach single-mode fiber
Cable Distance	Multimode: 2 km Single mode: 24 km

◆ **Special Note** ◆

The single mode version of this module has been deemed:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

Warning Label. This label indicates that the module contains an optical transceiver.

The CSM-155 modules include one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number.

RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the CSM module is plugged in, but no cable has been connected.

LINK (Link Status/Disabled). On Green when the corresponding port is enabled and a signal is present. Flashing Green when the corresponding port is disabled and a signal is present. This LED will be off when the port is disabled and no signal is present.

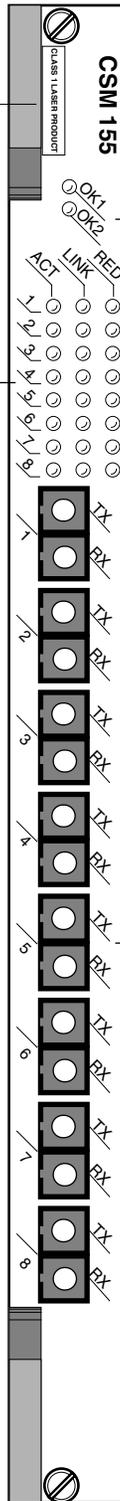
ACT (Activity). On Green when data is transmitted or received on the corresponding port.

Port LEDs

Module LEDs

Module Label. This label will indicate the CSM-155F type. It will read either **CSM 155 mm** (multimode cable) or **CSM 155 sm** (single mode cable).

Please refer to *Frame-to-Cell Switching Module (FCSM)* on page 40-17 for further information on these LEDs.



SC connectors will be color coded to indicate multimode (Black) or single mode (Blue).

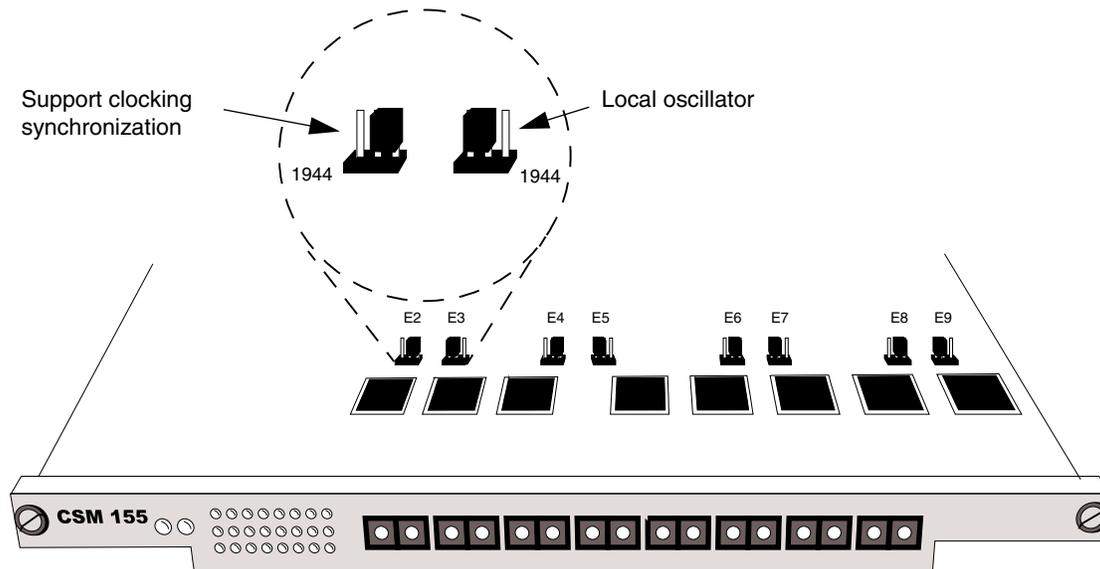
Cell Switching Module With Eight OC-3c/STM-1 Ports

Jumper Settings

Each of the eight ports on the CSM-155 board has a jumper (E2-E9) associated with it. Each jumper is labeled **1944** either to the left or to the right of the jumper pins. These jumpers enable you to configure whether the clock source is software controlled. If the middle pin is jumpered to the pin closest to the **1944** label, then software selection of the clocking mode is enabled. If the middle pin is jumpered to the “unlabeled” (i.e., furthest from the **1944** label), then the clocking mode is set to local oscillator only regardless of the software setting. (For more information on setting the clocking source through software, refer to Chapter 45, “Clocking ATM Networks.”)

Note

Some older versions of this module may not support clock synchronization. If you have any questions, contact Technical Support.



CSM-155 Clock Source Jumper Settings

Note

If your board includes Jumper E1, note that this jumper is set at the factory, and should not be changed.

CSM-622

The CSM-622 Cell Switching Module (CSM) contains two full-duplex SONET/SDH STS-12c ports that use fiber SC connectors. The ports support the OC-12c/STM-4c standard data rate of 622 Mbps. The CSM-622 can be factory configured with single mode or multimode fiber connectors. The intermediate-reach single mode version is referred to as the CSM-622-2SE; the long-reach single mode version is referred to as the CSM-622FSH-2SE; the multimode version is referred to as the CSM-622-2E. Multimode and single mode connectors are differentiated by a color code: multimode connectors are black, long-reach single mode connectors are yellow, and intermediate-reach single mode connectors are blue.

Each of the two OC-12c/STM-4c ports can support up to 4096 virtual circuits (either Virtual Paths or Virtual Channels) per port. In addition, each CSM-622 supports a total of 16,000 point-to-multipoint virtual circuits. The cell buffer size for each physical port is 131,072 cells.

The CSM-622 is suited for high-performance backbone connections within an ATM network. The OmniSwitch where this module is installed may also contain OC-3c/STM-1 links that connect high-performance workstations or backbones into the OmniSwitch; the CSM-622 might serve as a backbone trunk for these OC-3c/STM-1 connections.

CSM-622 Technical Specifications	
Number of ports	2 SONET/SDH
Connector Type	SC
Standards Supported	ATM Forum User-to-Network Interface 4.0, 3.1, and 3.0 ITU-T I.432 and G.957 Bellcore TR-NWT-000253 ATM Forum Traffic Management 4.0 Private Network-to-Network Interface (PNND) 1.0 Interim Interswitch Protocol (IISP)
Data Rate	622 Mbps
Virtual Circuits Supported	4096 point-to-point/port; 16,000 point-to-multipoint/CSM-622
Cell Buffer Size	131,072 per port
Connections Supported	OC-12c/STM-4c connections to ATM stations, backbones.
Optical output power	Multimode: -20 to -14 dBm Single mode (intermediate reach): -15 to -8 dBm Single mode (long reach): -3 to 2 dBm
Optical receiver sensitivity	Multimode: -26 to -14 dBm Single mode (intermediate reach): -28 to -8 dBm Single mode (long reach): -28 dBm (minimum), -30 dBm (typical)
Cable Supported	Multi-Mode: 62.5 micron multimode fiber Single mode (intermediate reach): intermediate-reach single-mode fiber Single mode (long reach): long-reach single-mode fiber
Cable Distance	Multimode: 500 meters Single mode (intermediate reach): 15 km Single mode (long reach): 40 km

◆ **Special Note** ◆

The single mode version of this module has been deemed:

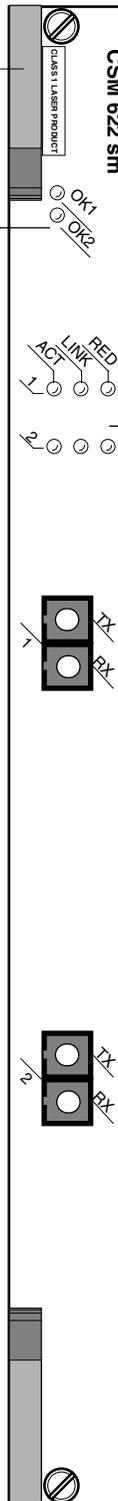
CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

Warning Label. This label indicates that the module contains an optical transceiver.

Please refer to *Frame-to-Cell Switching Module (FCSM)* on page 40-17 for further information on these LEDs.

SC connectors will be color coded to indicate multimode (Black), long-reach single mode (Yellow), or intermediate-reach single mode (Blue).



Module Label. This label will indicate the CSM-622 type. It will read either **CSM 622 mm** (multimode-reach cable), **CSM 622 sm** (intermediate-reach single mode cable), or **CSM 622 sm long reach** (long-reach single-mode cable).

The CSM-622 module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number.

Port LEDs
RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the CSM module is plugged in, but no cable has been connected.

LINK (Link Status/Disabled). On Green when the corresponding port is enabled and a signal is present. Flashing Green when the corresponding port is disabled and a signal is present. This LED will be off when the port is disabled and no signal is present.

ACT (Activity). On Green when data is transmitted or received on the corresponding port.

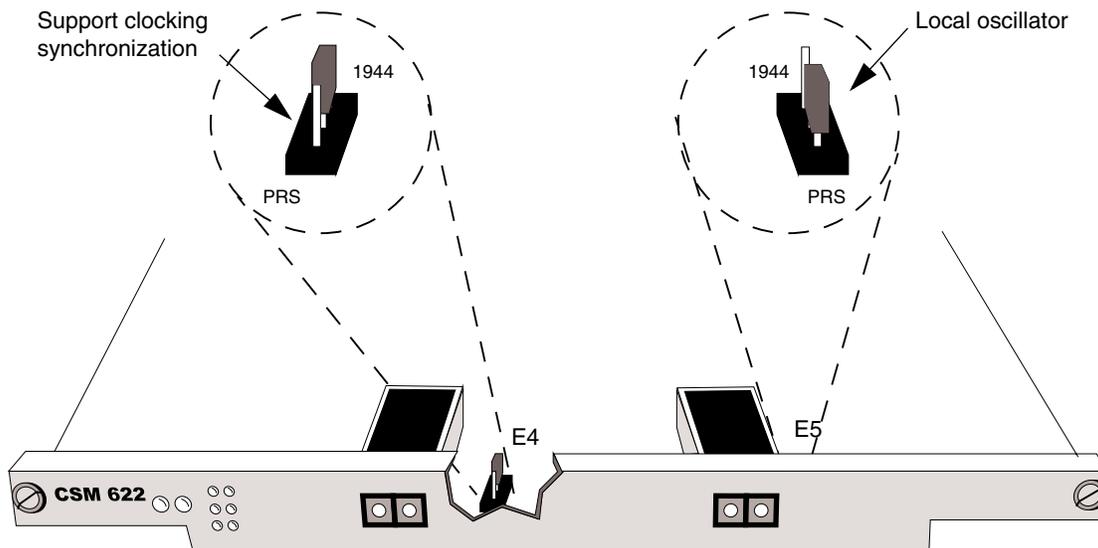
Cell Switching Module With Two OC-12c/STM-4c Ports

Jumper Settings

Each of the two ports on the CSM-622 board has a jumper (E4, E5) associated with it. These jumpers enable you to configure whether the clock source is software controlled. If the middle and top (i.e., the closest to the label **1944**) pins are jumpered, the clocking source for that port will be determined by the software, meaning that you can software select either clocking synchronization or the local oscillator (for more information on setting the clocking source through software, refer to Chapter 45, “Clocking ATM Networks.”) If the bottom (i.e., the closest to the label **PRS**) and middle pins are jumpered, the clocking source for that port will always be the local oscillator, regardless of the software setting, meaning you will not be able to use clocking synchronization.

Note

Some older versions of this module may not support clock synchronization. If you have any questions, contact Technical Support.



CSM-622 Clock Source Jumper Settings

Note

If your board has a Jumper E1, note that this jumper is set at the factory, and should not be changed.

CSM-155C-8

The CSM-155C-8 Cell Switching Module (CSM) contains eight RJ-45 ports. The ports support the STS-3c/STM-1 standard data rate of 155 Mbps. Each of the eight STS-3c/STM-1 ports supports up to 4096 virtual circuits (either Virtual Paths or Virtual Channels). In addition, each CSM-155 supports a total of 8192 point-to-multipoint virtual circuits. The cell buffer size for each physical port is 8192 cells.

The CSM-155C is available in wide format. Wide versions must be used in a wide chassis, such as the Omni-5wx and the Omni-9wx.

The CSM-155 is suited for either direct connections to ATM workstations, servers, or as an NNI link to a larger backbone. High-performance ATM workstations, servers, LAN switches, and routers can connect directly to CSM-155 ports.

CSM-155C-8 Technical Specifications	
Number of ports	8
Connector Type	RJ-45
Standards Supported	ATM Forum User-to-Network Interface 4.0, 3.1, and 3.0 ITU-T I.432 and G.957 ANSI T1.105 Bellcore TR-NWT-000253 ATM Forum Traffic Management 4.0 Private Network-to-Network Interface (PNNI) 1.0 Interim Interswitch Protocol (IISP)
Data Rate	155 Mbps
Virtual Circuits Supported	4096 point-to-point per port; 8192 point-to-multipoint per CSM-155
Cell Buffer Size	8192 per port
Connections Supported	STS-3c/STM-1 connections to ATM stations, backbones.
Cable Distance	90 meters

The CSM-155 modules include one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number.

RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the CSM module is plugged in, but no cable has been connected.

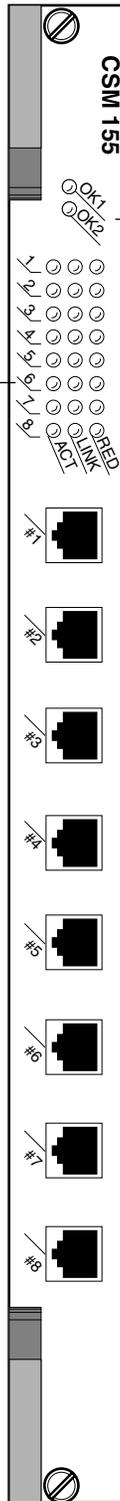
LINK (Link Status/Disabled). On Green when the corresponding port is enabled and a signal is present. Flashing Green when the corresponding port is disabled and a signal is present. This LED will be off when the port is disabled and no signal is present.

ACT (Activity). On Green when data is transmitted or received on the corresponding port.

Port LEDs

Module LEDs

Please refer to *Frame-to-Cell Switching Module (FCSM)* on page 40-17 for further information on these LEDs.



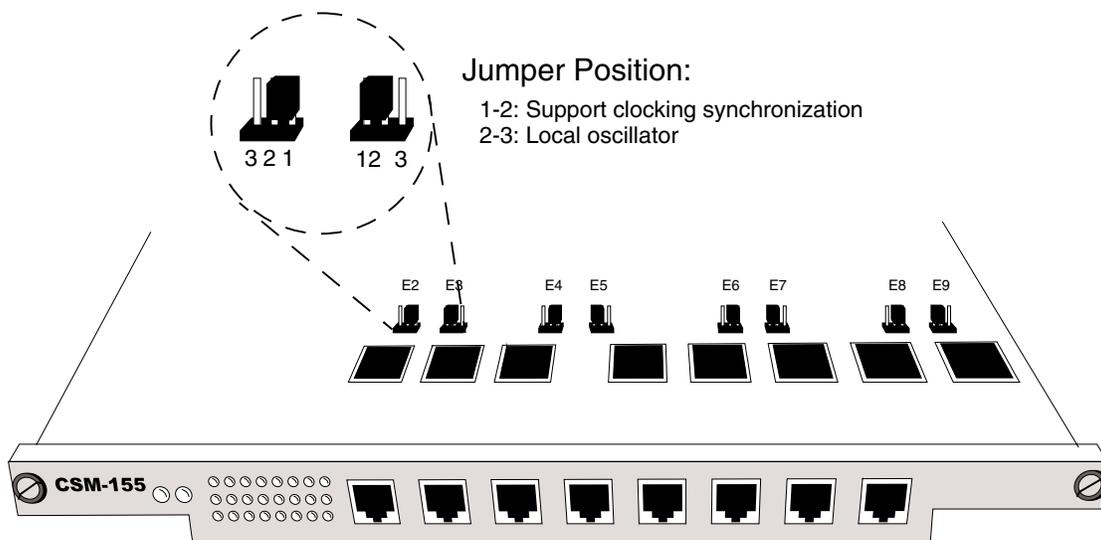
Cell Switching Module With Eight OC-3c/STM-1 Ports

Jumper Settings

Each of the eight ports on the CSM-155C-8 board has a jumper (E2-E9) associated with it. These jumpers enable you to configure whether the clock source is software controlled. If pins 1 and 2 are jumpered, the clocking source for that port will be determined by the software, meaning that you can software select either clocking synchronization or the local oscillator (for more information on setting the clocking source through software, refer to Chapter 45, “Clocking ATM Networks.”) If pins 2 and 3 are jumpered, the clocking source for that port will always be the local oscillator, regardless of the software setting, meaning you will not be able to use clocking synchronization.

Note

Some older versions of this module may not support clock synchronization. If you have any questions, contact Technical Support.



CSM-155C-8 Clock Source Jumper Settings

Note

If your board has a jumper E1, note that it is set at the factory, and should not be changed.

CSM-A25-12

The CSM-A25-12 cell switching module contains 12 ATM 25 Mbps ports. The 12 RJ-45 ports may connect to unshielded twisted pair (UTP) or shielded twisted pair (STP) cable. Typically, each port will connect to a single device, such as an ATM workstation or server.

Each of the twelve (12) 25 Mbps ports supports up to 512 virtual circuits (either Virtual Paths or Virtual Channels). In addition, each CSM-A25-12 module supports a total of 2000 point-to-multipoint virtual circuits. The cell buffer size for each physical port is 2048 cells.

Module ports are divided into two (2) banks of six (6) ports. Ports are numbered from 1 to 6 within each of the banks. The banks are labelled **A** and **B**. This grouping simplifies the display of LEDs, which are organized as a matrix. You can find the LED for a particular port by matching the port number with the bank letter within the LED matrix display (see illustration on the next page).

The CSM-A25-12 is available in wide or narrow format. Wide versions must be used in a wide chassis, such as the Omni-5wx and the Omni-9wx.

◆ **Note** ◆

The CSM-A25-12 supports a maximum of 9 bits for VPIs or VPI/VCI.

CSM-A25-12 Technical Specifications	
Number of ports	12
Connector Type	RJ-45
Standards Supported	ATM Forum User-to-Network Interface 4.0, 3.1, and 3.0
Data Rate	25 Mbps
Virtual Circuits Supported	512 point-to-point per port; 2000 point-to-multipoint per CSM-A25
Cell Buffer Size	2048 per port
Connections Supported	ATM 25 Mbps connections to ATM workstations or servers
Cable Distance	100 meters
Cable Supported	Unshielded twisted-pair (UTP)—100 ohm Shielded twisted-pair (STP)—100 ohm

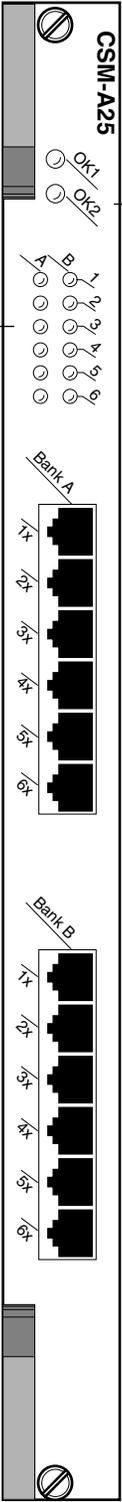
Each LED corresponds to a port on the module. Columns correspond to one of the two banks of ports (A or B). Rows refer to port numbers within each bank.

- On** A good cable connection exists to an ATM device.
- Off** A cable is not connected to the port.
- Blinks Fast** Traffic is being transmitted or received on the port.
- Blinks Slow** A cable is connected to the port, but a valid ATM connection has not been established.

Port LEDs

Module LEDs

Please refer to *Frame-to-Cell Switching Module (FCSM)* on page 40-17 for further information on these LEDs.



ATM 25 Mbps Cell Switching 12-Port Module

CSM-A25-24W

The CSM-A25-24W cell switching module contains 24 ATM 25 Mbps ports. The 24 RJ-45 ports may connect to unshielded twisted pair (UTP) or shielded twisted pair (STP) cable. Typically, each port will connect to a single device, such as an ATM workstation or server.

Each of the twenty-four (24) 25 Mbps ports supports up to 512 virtual circuits (either Virtual Paths or Virtual Channels). In addition, each CSM-A25-12 module supports a total of 4000 point-to-multipoint virtual circuits. The cell buffer size for each physical port is 2048 cells.

Module ports are divided into four (4) banks of six (6) ports. Ports are numbered from 1 to 6 within each of the four banks. The four banks are labelled **A**, **B**, **C**, and **D**. This grouping simplifies the display of LEDs, which are organized as a matrix. You can find the LED for a particular port by matching the port number with the bank letter within the LED matrix display (see illustration on the next page).

The CSM-A25-24 is available only in wide format. It must be used in a wide chassis, such as the Omni-3wx, Omni-5wx, and the Omni-9wx.

◆ **Note** ◆

The CSM-A25-24W supports a maximum of 9 bits for VPIs or VPI/VCI.

CSM-A25-24 Technical Specifications	
Number of ports	24
Connector Type	RJ-45
Standards Supported	ATM Forum User-to-Network Interface 4.0, 3.1, and 3.0
Data Rate	25 Mbps
Virtual Circuits Supported	512 point-to-point per port; 4000 point-to-multipoint per CSM-A25
Cell Buffer Size	2048 per port
Connections Supported	ATM 25 Mbps connections to ATM workstations or servers
Cable Distance	100 meters
Cable Supported	Unshielded twisted-pair (UTP)—100 ohm Shielded twisted-pair (STP)—100 ohm

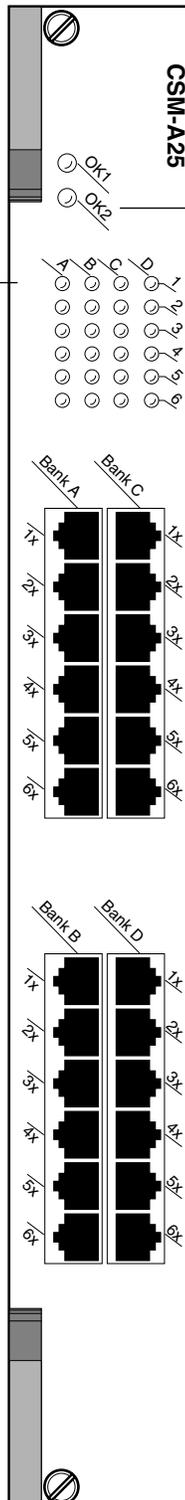
Each LED corresponds to a port on the module. Columns correspond to one of the four banks of ports (A, B, C, or D). Rows refer to port numbers within each bank.

- On** A good cable connection exists to an ATM device.
- Off** A cable is not connected to the port.
- Blinks Fast** Traffic is being transmitted or received on the port.
- Blinks Slow** A cable is connected to the port, but a valid ATM connection has not been established.

Port LEDs

Module LEDs

Please refer to *Frame-to-Cell Switching Module (FCSM)* on page 40-17 for further information on these LEDs.



ATM 25 Mbps Cell Switching 24-Port Module

CSM-U/CSM-U+

The Cell Switching Universal Module (CSM-U) contains three (3) adapter board slots in which you can install different cell switching interfaces. All adapter boards support the cell switching matrix. The available adapter board types are as follows:

- 2-port OC-3 fiber (multimode, single mode, and long-reach single mode)
- 2-port OC-3 copper
- 2-port DS3 or E3
- 4-port T1 (DS1) or E1
- 4-port T1 or E1 supporting circuit emulation
- 8-port T1 (DS1) or E1 supporting Inverse Multiplexing over ATM (IMA)
- 2-port OC-3 fiber (multimode, single mode, and long-reach single mode) with traffic shaping.

The CSM-U and all of its associated adapter boards use the wide module format. Wide modules must be used in a wide chassis, such as the Omni-3wx, Omni-5wx, or the Omni-9wx.

Switch software reads the ports on the CSM-U consecutively. For example, if the CSM-U contained three adapter boards, each board with two ports, then the top 2 ports would be reported in software as Ports 1 and 2 and the remaining ports would be reported as 3, 4, 5, and 6. However, labels on the front panel of the adapter boards will not match this internal numbering. The first port on each physical adapter board will always be labelled "1." In a CSM-U configuration of three, two-port adapter boards, the first port on the second module would have a front panel label of 1, but software would see this port as Port 3.

The CSM-U provides 12 bits for Virtual Path Identifiers (VPIs) or for VPI/Virtual Channel Identifiers (VCIs).

CSM-U+

In Release 4.3, an advanced version of the CSM-U called the CSM-U+ was introduced. This module provides 0 to 6 bits for VPIs and 8 to 14 bits for VCIs (14 total for VPIs and VCIs) in addition to all the features of the original CSM-U. (The default is 4 bits for VPIs and 10 bits for VCIs.) This module contains three (3) adapter board slots in which you can install any cell switching interface used on the original CSM-U. And this module also requires the use of a wide-format (Omni-3wx, Omni-5wx, or the Omni-9wx) chassis.

The following sections provide Technical Specifications and LED descriptions for each of the adapter boards.

CSM-U/CSM-U+ Technical Specifications	
Number of adapter boards	3
Maximum number of ports	24
Connector Types	SC fiber (OC-3 single mode and multimode) RJ-45 UTP (OC-3) RJ-48C (DS1, E1, T1 or E1 circuit emulation) BNC (DS-3 and E3)
Number of bits for VPIs or VPI/VCIs	CSM-U: 12 CSM-U+: 0 to 6 for VPIs and 8 to 14 for VCIs (14 total)

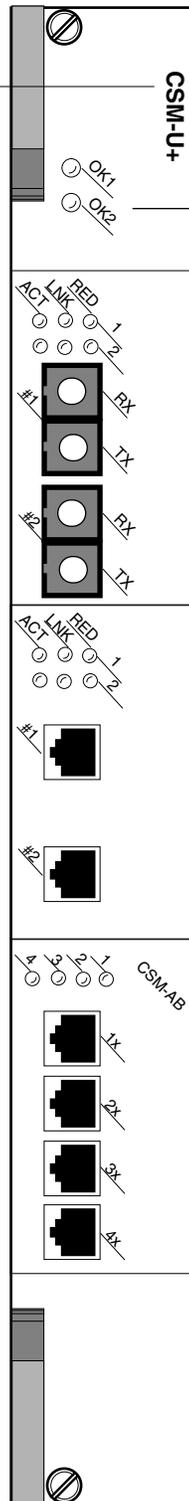
The CSM-U and CSM-U+ provide room for three (3) universal cell switching adapter boards. The illustration below shows a CSM-U+ with three different adapter board types: a fiber OC-3 board, a copper OC-3 board, and a DS1/E1 board. Each adapter board type is described in the pages that follow.

Module Label. This label will indicate the CSM-U type. It will read either **CSM-U** (original CSM-U with 12-bit VPIs or VPI/VCIs) or **CSM-U+** (advanced CSM-U with 0 to 6 bits for VPIs and 8 to 14 for VCIs).

Module LEDs

Please refer to *Frame-to-Cell Switching Module (FCSM)* on page 40-17 for further information on these LEDs.

Connector Slots



Cell Switching Universal Switching Module

CSM-AB-155F

The CSM-AB-155F cell switching adapter board contains two full-duplex SONET/SDH STS-3c ports that use fiber SC connectors. The ports support the OC-3c/STM-1 standard data rate of 155 Mbps. The CSM-AB-155 can be factory configured with single mode intermediate reach, single mode long reach, or multimode fiber connectors.

The single mode intermediate reach version of this adapter board is referred to as the CSM-AB-155-FS; the single mode long reach version is referred to as the CSM-AB-155-FSH; the multimode version is referred to as the CSM-AB-155-FM. Each connector type is differentiated by color: single mode intermediate reach connectors are blue; single mode long reach connectors are yellow; and multimode connectors are black.

Each of the OC-3c/STM-1 ports supports up to 4096 virtual circuits (either Virtual Paths or Virtual Channels). In addition, each CSM-AB-155F supports a total of 2048 point-to-multipoint virtual circuits. The cell buffer size for each physical port is 8192 cells.

The CSM-AB-155F is suited for either direct connections to ATM workstations, backbone connections, or as an NNI link to a larger backbone. High-performance ATM workstations, servers, LAN switches, and routers can connect directly to CSM-AB-155F ports; the CSM-AB-155F can then connect into an ATM network that might support a larger backbone.

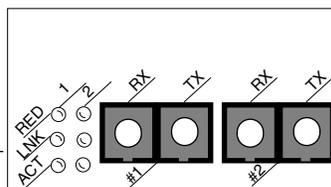
The CSM-AB-155 adapter board includes one column of LEDs for each port. The LEDs for a given port display in the column labeled with the port number.

RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the CSM board is plugged in, but no cable has been connected.

LINK (Link Status/Disabled). On Green when the corresponding port is enabled and a signal is present. Flashing Green when the corresponding port is disabled and a signal is present. This LED will be off when the port is disabled and no signal is present.

ACT (Activity). On Green when data is transmitted or received on the corresponding port.

Port
LEDs



The CSM-AB-155F LEDs

CSM-AB-155F Technical Specifications	
Number of ports	2 SONET/SDH
Connector Type	SC
Standards Supported	ATM Forum User-to-Network Interface 4.0, 3.1, and 3.0 ITU-T I.432 and G.957 ANSI T1.105 Bellcore TR-NWT-000253 ATM Forum Traffic Management 4.0 Private Network-to-Network Interface (PNNI) 1.0 Interim Interswitch Protocol (IISP)
Data Rate	155 Mbps
Virtual Circuits Supported	4096 point-to-point per port; 2048 point-to-multipoint per CSM-155
Cell Buffer Size	8192 per port
Connections Supported	OC-3c/STM-1 connections to ATM stations, backbones.
Optical output power	Multimode: -19 to -14 dBm Single mode intermediate reach: -15 to -8 dBm Single mode long reach: -5 to 0 dBm
Optical receiver sensitivity	Multimode: -30 to -14 dBm Single mode intermediate reach: -31 to -8 dBm Single mode long reach: -34 to -10 dBm
Cable Supported	Multimode: 62.5 micron multimode fiber Single mode intermediate reach: intermediate-reach single-mode fiber Single mode long reach: long-reach single-mode fiber
Cable Distance	Multimode: 4 km Single mode intermediate reach: 24 km Single mode long reach: 40 km

◆ **Special Note** ◆

The single mode version of this module has been deemed:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

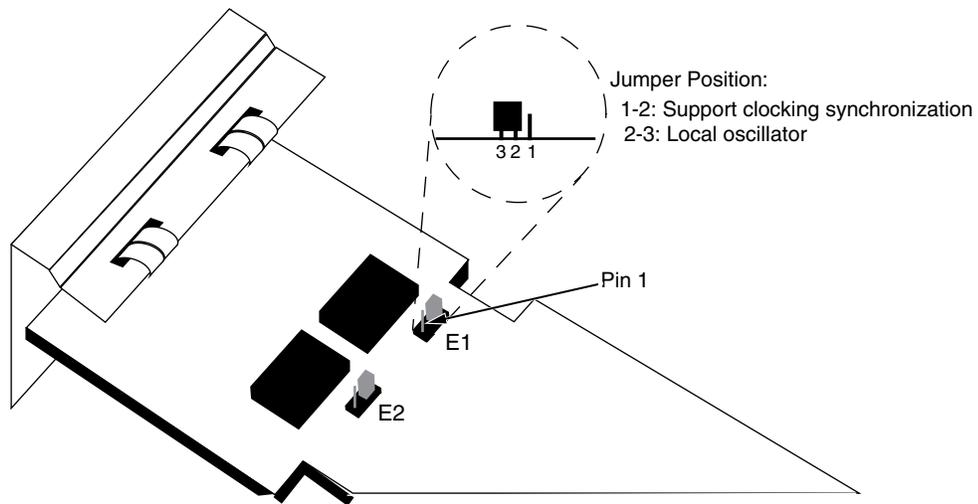
to IEC 825:1984/CENELEC HD 482 S1.

Jumper Settings

Each of the two ports on the CSM-AB-155F board has a jumper (E1-E2) associated with it. These jumpers enable you to configure whether the clock source is software controlled. If pins 1 and 2 are jumpered, the clocking source for that port will be determined by the software, meaning that you can software select either clocking synchronization or the local oscillator (for more information on setting the clocking source through software, refer to Chapter 45, "Clocking ATM Networks"). If pins 2 and 3 are jumpered, the clocking source for that port will always be the local oscillator, regardless of the software setting, meaning you will not be able to use clocking synchronization.

Note

Some older versions of this module may not support clock synchronization. If you have any questions, contact Technical Support.



CSM-AB-155F Clock Source Jumper Settings

CSM-AB-155C

The CSM-AB-155C cell switching adapter board contains two RJ-45 ports. The ports support the STS-3c/STM-1 standard data rate of 155 Mbps. Each of the STS-3c/STM-1 ports supports up to 4096 virtual circuits (either Virtual Paths or Virtual Channels). In addition, each CSM-AB-155C adapter board supports a total of 2048 point-to-multipoint virtual circuits. The cell buffer size for each physical port is 8192 cells.

The CSM-AB-155C is suited for either direct connections to ATM workstations, servers, or as an NNI link to a larger backbone. High-performance ATM workstations, servers, LAN switches, and routers can connect directly to CSM-AB-155C ports.

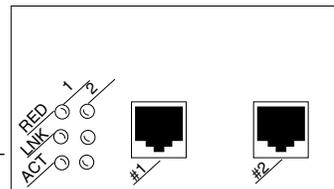
The CSM-AB-155C adapter board includes one column of LEDs for each port. The LEDs for a given port display in the column labeled with the port number.

RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the CSM board is plugged in, but no cable has been connected.

LINK (Link Status/Disabled). On Green when the corresponding port is enabled and a signal is present. Flashing Green when the corresponding port is disabled and a signal is present. This LED will be off when the port is disabled and no signal is present.

ACT (Activity). On Green when data is transmitted or received on the corresponding port.

Port
LEDs



The CSM-AB-155C LEDs

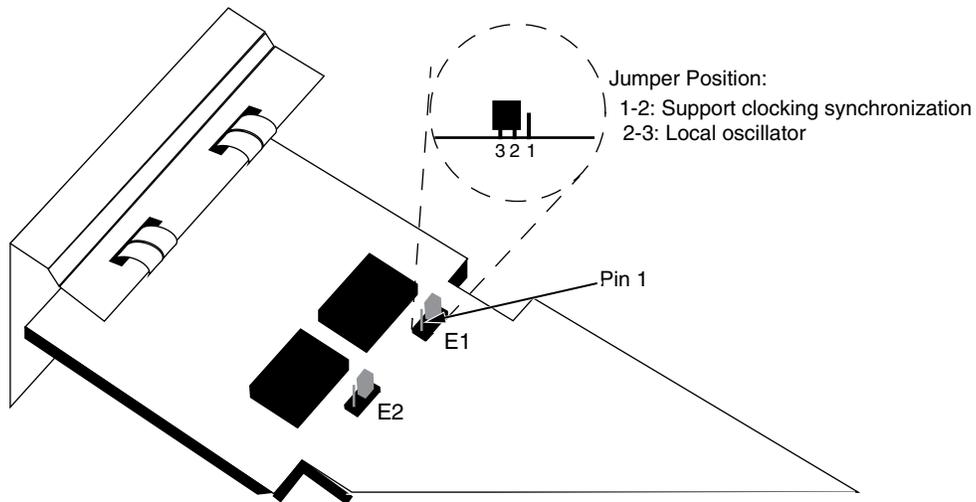
CSM-AB-155C Technical Specifications	
Number of ports	2
Connector Type	RJ-45
Standards Supported	ATM Forum User-to-Network Interface 4.0, 3.1, and 3.0 ITU-T I.432 and G.957 ANSI T1.105 Bellcore TR-NWT-000253 ATM Forum Traffic Management 4.0 Private Network-to-Network Interface (PNNI) 1.0 Interim Interswitch Protocol (IISP)
Data Rate	155 Mbps
Virtual Circuits Supported	4096 point-to-point per port; 2048 point-to-multipoint per CSM-155
Cell Buffer Size	8192 per port
Connections Supported	STS-3c/STM-1 connections to ATM stations, backbones.
Cable Distance	90 meters

Jumper Settings

Each of the two ports on the CSM-AB-155C board has a jumper (E1-E2) associated with it. These jumpers enable you to configure whether the clock source is software controlled. If pins 1 and 2 are jumpered, the clocking source for that port will be determined by the software, meaning that you can software select either clocking synchronization or the local oscillator (for more information on setting the clocking source through software, refer to Chapter 45, "Clocking ATM Networks.") If pins 2 and 3 are jumpered, the clocking source for that port will always be the local oscillator, regardless of the software setting, meaning you will not be able to use clocking synchronization.

Note

Some older versions of this module may not support clock synchronization. If you have any questions, contact Technical Support.



CSM-AB-155C Clock Source Jumper Settings

CSM-AB-DS1/E1-4W

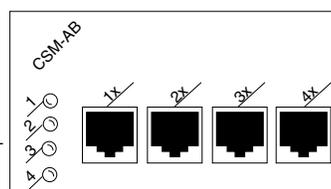
The CSM-AB-DS1/E1 adapter board contains four DS1 (T1) or E1 ports using RJ-48C connectors. The DS1 version of this adapter board is referred to as the CSM-AB-DS1-4W; the E1 version is referred to as the CSM-AB-E1-4W.

You must adjust jumpers on the E1 version of this adapter board to set the cable resistance (75 or 120 ohm) of the connection correctly. These adapter boards include an integrated CSU/DSU to enable direct connection to a DS1/E1 device, such as a PBX.

You can configure several physical port parameters through switch software commands. Configuration options include frame format, facility datalink, and line coding. In addition, the switch can store up to 24 hours of local and remote statistics.

Port LEDs. Each port on this adapter board is assigned a labelled status LED. Each LED will be in one of four states. The following describes each state:

- Off** There is no link and no data transmitting. Possibly no cable is connected.
- Green (Solid)** The port is enabled and a signal is present, but no data is being transmitted or received.
- Green (Blinking)** Data (ATM cells) are being transmitted or received on this port.
- Yellow (Solid)** An error has occurred on the port.



The CSM-AB-DS1/E1 LEDs

CSM-AB-DS1/E1 Technical Specifications	
Number of ports	4 DS1 (T1) or E1
Connector Type	RJ-48C
Standards Supported	RFC 1406
Frame Formats	DS1: Superframe, Extended Superframe, Unframed E1: E1, E1-CRC, E1-MF, E1-CRC-MF, Unframed
Line Type	DS1: B8ZS or AMI E1: HDB3 or AMI
Data Rates Supported	DS1: 1.544 Mbps E1: 2.048 Mbps
Facility Datalink Protocol	ANSI T1.403 and AT&T 54016
Connections Supported	Physical Data Terminal Equipment (DTE) or Data Communication Equipment (DCE)
Cable Distance	DS1/E1 (short haul): 200 meters DS1/E1 (long haul): 1829 meters

CSM-AB-DS3/E3-2W

The CSM-AB-DS3/E3 adapter board contains two BNC ports that support DS-3 or E3 connections. Each port connection provides 44.736 Mbps (DS-3) or 34.368 Mbps (E3) of bandwidth and connects to coaxial (RG-59) cable. The DS-3 version of this adapter board is referred to as the CSM-AB-DS3-2W; the E3 version of this adapter board is referred to as the CSM-AB-E3-2W.

CSM-AB-DS3/E3 ports are suited for connections to ATM carrier services. The CSM-AB-DS3/E3 ports are physical DTE (Data Termination Equipment) devices that connect to physical DCE (Data Communication Equipment) devices, such as DSUs (Data Service Unit).

By default DS3 ports use Cbitparity line encoding, but you can configure these ports to use M23. By default E3 ports uses G.751 line encoding, but you can configure them to use G.832. You should configure all ports to use the same line encoding as the ATM service provider. You can configure loopback controls for all port types.

Two different mapping protocols are used to transmit ATM cells over DS-3 and E3: PLCP (Physical Layer Convergence Protocol) and ATM Direct Mapped (ADM) System. The two protocols are not compatible. Many existing implementations use PLCP as defined in ANSI T1.624-1993, but many new implementations use ADM. The CSM-AB-DS3/E3 ports support both physical layer protocols.

The CSM-AB-DS3/E3 adapter board includes one column of LEDs for each port. The LEDs for a given port display in the column labeled with the port number.

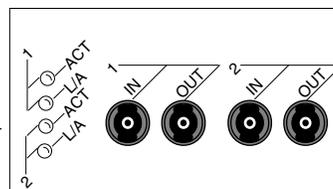
ACT (Activity). On Green when data is transmitted or received on the corresponding port.

L/A (Link/Alarm). Both ports on this adapter board use a dual-color Link/Alarm LED which convey two different states. The following describes each state:

Green The port is enabled and a signal is present.

Yellow An error has occurred on the port.

Port LEDs



The CSM-AB-DS3/E3 LEDs

CSM-AB-DS3/E3 Technical Specifications	
Number of ports	2
Connector Type	BNC
Standards Supported	ANSI T1.624-1993 (PLCP Mapping) IEEE P802.6
Data Rate	DS-3: 44.736 Mbps E3: 34.368 Mbps
Line Types Supported	DS-3: CbitParity or M23 E3: G.751 or G.832
Sublayers Supported	PLCP or ADM
Connections Supported	DS-3 and E3 connections to ATM carrier service.
Cable Supported	Coaxial RG-59 (75 ohm)
Cable Distance	185 m

CSM-AB-CE-T1/E1-4W

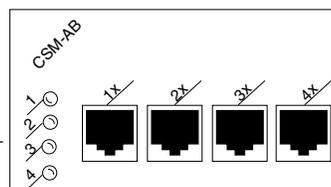
The CSM-AB-CE circuit emulation adapter board converts traditional circuit emulation traffic from T1 or E1 ports to ATM cells for transport over an ATM network. This module is best employed as a means of connecting legacy Time Division Multiplexing (TDM) traffic to an enterprise ATM network. It contains four T1 or E1 ports. The T1 version of this adapter board is referred to as the CSM-AB-CE-T1-4W; the E1 version is referred to as the CSM-AB-CE-E1-4W.

You can configure several circuit emulation parameters through switch software commands. Configurable options include service mode (structured or unstructured), clocking mode, cell delay variation, and ATM reassembly buffer size. Configuration options specifically for T1 and E1 ports include frame format, facility datalink, and line coding. In addition, the switch can store up to 24 hours of local and remote statistics for T1 and E1 ports.

The CSM-AB-CE modules use four RJ-48C connectors. You must adjust jumpers on the E1 version of this adapter board to set the cable resistance (75 or 120 ohm) of the connections correctly.

Port LEDs. Each port on this adapter board is assigned a labelled status LED. Each LED will be in one of four states. The following describes each state:

- | | |
|-------------------------|--|
| Off | There is no link and no data transmitting. Possibly no cable is connected. |
| Green (Solid) | The port is enabled and a signal is present, but no data is being transmitted or received. |
| Green (Blinking) | Data (ATM cells) are being transmitted or received on this port. |
| Yellow (Solid) | An error has occurred on the port. |



The CSM-AB-CE Adapter Board LEDs

CSM-AB-CE Technical Specifications	
Number of ports	4 T1 or E1
Connector Type	RJ-48C
Standards Supported	RFC 1406 ATM Forum CES-IS, version 2
Frame Formats	T1: Superframe, Extended Superframe, Unframed E1: E1, E1-CRC, E1-MF, E1-CRC-MF, Unframed
Line Coding	T1: B8ZS or AMI E1: HDB3 or AMI
Data Rates Supported	T1: 1.544 Mbps E1: 2.048 Mbps
Facility Datalink Protocol	ANSI T1.403 and AT&T 54016
Data Transfer Services	Structured or Unstructured
Clocking	Synchronous, SRTS, Adaptive
Virtual Circuits Supported	Permanent Virtual Circuits (PVCs)
Connections Supported	Physical Data Terminal Equipment (DTE) or Data Communication Equipment (DCE)
Cable Distance	T1/E1 (short haul): 200 meters T1/E1 (long haul): 1829 meters

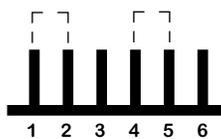
CSM-AB-CE-E1-4W Impedance Jumpers

The CSM-AB-CE-E1-4W submodule has four (4) jumpers (one for each port) to set the impedance level (see the table below). The jumpers are located on the top of the submodule near the ports. The CSM-AB-CE-E1-4W submodule supports 75 Ohm and 120 Ohm (the default) impedance levels.

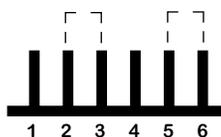
CSM-AB-CE-E1-4W Impedance Jumper Numbers

Port Number	Jumper Number	Port Number	Jumper Number
1	J5	3	J7
2	J6	4	J8

As shown in the figure on the following page, you must connect two pairs of pins on each jumper. To set the port for coaxial cable (75 Ohm impedance), you must connect pins 1 and 2 to each other and pins 4 and 5 to each other. To set the port for twisted pair cable (120 Ohm impedance), you must connect pins 2 and 3 to each other and pins 5 and 6 to each other.



75 Ohm (Coaxial)



120 Ohm (Twisted Pair)
(Factory Default)

CSM-AB-CE-E1-4W Jumper Settings

CSM-AB-CE-E1-4W RJ-48 Grounding Jumpers

The CSM-AB-CE-E1-4W submodule has four (4) jumpers (one for each port) that allow you to ground Pins 7 and 8 of each RJ-48C port. The jumpers are located on the top of the submodule and are identified in the table below. To ground a port, use a shunt to connect the two pins of the jumper.

CSM-AB-CE-E1-4W Grounding Jumper Numbers

Port Number	Jumper Number	Port Number	Jumper Number
1	J9	3	J11
2	J10	4	J12

CSM-AB-CM

The CSM-AB-CM Clocking Module is a daughtercard that plugs into one of the three submodule slots in the CSM-U or CSM-U+ motherboard. It adds the following abilities to the OmniSwitch:

- To internally generate Stratum 3, 8 KHz and 19.44 MHz clocks for distribution to the OmniSwitch backplane.
- To derive an input reference timing source from the T1 or E1 line.
- To monitor the clocking signal for inaccurate or missing signal, and switch to a backup clock source, if necessary.
- To generate a 19.44 MHz clock for distribution to the OmniSwitch backplane by multiplying the backplane's 8 kHz clock.

◆ Important Note ◆

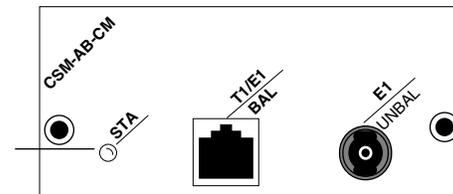
Only one (1) CSM-AB-CM Clocking Module is supported on a switch. Therefore, you *cannot* use one CSM-AB-CM module to back up another.

The Clocking Module contains one RJ-48 port for balanced T1 or E1, and one BNC port for unbalanced E1. Only one of these ports can be used at a time. The board contains configuration jumpers that must be set before you use the board. For details on setting these jumpers, refer to the installation instructions that accompany the board.

The CSM-AB-CM clocking module has one LED.

- ON** (Solid). Module active; normal operation.
- ON** (Flash). Module active; clock signal status change detected; hardware switch occurs.

Port LED



The CSM-AB-CM LED

CSM-AB-CM Technical Specifications	
Number of ports	2 (1 usable at any one time)
Connector Type	RJ-48C (T1, 100 ohm or E1, 120 Ohm) BNC (E1, 75 Ohm)
Standards Supported	American National Standard for Telecommunications: ANSI T1.101-1994 American National Standard for Telecommunications: ANSI T1.403-1995 Network-to-Customer Installation-- DS1 Metallic Interface Bellcore "System Interface" TR-TSY-000510, Issue 2, July, 1987 Bellcore "Transport Systems Generic Requirements (TSGR): Common Requirements" TR-TSY-000499, Issue, December, 1989 ITU Recommendation G.703: Physical/Electrical Characteristics of Hierarchical Digital Interfaces, 1991 ITU Recommendation G.823: The Control of Jitter and Wander within Digital Networks Which Are Based on the 2048 Kbit/s Hierarchy.
Data Rates Supported	T1: 1.544 Mbps E1: 2.048 Mbps
Clocking Stratum Support	Stratum 3 accuracy (4.6×10^{-6} or better)
Line Coding	T1: B8ZS or AMI E1: HDB3 or AMI
Cable Distance	T1/E1 (short haul): 200 meters T1/E1 (long haul): 1829 meters BNC: 185 meters

CSM-AB-CM Jumper Settings

See the tables below for the appropriate jumper settings or your CSM-AB-CM submodule. If you are using a balanced E1 port, for example, pins 2 and 3 must be jumpered on Jumper E2 and pins 1 and 2 must be jumpered on Jumpers JP1, JP2, and JP3. (Note: The acronym “N/C” in the tables below means “no connection.”)

CSM-AB-CM Port Type Jumper Settings

	Jumper Settings						
Jumper Number:	E1	E2	E3	E4	JP1	JP2	JP3
Port Type							
T1	1&2	1&2	1&2	1&2	N/C	N/C	N/C
Balanced E1	N/C	2&3	N/C	N/C	1&2	1&2	1&2
Unbalanced E1	2&3	2&3	2&3	2&3	N/C	N/C	N/C

CSM-AB-CM Port Shield Jumper Settings

	Jumper Settings	
Jumper Number:	E5	E6
Shield Type		
T1	1&2	N/C
E1 Unbalanced	N/C	1&2

CSM-AB-IMA-DS1/E1-8W

The CSM-AB-IMA-DS1/E1-8W adapter board contains eight (8) DS1 (T1) or E1 ports using RJ-48C connectors. The DS1 version of this adapter board is referred to as the CSM-AB-IMA-DS1-8W; the E1 version is referred to as the CSM-AB-IMA-E1-8W. The CSM-AB-IMA-DS1/E1-8W adapter board can transmit and receive up to four (4) IMA groups. You can display and configure IMA groups through commands contained in the IMA submenu. See Chapter 43, “Inverse Multiplexing over ATM (IMA),” for descriptions of these commands.

◆ Note ◆

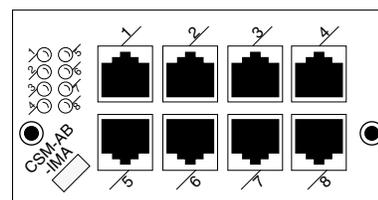
Groups cannot span multiple CSM-AB-IMA-DS1/E1-8W adapter boards.

The CSM-AB-IMA-DS1/E1-8W adapter board plugs into a Cell Switching Universal Module (CSM-U) or CSM-U or CSM-U+. The CSM-U and CSM-U+ contain three (3) adapter board slots in which you can install CSM-AB-IMA-DS1/E1-8W and many other cell switching adapter boards including OC-3, DS3, E3, DS1/E1, or T1/E1 with circuit emulation interfaces. All adapter boards support the cell switching matrix. The CSM-U and CSM-U+ and all of their associated adapter boards use the wide module format. Wide modules must be used in a wide chassis, such as the Omni-3wx, Omni-5wx, or Omni-9wx.

You must adjust jumpers on the E1 version of this adapter board to set the cable impedance (75 or 120 Ohm) of the connection correctly. These adapter boards include an integrated CSU/DSU to enable direct connection to a DS1/E1 device, such as a PBX. See *CSM-AB-IMA-E1-8W Jumpers* on page 40-67 for more information on setting these jumper ports. See Appendix B, “Custom Cables,” for more information on 75 Ohm cables for the CSM-AB-IMA-E1-8W submodule.

Port LEDs. Each port on this adapter board is assigned a labelled status LED. Each LED will be in one of four states. The following describes each state:

- | | |
|-------------------------|--|
| Off | There is no link and no data transmitting. Possibly no cable is connected. |
| Green (Solid) | The port is enabled and a signal is present, but no data is being transmitted or received. |
| Green (Blinking) | Data (ATM cells) are being transmitted or received on this port. |
| Yellow (Solid) | An error has occurred on the port (e.g., loss of signal, loss Link Out of Delay Synchronization, Red Alarm). |



The CSM-AB-IMA-DS1-8W/CSM-AB-IMA-EI-8W Adapter Board LEDs

CSM-AB-IMA-DS1-8W/CSM-AB-IMA-E1-8W Technical Specifications	
Number of ports	8 DS1 (T1) or E1
Connector Type	RJ-48C
Standards Supported	ANSI T1.102, T1.107, T1.231, and T1.646 ATM Forum af-phy-0086.000, <i>ATM Forum Inverse Multiplexing for ATM (IMA) Specification</i> , Version 1.0, July 1997; and af-phy-0086.001, <i>ATM Forum Inverse Multiplexing for ATM (IMA) Specification</i> , Version 1.1, March 1999 ATM Forum User-to-Network Interface 4.0, 3.1, and 3.0 ISO 2593 ITU-T G.703; G.704; G.804; G.826; I.321; I.432; and I.610, Section 7.1 RFC 1213 and 1406
Frame Formats	DS1: Superframe, Extended Superframe E1: E1, E1-CRC
Line Type	DS1: B8ZS E1: HDB3
Data Rates Supported	DS1: 1.544 Mbps E1: 2.048 Mbps
Facility Datalink Protocol	ANSI T1.403 and AT&T 54016
Connections Supported	Physical Data Terminal Equipment (DTE) or Data Communication Equipment (DCE)
Cable Distance	DS1/E1 (short haul): 200 meters T1/E1 (long haul): 1829 meters
Maximum Number of IMA Groups	4
Power Consumption	2.5 amps

The CSM-AB-IMA-DS1/E1-8W submodule uses the same physical connections as standard E1 and DS1 switching modules and adapter boards (e.g., the CSM-AB-DS1-4W/CSM-AB-E1-4W).

◆ **Note** ◆

See Chapter 53, “Managing T1 and E1 Ports,” for more information on DS1 and E1 ports.

CSM-AB-IMA-E1-8W Jumpers

The E1 version of this submodule supports both twisted pair (120 Ohm) and coaxial (75 Ohm) cable types. In addition, some applications of the E1 submodule require that the Pins 7 and 8 of the ports be grounded. Therefore, the CSM-AB-IMA-E1-8W submodule provides jumpers to set the correct impedance and jumpers to ground the ports.

◆ Note ◆

For more detailed information on the types of cables to use with this submodule, see Appendix B, “Custom Cables.”

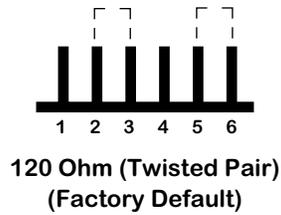
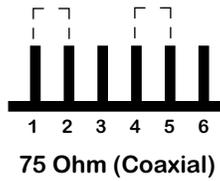
CSM-AB-IMA-E1-8W Impedance Jumpers

The CSM-AB-IMA-E1-8W submodule has eight jumpers (one for each port) to set the impedance level (see the table below). The jumpers are located on the side of the submodule opposite the ports. The CSM-AB-IMA-E1-8W submodule supports 75 Ohm and 120 Ohm (the default) impedance levels.

CSM-AB-IMA-E1-8W Impedance Jumper Numbers

Port Number	Jumper Number	Port Number	Jumper Number
1	J1	5	J11
2	J2	6	J12
3	J7	7	J13
4	J8	8	J14

As shown in the figure on the following page, you must connect two pairs of pins on each jumper. To set the port for coaxial cable (75 Ohm impedance), you must connect pins 1 and 2 to each other and pins 4 and 5 to each other. To set the port for twisted pair cable (120 Ohm impedance), you must connect pins 2 and 3 to each other and pins 5 and 6 to each other.



CSM-AB-IMA-E1-8W Jumper Settings

CSM-AB-IMA-E1-8W RJ-48 Grounding Jumpers

The CSM-AB-IMA-E1-8W submodule has eight jumpers (one for each port) that allow you to ground Pins 7 and 8 of each RJ-48C port. The jumpers are located on the top of the submodule and are identified in the table below. To ground a port, use a shunt to connect the two pins of the jumper.

CSM-AB-IMA-E1-8W Grounding Jumper Numbers

Port Number	Jumper Number	Port Number	Jumper Number
1	J5	5	J3
2	J4	6	J6
3	J18	7	J16
4	J15	8	J17

CSM-ABT-155F

The CSM-ABT-155F cell switching adapter board contains two full-duplex SONET/SDH STS-3c ports that use fiber SC connectors. The ports support the OC-3c/STM-1 standard data rate of 155 Mbps. The CSM-ABT-155F also provides user-configurable VC-based traffic shaping. The CSM-ABT-155F can be factory configured with single mode intermediate reach, single mode long reach, or multimode fiber connectors.

The single mode intermediate reach version of this adapter board is referred to as the CSM-ABT-155-FS-2W; the single mode long reach version is referred to as the CSM-ABT-155-FH-2W; the multimode version is referred to as the CSM-ABT-155-FM-2W. Each connector type is differentiated by color: single mode intermediate reach connectors are blue; single mode long reach connectors are yellow; and multimode connectors are black.

Each of the OC-3c/STM-1 ports supports up to 4096 virtual circuits (either Virtual Paths or Virtual Channels). In addition, each CSM-ABT-155F supports a total of 2048 point-to-multipoint virtual circuits. The cell buffer size for each physical port is 8192 cells.

The CSM-ABT-155F is suited for either direct connections to ATM workstations, backbone connections, or as an NNI link to a larger backbone. High-performance ATM workstations, servers, LAN switches, and routers can connect directly to CSM-ABT-155F ports; the CSM-ABT-155F can then connect into an ATM network that might support a larger backbone.

Installing a CSM-ABT-155F in a CSM-U/CSM-U+

The width of the CSM-ABT-155F prevents installation of another daughtercard in a neighboring CSM-U/CSM-U+ slot. For example, if you install a CSM-ABT-155F daughtercard in Slot 1 of a CSM-U+, then you cannot install any other daughtercards in CSM-U+ Slot 2.

Alcatel recommends that you install a CSM-ABT-155F daughtercard in Slot 1 or Slot 3 of a CSM-U or CSM-U+, since this will allow you to install a maximum of two (2) daughtercards. It is possible to install a CSM-ABT-155F in daughtercard Slot 2 in a CSM-U or CSM-U+. However, this is not recommended because you will *not* be able to install additional daughtercards in your CSM-U or CSM-U+.

CSM-ABT-155F Installation Guidelines

	CSM-U/CSM-U+ Daughtercard Slot 1	CSM-U/CSM-U+ Daughtercard Slot 2	CSM-U/CSM-U+ Daughtercard Slot 3
CSM-ABT-155F in CSM-U/ CSM-U+ Daughtercard Slot 1	CSM-ABT-155F	<i>Must</i> be empty	CSM-AB or CSM-ABT-155F (Can be empty)
CSM-ABT-155F in CSM-U/ CSM-U+ Daughtercard Slot 2	<i>Must</i> be empty	CSM-ABT-155F	<i>Must</i> be empty
CSM-ABT-155F in CSM-U/ CSM-U+ Daughtercard Slot 3	CSM-AB or CSM-ABT-155F (Can be empty)	<i>Must</i> be empty	CSM-ABT-155F

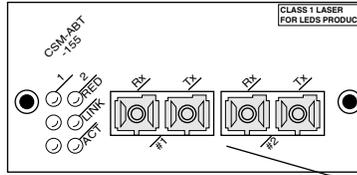
The CSM-ABT-155F adapter board includes one column of LEDs for each port. The LEDs for a given port display in the column labeled with the port number.

RED (Red Alarm). On Amber when a receive failure occurs. A receive failure results when the port is persistently losing frames or when a cable is not inserted. This LED will be on when the CSM board is plugged in, but no cable has been connected.

LINK (Link Status/Disabled). On Green when the corresponding port is enabled and a signal is present. Flashing Green when the corresponding port is disabled and a signal is present. This LED will be off when the port is disabled and no signal is present.

ACT (Activity). Blinking Green when data is transmitted or received on the corresponding port.

Port LEDs



Warning Label. This label indicates that the module contains an optical transceiver.

SC connectors will be color coded to indicate multimode (Black), long-reach single mode (Yellow), or intermediate-reach single mode (Blue).

The CSM-ABT-155F Front Panel

CSM-ABT-155F Technical Specifications	
Number of ports	2 SONET/SDH
Connector Type	SC
Standards Supported	ATM Forum User-to-Network Interface 4.0, 3.1, and 3.0 ITU-T I.432 and G.957 ANSI T1.105 Bellcore TR-NWT-000253 ATM Forum Traffic Management 4.0 Private Network-to-Network Interface (PNNI) 1.0 Interim Interswitch Protocol (IISP)
Data Rate	155 Mbps
Virtual Circuits Supported	4096 point-to-point per port; 2048 point-to-multipoint per CSM-155
Cell Buffer Size	8192 per port
Connections Supported	OC-3c/STM-1 connections to ATM stations, backbones.
Optical output power	Multimode: -19 to -14 dBm Single mode intermediate reach: -15 to -8 dBm Single mode long reach: -5 to 0 dBm
Optical receiver sensitivity	Multimode: -30 to -14 dBm Single mode intermediate reach: -31 to -8 dBm Single mode long reach: -34 to -10 dBm
Cable Supported	Multimode: 62.5 micron multimode fiber Single mode intermediate reach: intermediate-reach single-mode fiber Single mode long reach: long-reach single-mode fiber
Cable Distance	Multimode: 4 km Single mode intermediate reach: 24 km Single mode long reach: 40 km
Power Consumption	1.2 amps at 5 Volts
Traffic Classes Supported	CBR rt-VBR nrt-VBR UBR (Shaped Traffic) Regular (Unshaped Traffic) Tunneling

◆ **Special Note** ◆

The single mode version of this module has been deemed:

CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

to IEC 825:1984/CENELEC HD 482 S1.

41 Managing Cell Switching Modules (CSMs)

Cell Switching Modules (CSMs) support point-to-point and point-to-multipoint connections over OC-3c/STM-1 and OC-12c/STM-4c connections. Virtual Paths and Virtual Channels may be configured on any CSM port. Each virtual circuit may be configured as a private UNI connection to an ATM End System (ES), a PNNI connection that supports the routing features in PNNI version 1.0, or as an IISP connection that supports static routes via the IISP routing protocol.

CSM ports and the virtual circuits associated with those ports are configured through commands on the ATM menu. These commands allow you to specify Quality of Service (QoS) and traffic management parameters for each virtual circuit. Software configuration commands are described in this chapter.

CSM modules must be used with the ATM cell switching backplane. They can reside in an OmniSwitch chassis with other CSM modules or with frame-based modules, such as Ethernet, Fast Ethernet, and Token Ring modules. Descriptions of ATM switch hardware can be found in Chapter 40 of this manual, “Cell Switching Modules (CSMs).”

All CSM modules support ATM User-Network Interface (UNI) specification versions 3.0 and 3.1. If you have installed the optional software for multiple peer group PNNI, then you can configure CSM modules for UNI signalling specification version 4.0. (See Chapter 46, “Configuring and Monitoring PNNI,” for more information on the optional software for multiple peer group PNNI.)

This chapter describes the initial configuration of CSM ports, Virtual Paths, and Virtual Channels. It provides background on how Quality of Service, Traffic Descriptors, Leaky Buckets, and Flow Control are handled by the OmniSwitch and CSM modules. In addition, it provides step-by-step instructions for configuring CSM port and circuit parameters. Information on the PNNI routing protocol and how to configure PNNI parameters can be found in Chapter 46, “Configuring and Monitoring PNNI.”

Connection Admission Control (CAC) and Call Overbooking

Additionally, the OmniSwitch supports Connection Admission Control (CAC) and Call Overbooking features.

CAC (Connection Admission Control)

CAC is a control function of the ATM Traffic Contract established between the source and the network during the call set-up phase that determines whether a connection can be established at the ingress switch. When CAC is enabled (default), the network calculates whether enough resources are available to support the connection at the desired QoS level without negatively impacting the QoS of any previously-established connections. CAC can be disabled on a per-link basis with the **map** UI command. See *Modifying a Port Configuration* on page 41-29 for more information.

Call Overbooking

To minimize traffic congestion and optimize access to network resources for different QoS classes, a switch needs to be able to monitor available bandwidth. The Call Overbooking feature allows available bandwidth on a CSM virtual port to be calculated by modifying the port's Overbooking Factor, to reduce or increase bandwidth on a logical or physical link, as needed. In addition to viewing available bandwidth on a single or multiple CSM virtual port(s), Call Overbooking can be viewed and configured with the **vap** and **map** UI commands, respectively. See *Viewing Port Configurations* on page 41-63 or *Modifying a Port Configuration* on page 41-29 for more information.

Several User Interface (UI) commands used to manage CSM modules are referenced in this chapter. For documentation on Command Line Interface (CLI) commands to manage CSM modules, see the *Text-Based Configuration CLI Reference Guide*.

◆ Important Notes ◆

The content in this chapter requires familiarity with ATM concepts. The focus of the chapter is to describe the OmniSwitch implementation of various ATM switch features, rather than to explain ATM concepts.

In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. See Chapter 8, "The User Interface," for documentation on changing from CLI mode to UI mode.

Required Image Files

The following image files are required to run OmniSwitch CSMs:

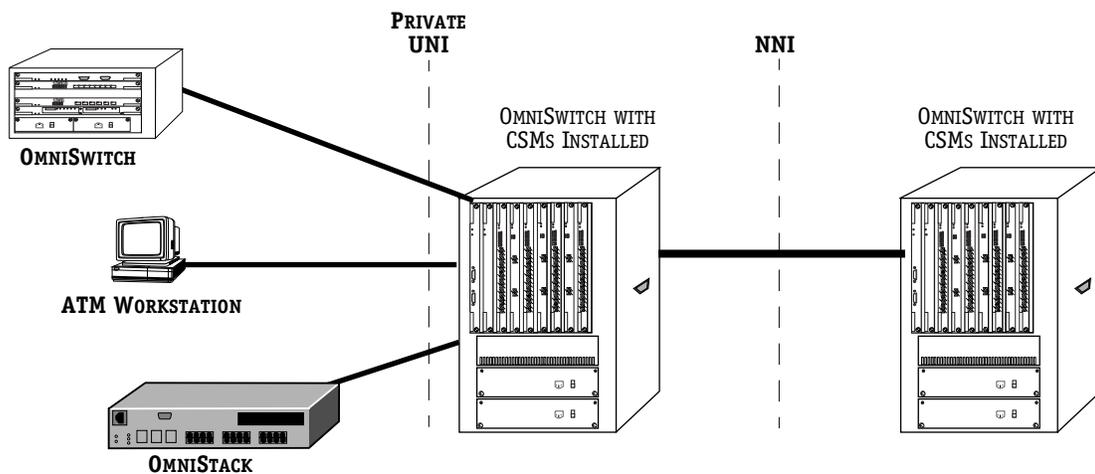
asm.img (MPM-1G or MPM-III and an FCSM-I or FCSM-II) *or* **asmc.img** (MPM-C)
cell.img
sonet.img

These image files will also let you run the single-peer group version of PNNI. To run the multiple-peer group version of PNNI, you must instead load the following files into your switch:

asm_mpg.img (MPM-1G or MPM-III and an FCSM-I or FCSM-II) *or* **asmc_mpg.img** (MPM-C)
cell_mpg.img
sonet.img

OmniSwitch ATM Network Example

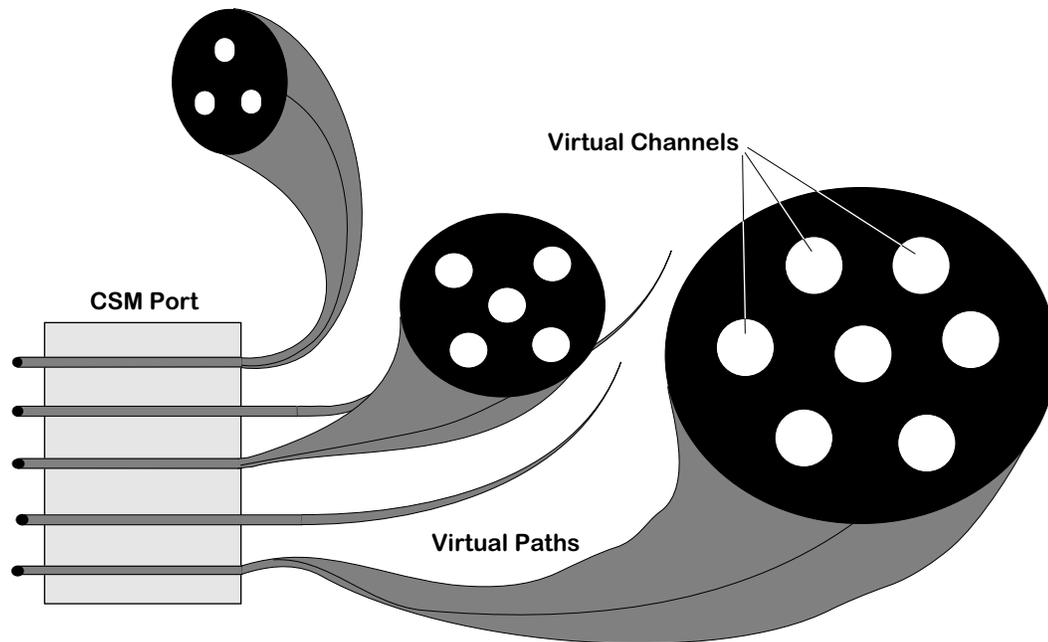
The following figure shows a typical OmniSwitch/CSM module configuration. Note that CSM modules can connect directly to ATM end stations, LAN switches, or to other OmniSwitches.



Typical OmniSwitch ATM Switch Network Configuration

Virtual Circuits

Each CSM port supports a number of virtual circuits. A virtual circuit is the connection on which data is transmitted over the ATM network. In addition, Quality of Service and traffic management parameters are defined on a virtual circuit basis. The OmniSwitch supports point-to-point and point-to-multipoint virtual circuits. These connections can be either Virtual Paths (VPs) or Virtual Channels (VCs). A Virtual Path is a path through the ATM network representing a group of Virtual Channels. Virtual Channels are independent connections that are part of a Virtual Path. The following diagram illustrates this hierarchy.



Virtual Paths and Virtual Channels

Each Virtual Path Connection or Virtual Channel Connection has a defined traffic contract. This traffic contract includes a description of the type of traffic that will use the circuit, the Quality of Service expected on that circuit, and traffic descriptors that quantify the cell rate and a burst size allowed. More detailed information on the traffic contract and traffic management parameters can be found in *Traffic Management* on page 41-13.

◆ Note on Terminology ◆

The term, “virtual circuit,” refers to either a Virtual Path Connection or a Virtual Channel Connection.

VPIs and VCIs

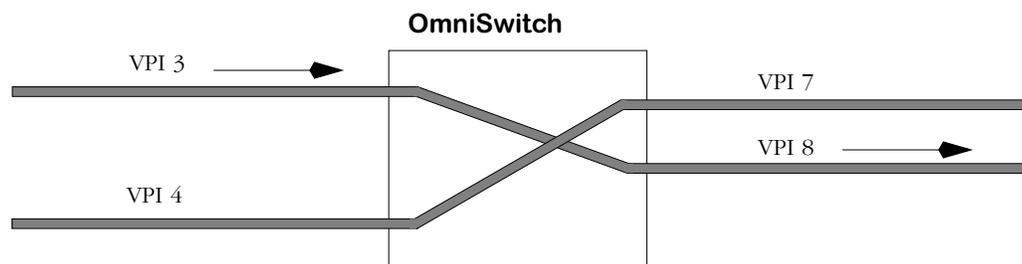
Virtual Paths and Virtual Channels are identified by their Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). The VPI and VPI/VCI act as an address for a connection. They do not describe the specific address of an ATM end device, but they do describe the connection that leads to the device.

◆ Note on Terminology ◆

A “VPI” identifies a Virtual Path and a “VPI/VCI” identifies a Virtual Channel. A Virtual Channel requires both the VPI and VCI values.

Each switch contains a table of VPI and VPI/VCI values relating to each physical link. Each incoming VPI/VCI is joined with an outgoing VPI/VCI. If an incoming cell passes through the switch, it is switched to the outgoing VPI/VCI. The incoming and outgoing VPI or VPI/VCI may or may not have the same value. In fact, when a cell is received by a switch and transmitted further along the connection, the cell’s VPI/VCI is sometimes changed. The cell is still on the same logical connection, but each switch may use different numbers to identify that connection.

For example, in the diagram below, incoming cells to the OmniSwitch on VPI 3 are internally switched to VPI 8. (This process is referred to as “label swapping.”) VPI 3 and VPI 8 identify the same logical connection; the switches that establish the links just use different names.



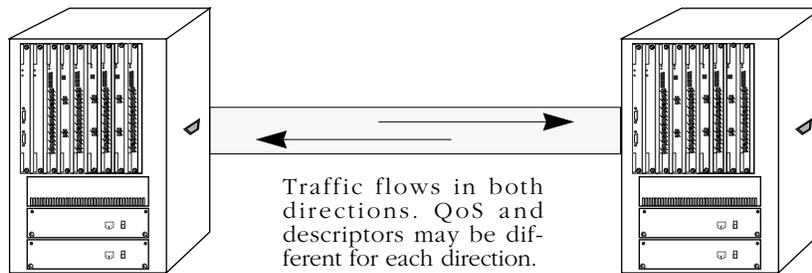
VPI/VCI Values May Not Be Consistent Along a Connection

The VPI value of zero (0) is used for management and ATM uplink (e.g., LANE) connections. Within all Virtual Paths, VCI values ranging from 0 to 31 are reserved for circuit management.

Point-to-Point Virtual Circuits

A point-to-point virtual circuit is a single logical connection between two switches. Each switch may use different VPI and VPI/VCI values to identify the connection. Traffic can flow in both directions on a point-to-point circuit. However, Quality of Service and traffic descriptors can be configured differently for each direction on the circuit.

Each physical port on a CSM-155 module supports up to 4096 point-to-point virtual circuits, and each port on a CSM-622 module supports up to 4096 point-to-point virtual circuits per port.



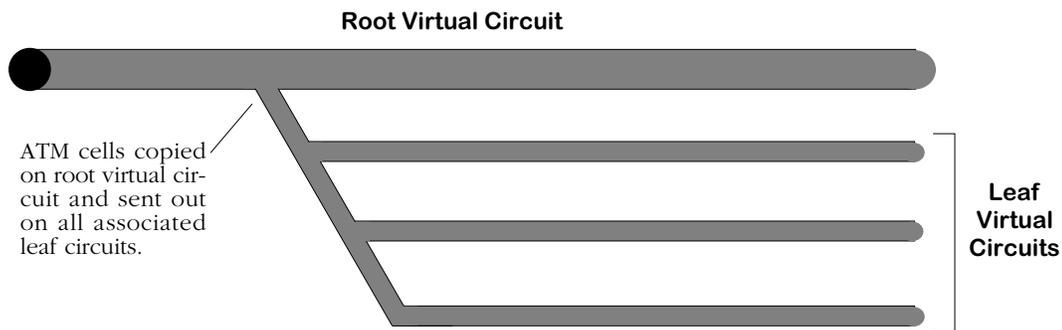
A Point-to-Point Virtual Circuit

Point-to-Multipoint Virtual Circuits

Point-to-multipoint virtual circuits, also referred to as “multicast” virtual circuits, may be configured on any virtual circuit. Within a point-to-multipoint virtual circuit, one circuit is the primary, or “root,” circuit and the others are “leaf” circuits. Quality of Service (QoS) and other traffic parameters are set up for the root circuit and these same parameters are inherited by all leaf circuits.

An entire CSM-155 module supports 8192 point-to-multipoint virtual circuits, and a CSM-622 module supports up to 16,384 point-to-multipoint connections.

Functionally a point-to-multipoint virtual circuit operates by copying a cell for each output leaf circuit and sending that copied cell out each circuit. Data traffic flows from root to leaf, but not from leaf to root. Leaf virtual circuits do not communicate directly with each other on a point-to-multipoint connection.



A Point-to-Multipoint Virtual Circuit

PVCs, SVCs, and Soft PVCs

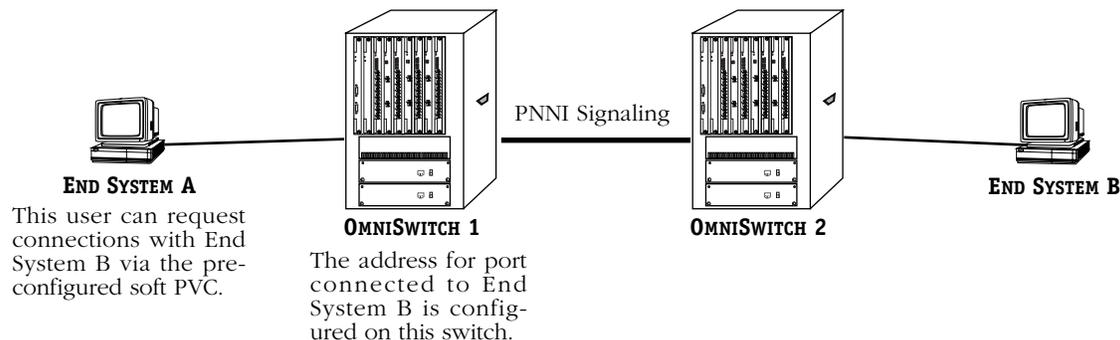
Virtual circuits may be permanent or switched. Permanent Virtual Circuits, or PVCs, must be configured through the **cvc** command, which is described in *Creating a Permanent Virtual Circuit* on page 41-33. PVC information is stored in flash memory on the MPM module; if you restart the switch, the PVC would be restored. Switched Virtual Circuits, or SVCs, are learned by the OmniSwitch through communication with the ATM attached devices. SVCs are built up and taken down based on demands for virtual connections by ATM end devices. If an SVC connection is lost or the switch is restarted, then the circuit is lost and the source device must request the connection again.

◆ Note ◆

See *Configuring a Cell Switch for Switched Virtual Circuits (SVCs)* on page 41-46 for information on configuring a cell switch for SVCs.

The OmniSwitch also supports “soft PVCs.” Like standard PVCs, soft PVCs require some user configuration. However, like SVCs, soft PVCs use PNNI signaling to establish connections. The **scvc** command is used to set up soft PVCs (see Chapter 42, “Advanced CSM Management”). Configuration data for soft PVCs is saved; if the OmniSwitch is restarted, the soft PVCs still exist.

The following diagram illustrates a soft PVC configuration. The soft PVC actually stretches from the port connected to End System A to the port connected to End System B; the destination address is the address of the port connected to End System B. You can find the address of this port through the **vap** command.



Soft PVC Configuration

The following table outlines the differences between the three types of virtual circuits:

Characteristics of PVCs, SVCs, and Soft PVCs

Type of Virtual Circuit	User Configured?	Command Used to Configure	Information Saved On Restart?	Connection Always Up?
PVC	Yes	cvc	Yes	Yes
SVC	No	N/A	No	No
Soft PVC	Yes	scvc	Yes	No

ATM Traffic Types

ATM can support data, voice, and video traffic. Each type of traffic uses the standard 53-byte cell with a 5-byte header, but the bandwidth and QoS requirements for each type of traffic may be different. Some traffic types are time-dependent and very sensitive to delays in the transmission of cells. Other traffic types are content-dependent and very sensitive to cell loss.

Time-dependent traffic, also called “isochronous” traffic, includes voice, video, and multimedia traffic. For example, real-time video requires that cells be received in order with little space between them. Loss of non-critical cells for a video might lower the quality of the video somewhat, but variation in the speed at which video traffic is received might result in jitter that would render the received cells useless.

Content-dependent traffic, such as data traffic, requires that a high amount of the original transfer be received. Data traffic is sensitive to cell loss, but can tolerate variations in the time of cell delivery over the network. For example, a file transfer can withstand a delay of a second or two, but loss of data would mean that the resulting data would not meet the demands of the application and retransmission would be required.

Because ATM can deal with the demands of different types of traffics, several categories of traffic have been defined. These types are as follows.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) traffic is the most time-dependent of the traffic types. CBR traffic consists of a continuous stream of bits flowing at a predefined constant rate. Once transmission of CBR traffic begins, it must be continued uninterrupted, end-to-end, until its completion. In addition, buffering on both ends of the connection must ensure proper ordering of traffic. CBR traffic may include circuit emulation (i.e., transport of an entire T1 or E1 circuit), voice, video, or PABX traffic.

Real-Time Variable Bit Rate (rt-VBR)

There are two types of Variable Bit Rate (VBR) traffic—real-time and non-real-time. Both types, like CBR traffic, require guaranteed delivery service. However, the data rate at which VBR traffic can flow may vary; cell traffic does not have to be constant as with CBR traffic. Real-time VBR (rt-VBR) traffic is more sensitive to transit delays and jitter than non-real-time VBR (nrt-VBR) traffic. Real-time VBR traffic may include compressed video, compressed voice with silence suppression, or HDLC link emulation with idle removal.

Some VBR encoding schemes mark essential cells (i.e., cells that are required to keep up the quality of the application) and less essential cells (i.e., optional cells that simply improve the voice or picture quality) differently. In marking high and low priority cells differently, the lower priority cells can be discarded under congested conditions.

Non-Real-Time Variable Bit Rate (nrt-VBR)

Non-real-time Variable Bit Rate (nrt-VBR) traffic is similar to real-time VBR traffic but it has more tolerance for transit delay and jitter. Non-real-time VBR traffic may include frame relay traffic.

Available Bit Rate (ABR)

Available Bit Rate (ABR) traffic requires guaranteed delivery service for applications that can tolerate a wide variation in transmission delay. Services for ABR traffic reduce cell loss but only use bandwidth as it becomes available after other higher-priority traffic types (i.e., traffic requiring guaranteed delivery and low transit delay, such as CBR and VBR) have been supported. ABR traffic typically includes data traffic, which is not tolerant to cell loss, but can tolerate variations in the speed of transit.

ABR traffic uses Resource Management (RM) cells to dynamically control the rate of traffic as network conditions change. The network and ATM End Systems (ESs) communicate via RM cells about the ability of each End System to receive traffic at a given rate and about general network conditions. The network informs the ES of congestion on the network and the rate at which to send data. The OmniSwitch does not currently support ABR traffic. Resource Management is discussed further in *Flow Control* on page 41-12.

Unspecified Bit Rate (UBR)

All LAN traffic sent today uses Unspecified Bit Rate (UBR) traffic. The ATM network makes its “best effort” to deliver UBR traffic. Delivery is not guaranteed, and is normally only transferred after other traffic types have been serviced. Under congestion conditions, UBR traffic will be discarded before other traffic types. However, with OmniSwitch’s buffer management, congestion will be avoided. When congestion does occur, Partial Packet Discard (PPD) and Random Early Discard (RED) can provide high throughput for UBR traffic.

Quality of Service (QoS)

The different types of network traffic that ATM supports (voice, video, and data) require different treatment by the network. As discussed in *ATM Traffic Types* on page 41-8, each traffic type varies in its tolerance for cell loss, cell transfer delay, and cell delay variation. These differences translate to different service levels.

Each service level has certain transmission characteristics. These transmission characteristics include Cell Loss Ratio (CLR), Cell Delay Variation (CDV), and Cell Transfer Delay (CTD). The CLR is a measure of the number of cells lost as a percentage of the total number of transmitted cells. The CDV, also referred to as “jitter,” is the change in cell spacing as traffic moves from one switch to another switch. CTD is a measure of the amount of delay that can be expected from the time a cell is sent from one node to another, or from the first node in a Virtual Path to the end node in the path. The CLR, CDV, and CTD are defaulted for each service level; they are not user-configurable on the OmniSwitch in this release.

Each service level additionally requires a different traffic contract and uses a different Generic Cell Rate Algorithm (GCRA). The traffic contract and GCRA can be partially controlled by the user. See *Traffic Policing and Leaky Bucket Algorithms* on page 41-19 for more information on the traffic contract and GCRA.

A service level is definable at the virtual circuit level through the **cvc** or **scvc** commands. A Class of Service must be specified for each virtual circuit (Virtual Path or Virtual Channel).

The ATM Forum defines four (4) different service classes and one unspecified service class. The OmniSwitch is compliant with the ATM Forum classes and expands on these service levels by providing up to sixteen (16) user-configurable priority levels. The priority level is definable on a per virtual circuit basis and provides an additional layer of granularity in defining traffic priority. For example, circuits with the same Class of Service may contain different priority values; the circuit with higher priority will be given preference over the other circuits during times of congestion even if the two circuits use the same Class of Service. The OmniSwitch supports the following classes of service.

Class 1: Constant Bit Rate (CBR)

Class 1 supports Constant Bit Rate (CBR) traffic. It provides the service and performance of a private digital line. Traffic support may be CBR or CBR from a primary reference source, which is given the highest priority. Class 1 service guarantees zero cell loss. It may include real-time VBR traffic when a traffic contract requiring a Maximum Burst Size (MBS) of 2 or less is used. If a virtual connection is created for real-time VBR traffic and an MBS parameter greater than 2 is specified, then Class 1 will additionally support VBR traffic for real-time applications. Otherwise, Class 1 service includes only CBR traffic.

Class 2: Real-Time Variable Bit Rate (rt-VBR)

Class 2 supports Variable Bit Rate (VBR) traffic for real-time applications such as audio and video. It may include support for packetized video and audio in teleconferencing and multimedia applications.

Class 3: Non-Real-Time Variable Bit Rate (nrt-VBR)

Class 3 supports VBR traffic for non-real time, connection-oriented traffic. This may include traffic that is sensitive to cell loss but not sensitive to transit delays, such as frame relay traffic.

Class 4: Available Bit Rate (ABR) and Unspecified Bit Rate (UBR)

Class 4 supports Available Bit Rate (ABR) and Unspecified Bit Rate (UBR) traffic. This may include traffic from connectionless data protocols, such as IP and LAN Emulation.

Unspecified Class: Unspecified Bit Rate (UBR)

The QoS class for Unspecified Bit Rate (UBR) traffic is transmitted on a “best effort” basis. The highest speed will be achieved after traffic in other classes have been serviced.

Flow Control

The OmniSwitch supports two forms of flow control: Explicit Rate Resource Management (RM) and the Explicit Forward Congestion Indicator (EFCI). These flow control mechanisms are used to prevent congestion by informing ATM End Systems about congestion conditions before they worsen. Resource management is used to control the flow of Available Bit Rate (ABR) traffic through the use of RM. EFCI notifies network devices of congestion through the use of a bit within the header of an ATM cell.

Resource Management

In the explicit rate method of flow control, the network continuously provides ATM end stations with instant information on the availability of bandwidth along the virtual circuit path. Through the use of Resource Management (RM), end stations learn the maximum current rate (in cells/second) at which cells can be transmitted. This information leads to more efficient link utilization.

Resource management is only available for connections reserved for ABR traffic. Such flow control is not useful for traffic types that require a constant or nearly constant bit rate, such as CBR and VBR traffic. Flow control is not used with CBR traffic because the rate of flow must always be constant. VBR traffic rates do vary, but variations are caused by characteristics of the VBR traffic itself rather than external flow controls. The OmniSwitch does not currently support resource management.

Explicit Forward Congestion Indication (EFCI)

An ATM cell header contains a congestion-control bit called the Explicit Forward Congestion Indication (EFCI). As an ATM switch, the OmniSwitch sets this bit on cells during times of congestion. When an ATM End System (such as a LAN switch) sees the EFCI bit set, it knows that congestion is occurring on the virtual circuit. That LAN switch may then adjust cell flow downward until cells without the EFCI bit set are received.

In addition to setting EFCI, the OmniSwitch provides statistics on the number of EFCI cells received and forwarded.

Traffic Management

The OmniSwitch uses a variety of methods to manage traffic on its virtual circuits. The goal of traffic management is to prevent congestion. Congestion can lead to traffic queuing, decreased performance, and cell discarding. The OmniSwitch provides the following methods for preventing congestion and managing traffic:

- Buffer management
- Traffic Contract Parameters
- Class of Service
- Virtual Circuit Priority

The OmniSwitch buffer management scheme is the first level of traffic management. Buffer management is handled automatically within the hardware cell switching fabric and does not require user configuration. The buffer management scheme used by the ATM cell switching fabric is described in Chapter 40, “Cell Switching Modules (CSMs).”

Each virtual circuit has a set of parameters and algorithms that comprise the “traffic contract.” These parameters, called “traffic descriptors,” describe how fast data can flow on the circuit and the maximum size of a burst allowed on the circuit. When traffic violates these parameters, it is subject to a policing algorithm referred to as the Generic Cell Rate Algorithm (GCRA). The GCRA may tag cells for discard eligibility, or simply discard cells that violate the traffic contract.

The traffic contract and GCRA affect only traffic on the virtual circuit for which they are defined. Within a Virtual Path or a single physical link, some virtual circuits will have a higher priority than others due to their Class of Service and User Priority—two variables that can be configured through OmniSwitch software. If congestion reached levels that could not be managed by buffers or GCRA, the OmniSwitch would use Class of Service and User Priority to determine which traffic would receive priority on the physical link.

The OmniSwitch with ATM switching functionality uses the following information to determine how to police, tag, and discard traffic:

- Cell Loss Priority (CLP)
- Traffic Contract Descriptors
- Traffic Contract Enforcement Methods

Some ATM cells within a single virtual circuit may have a higher priority than other cells in the same circuit. The priority level of a cell is determined by its Cell Loss Priority (CLP) bit setting. The OmniSwitch uses this priority bit to decide whether some cells will be discarded under certain conditions.

The traffic contract is comprised of combinations of traffic descriptors that specify maximum rates of data flow along the circuit. When there is a violation of one or more of these parameters, the GCRA uses several different enforcement methods to police the traffic.

Cell Loss Priority (CLP) and Policing

The Cell Loss Priority (CLP) bit is a 1-bit field in the ATM cell header that indicates the relative priority of the cell. It can be used during times of congestion to discard cells with a low priority and keep cells with a high priority. Cells with a CLP bit set to 0 (CLP=0) are high priority and cells with a CLP bit set to 1 (CLP=1) are low priority.

The CLP bit is also used by the OmniSwitch as an identifier. Some traffic descriptors and policing algorithms will only monitor high priority or low priority cells. Sometimes, the OmniSwitch will monitor both types of cells; when both types of cell flows are monitored, the identifier “CLP=0+1” is used.

The cell flows monitored, or policed, by the switch will depend on the Class of Service for a virtual circuit and the traffic descriptor specified for the circuit. There are four possible police modes (summarized in the following table).

Cell Flows Monitored in Each Police Mode

Policing Mode	Cell Flow Monitored	Explanation
No Policing	None	No policing done. This mode is not used in the switch.
Police 1	CLP=0	Policing only on the CLP=0, or high priority, cell flow. This mode is used only in the second leaky bucket.
Police 2	CLP=1	Policing only on the CLP=1, or low priority, flow. This mode is not used in the switch.
Police 3	CLP=0+1	Policing on both CLP=0 (high priority) and CLP=1 (low priority) cell flows. This mode is used in the first leaky bucket for all traffic types.

In the current release, only two policing options are used (Police 1 and Police 3), and these two options are not user-selectable. Depending on the traffic descriptor chosen and the GCRA employed, either the Police 1 or Police 3 mode will be used.

The cell flow monitored for all traffic types is detailed in a series of tables in the section, *The ATM Menu* on page 41-26.

Tagging Based on CLP

During times of congestion, the Generic Cell Rate Algorithm (GCRA) (described in *Traffic Policing and Leaky Bucket Algorithms* on page 41-19) may use a technique called “tagging” to change the CLP bit value. Depending on the parameters of a traffic contract, congestion may cause the OmniSwitch to change CLP=0 cells to CLP=1 cells, changing their status from high priority to low priority. The traffic contract may also cause the cell to be discarded.

Policing and AAL5 Discarding

On CSMs with the newer IOP2 ASIC (shown in the table below), policing will fail if either of the following methods of AAL5 discarding is enabled:

- Partial Packet Discard (PPD)
- Early Packet Discard (EPD)

Therefore, you must use policing or enabling AAL5 discarding when you create a Permanent Virtual Circuit (PVC) with the **cvc** command (which is described in *Creating a Permanent Virtual Circuit* on page 41-33) or a Soft PVC (SPVC) with the **scvc** command (which is described in Chapter 42, “Advanced CSM Management.”)

On CSMs with the IOP2 ASIC, EPD is the default if Unspecified Bit Rate (UBR), Variable Bit Rate Non-Real Time (VBR_NRT), or Available Bit Rate (ABR) is selected as the transport priority traffic type. To make AAL5 discarding disabled as the default setting on a switch, add the following line to the management module command file (**mpm.cmd** on the MPM-1G, **mpmc.cmd** on the MPM-C, and **mpm3.cmd** on the MPM-III):

```
aal5_dx=0
```

This line *must* be placed before the **cmlnit** line. See Chapter 11, “Managing Files,” for more information on editing the command file.

CSMs with the IOP2 ASIC

CSM Module	Part Number	CSM Module	Part Number
CSM-155-6M2S	P/N 050113-76	CSM-622FSH-2E	P/N 050133-88
CSM-155-6M2SL	P/N 050113-81	CSM-A25-12	P/N 050134-68
CSM-155-8	P/N 050113-75	CSM-A25-24	P/N 050134-69
CSM-155-8S	P/N 050113-73	CSM-U	P/N 050157-88
CSM-155C-8	P/N 050113-74	FCSM-I-4C	P/N 050129-68
CSM-155-FSL-8	P/N 050113-80	FCSM-IIW-4C	P/N050181-68
CSM-622-2E	P/N 050133-90	FCSM-IIW-4C	P/N 050181-66
CSM-622-2SE	P/N 050133-89	CSM-U+	P/N 050345-66

Traffic Contract Descriptors

Each Virtual Circuit—either a Virtual Path Connection or Virtual Channel Connection—has a defined traffic contract. This traffic contract includes a description of the type of traffic that will use the circuit, the Class of Service expected on that circuit, and a traffic descriptor that quantifies the cell rate allowed.

Traffic descriptors are defined for each direction of a connection—from source to destination and from destination to source. It is possible for traffic descriptor values to be different in each direction. Values for the following traffic descriptor parameters can be specified through software.

Peak Cell Rate (PCR). The maximum number of cells per second allowed on the virtual circuit. The PCR is specified for all types of ATM traffic.

Sustainable Cell Rate (SCR). The maximum average cell rate (in cells per second) allowed for traffic. The SCR is always less than the Peak Cell Rate. The SCR is not specified for Constant Bit Rate (CBR) traffic, as this traffic requires a steady data flow at all times. For CBR traffic, the PCR is equal to the SCR.

Maximum Burst Size (MBS). The maximum number of cells that can be sent in a burst at the Peak Cell Rate. The MBS is not specified for CBR traffic. CBR traffic is constant and continuous, not bursty.

The PCR, SCR, and MBS parameters are combined into six (6) traffic descriptors. These traffic descriptors also include information on policing and enforcement modes. (See 3) *Requested Tx Traffic Descriptor Type* on page 41-41 for descriptions of the six traffic descriptors.) Different Classes of Service require different traffic descriptors. For example, as discussed earlier, CBR traffic does not require setting the SCR or MBS traffic parameters. In addition, other types of traffic may require setting all traffic parameters, but the parameters may apply to only CLP=0 cells or to the combined CLP=0+1 cell flow.

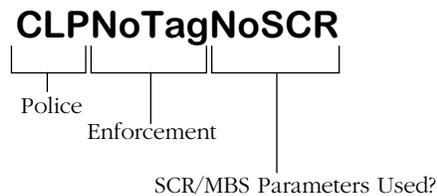
The following table outlines the cell flow(s) checked (or policed) by the PCR, SCR, and MBS parameters for each traffic descriptor. The traffic descriptor names used in the table are the same ones used in User Interface software.

Traffic Checked for Each Traffic Descriptor Bundle

Traffic Descriptor	Peak Cell Rate (PCR) Check	Sustained Cell Rate (SCR) Check	Maximum Burst Size (MBS) Check
NoCLPNoSCR	CLP=0+1	Not Checked	Not Checked
CLPNoTagNoSCR	CLP=0+1 and CLP=0	Not Checked	Not Checked
CLPTagNoSCR	CLP=0+1 and CLP=0	Not Checked	Not Checked
NoCLPSCR	CLP=0+1	CLP=0+1	CLP=0+1
CLPNoTagSCR	CLP=0+1	CLP=0	CLP=0
CLPTagSCR	CLP=0+1	CLP=0	CLP=0

Understanding Traffic Descriptor Names

Each traffic descriptor name contains three (3) parts. The first part indicates the police mode, the second indicates the enforcement mode, and the third indicates traffic descriptor parameters that can be set. The following diagram identifies these three parts.



The first part tells you something about the type of traffic being checked, or policed, by leaky buckets. This part will be either **NoCLP** or **CLP**. **NoCLP** means that only the aggregate of CLP=0+1 traffic will be checked. **CLP** means that CLP=0 traffic will be checked and CLP=0+1 traffic may also be checked.

The second part of the traffic descriptor name tells you something about the traffic enforcement method. The options are **Tag** and **NoTag**. (Some traffic descriptors do not list either **Tag** or **NoTag**; in these cases, the implied option is **NoTag**.) **Tag** means that for CBR and VBR traffic during periods of no congestion, cells will be tagged when the traffic contract is violated.

The third part indicates whether Sustained Cell Rate (SCR) and Maximum Burst Size (MBS) parameters are used as part of the traffic contract. **SCR** means that you can specify SCR and MBS parameters, and **NoSCR** means that you only specify a Peak Cell Rate (PCR) parameter.

Traffic Contract Enforcement

Traffic descriptors indicate the cell flow to monitor and the parameters to check cell flows against. Once traffic violates any of the specified parameters, some form of traffic enforcement will take place. The GCRA, or leaky bucket, determines the type of enforcement option used. Generally, traffic that violates the specified contract will either be tagged for discard eligibility or it will be discarded.

The OmniSwitch uses enhanced GCRA that employ congestion-based traffic enforcement in addition to standard static enforcement. Congestion-based traffic enforcement discards cells only when there is congestion; it does not discard cells when there is plenty of bandwidth on a connection. Static traffic enforcement discards any cells that violate traffic contract parameters, even when there is available bandwidth to support the transporting of these cells. The OmniSwitch provides an option for static enforcement, but also provides three congestion-based enforcement methods.

The following table outlines what happens to cells that violate the traffic contract during times of no congestion and times of congestion under the four enforcement options:

What Happens to Traffic Exceeding the Traffic Contract

Enforcement Option	During Congestion		No Congestion	
	CLP=0	CLP=1	CLP=0	CLP=1
Congestion 1	Tag	Discard	Tag	Tag
Congestion 2	Discard	Discard	Tag	Tag
Congestion 3	Discard	Discard	Tag	Discard
Static	Discard	Discard	Discard	Discard

Enforcement of Contract Tightens ↓

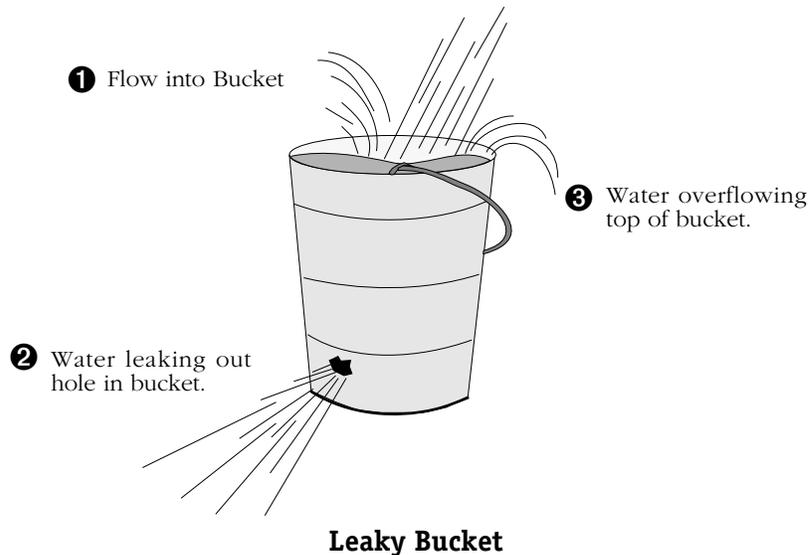
The status of congestion is determined by the amount of available input and output buffers. The congestion method used depends on the Class of Service and traffic descriptor. A different enforcement method may be used for each GCRA. See *The ATM Menu* on page 41-26 for information on the traffic enforcement method used for each Class of Service.

In the current release, only two enforcement options are used (Congestion 2 and Static), and these two options are not user-selectable. Depending on the GCRA employed, either the Congestion 2 or static traffic enforcement method will be used.

Traffic Policing and Leaky Bucket Algorithms

Traffic management for CSM modules involves traffic policing algorithms referred to as Generic Cell Rate Algorithms (GCRAs). These algorithms control what happens to different types of traffic during times of congestion and times of no congestion. These algorithms are also referred to as “leaky buckets” because water flowing through a leaky bucket provides a good analogy for data traffic on a virtual circuit.

It is important to note that the leaky bucket is not a queue and does not buffer, store, or slow down data on a virtual circuit. It is just a model for understanding the traffic contract and what happens to traffic that violates that contract. There are several parts to the leaky bucket that are important. The illustration below points them out:



The size and speed of the flow into the bucket (1 above) depend on the amount of water coming from the source. This water flow is an analogy for the data traffic received on an ATM virtual circuit. The amount of flow will vary depending on buffer management and use of the circuit by ATM devices.

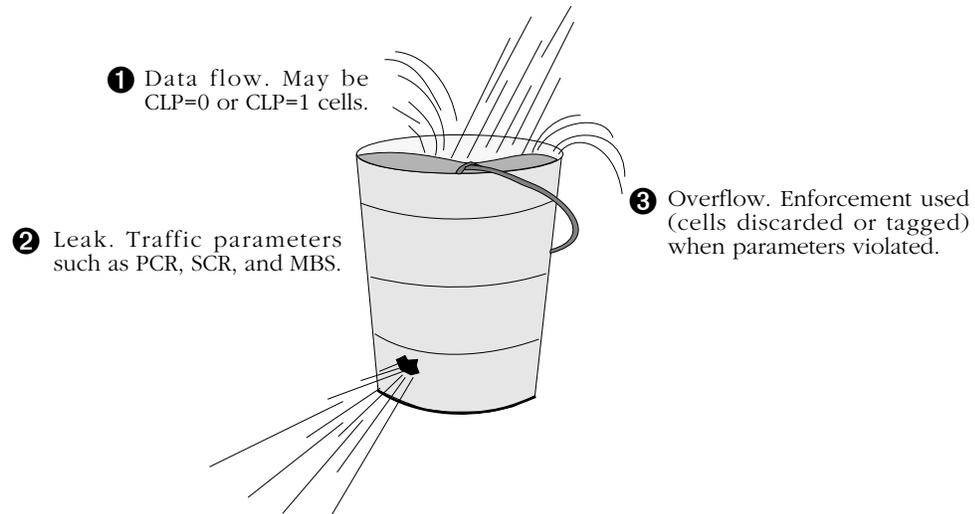
If a bucket has a hole, water will eventually leak out. While this may not be a good thing if you are carrying the water bucket, it is a good thing on an ATM virtual circuit. The hole in the bucket (2 above) is analogous to the traffic parameters for the virtual circuit that measure traffic compliance. These parameters—Peak Cell Rate (PCR), Sustaining Cell Rate (SCR), and Maximum Burst Size (MBS)—specify how fast and how much traffic can flow through the leaky bucket. These parameters are described in *Traffic Contract Descriptors* on page 41-16.

The leaky bucket and the hole do not slow down traffic or imply that traffic is queued; they just indicate how much traffic can flow on the circuit without violating the traffic contract. The larger the hole in the bucket, the larger the traffic parameters.

There may be times on a virtual circuit when traffic is so heavy that it fills the bucket before the rest of the traffic can drain through the hole in the bucket. This case where traffic “overflows” the bucket indicates a violation of the traffic contract (3 above). When traffic overflows the bucket, it is subject to the traffic contract enforcement method used for the particular leaky bucket. Essentially, violating traffic will either be discarded or tagged as eligible for discard. Tagging for discard means changing a cell’s CLP bit to the lower priority (i.e., CLP=1), which means this cell may be discarded during times of congestion. For more information on the CLP bit, see *Cell Loss Priority (CLP) and Policing* on page 41-14.

Traffic Policing and Leaky Bucket Algorithms

The illustration below shows the same leaky bucket with the ATM equivalents for flow into the bucket (❶), the leak or traffic parameters (❷), and overflow or traffic enforcement (❸). These three attributes are used by the leaky bucket algorithm, or Generic Cell Rate Algorithm (GCRA), to measure traffic compliance on the virtual circuit.



The Leaky Bucket as a Traffic Policer

The leaky bucket algorithm is essentially a two-step process—policing and enforcing. In the first step, policing, traffic is checked against traffic parameters defined for the virtual circuit. This step involves ❶ and ❷ in the above illustration. A traffic monitor keeps track of the number of cells exceeding the traffic contract. Depending on the Class of Service and traffic descriptors, one or both of the CLP flows (CLP=0 and CLP=1) will be checked for compliance with the traffic descriptors. The section *Traffic Contract Descriptors* on page 41-16 describes the cell flows that are checked for each traffic parameter.

When cells are not in compliance with the traffic descriptors, the second step of the leaky bucket algorithm, enforcement, begins. Enforcement is the action that the leaky bucket algorithm takes when traffic violates the contract. This step involves ❸ in the above illustration. The enforcement action taken will either be to tag the cell for discard eligibility or to discard the cell. OmniSwitch leaky buckets can be congestion-based, which means the algorithm will consider congestion conditions before taking action. The different enforcement options are described in *Traffic Contract Enforcement* on page 41-18.

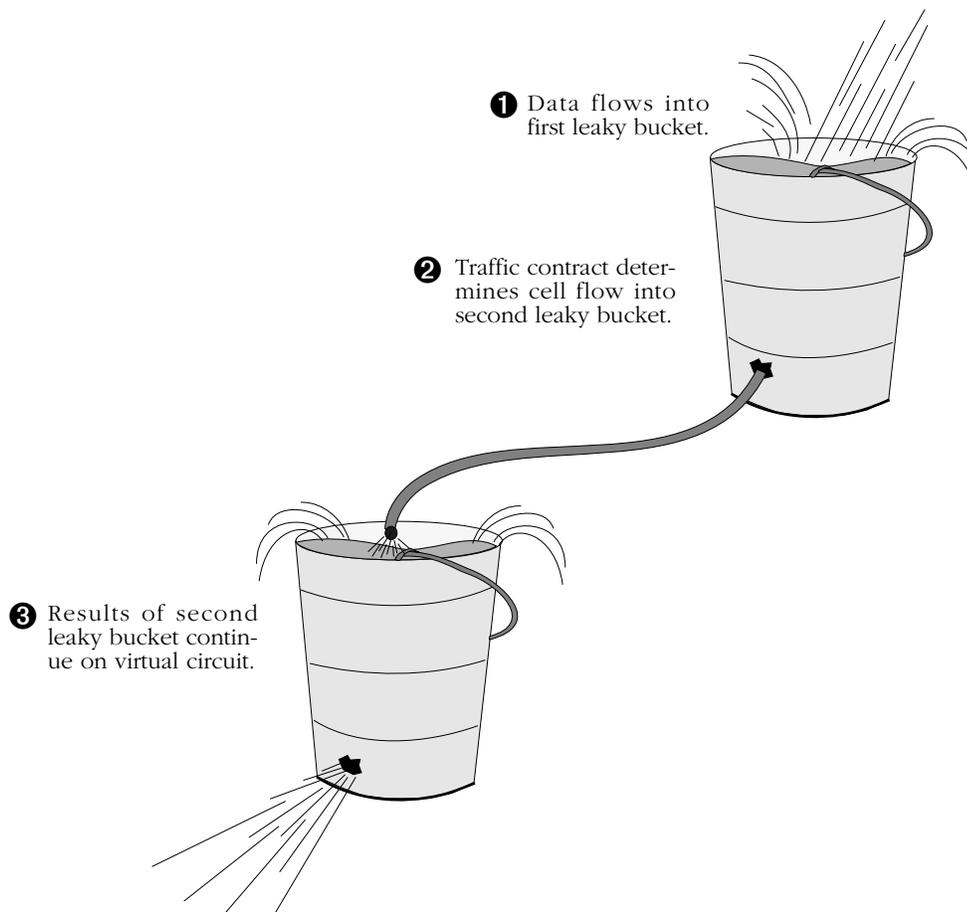
Dual Leaky Buckets

The OmniSwitch actually uses two leaky buckets on each virtual circuit. The second leaky bucket provides an extra check for compliance with the traffic contract. The results of the first leaky bucket flow into the second leaky bucket.

Typically, each leaky bucket monitors a different cell flow and may use a different traffic contract enforcement method. In the first leaky bucket, traffic contract parameters (PCR, SCR, MBS) check the combined cell flow (i.e., $CLP=0+1$).

In the second leaky bucket, either the combined flow ($CLP=0+1$) or the high priority flow ($CLP=0$) is checked. The cell flow that is checked in the second leaky bucket depends on the Class of Service and traffic descriptor selected. See *The ATM Menu* on page 41-26 for the cell flows checked for each Class of Service on the second leaky bucket.

The following illustration shows how the dual leaky buckets function on a virtual circuit.



Dual Leaky Buckets on Each Virtual Circuit

Leaky Buckets and Class of Service

The type of policing and enforcement used by a leaky bucket is determined by the Class of Service and traffic descriptors specified for the virtual circuit. Leaky buckets are not user-configurable in this release.

Within each Class of Service, the policing and enforcement methods are consistent for the first leaky bucket. The first leaky bucket monitors the combined CLP=0+1 cell flow for the Peak Cell Rate (PCR) traffic parameter only.

The second leaky bucket monitors CLP=0 cells or the combined CLP=0+1 cell flow, depending on the traffic descriptor and Class of Service selected. The enforcement method used for the second leaky bucket also depends on the traffic descriptor chosen.

The traffic parameters monitored and the enforcement method used in each leaky bucket is detailed for each Class of Service in tables on the following pages.

Class of Service Profiles

This section provides profiles on the cell flows policed, the enforcement method used, and the default priority assigned to virtual circuits for each traffic descriptor/Class of Service combination. A row is provided for each of the six selectable traffic descriptors (see 3) *Requested Tx Traffic Descriptor Type* on page 41-41 for descriptions of the six traffic descriptor bundles). The “Police” column indicates the cell flow monitored by traffic parameters. The “Enforce” column indicates the enforcement method used (see *Traffic Contract Enforcement* on page 41-18 for a description of enforcement methods). The “Priority” column indicates the user priority value (0-15) assigned to virtual circuits (a lower priority values means higher priority).

Constant Bit Rate (CBR)

Policing and Enforcement in Each Leaky Bucket for Class of Service 1(CBR)

Traffic Descriptor Specified	Leaky Bucket 1 (GCRA A)			Leaky Bucket 2 (GCRA B)		
	Police	Enforce	Priority	Police	Enforce	Priority
None	CLP=0+1	Static	4	CLP=0+1	Static	4
NoCLPNoSCR	CLP=0+1	Static	4	CLP=0+1	Static	4
CLPNoTagNoSCR	CLP=0+1	Static	4	CLP=0	Static	4
CLPTagNoSCR	CLP=0+1	Congestion 3	4	CLP=0	Congestion 2	4
NoCLPSCR	Not Applicable. SCR and MBS parameters are not used with CBR traffic.					
CLPNoTagSCR						
CLPTagSCR						

Variable Bit Rate, Real Time (rt_VBR)

Policing and Enforcement in Each Leaky Bucket for Class of Service 2 (rt_VBR)

Traffic Descriptor Specified	Leaky Bucket 1 (GCRA A)			Leaky Bucket 2 (GCRA B)		
	Police	Enforce	Priority	Police	Enforce	Priority
None	CLP=0+1	Static	8	CLP=0+1	Static	8
NoCLPNoSCR	CLP=0+1	Static	8	CLP=0+1	Static	8
CLPNoTagNoSCR	CLP=0+1	Static	8	CLP=0	Static	8
CLPTagNoSCR	CLP=0+1	Congestion 3	8	CLP=0	Congestion 2	8
NoCLPSCR	CLP=0+1	Static	8	CLP=0+1	Static	8
CLPNoTagSCR	CLP=0+1	Static	8	PCR: CLP=0+1 SCR/MBS: CLP=0	Static	8
CLPTagSCR	CLP=0+1	Congestion 3	8	PCR: CLP=0+1 SCR/MBS: CLP=0	Congestion 2	8

Variable Bit Rate, Non-Real Time (nrt_VBR)

Policing and Enforcement in Each Leaky Bucket for Class of Service 3 (nrt_VBR)

Traffic Descriptor Specified	Leaky Bucket 1 (GCRA A)			Leaky Bucket 2 (GCRA B)		
	Police	Enforce	Priority	Police	Enforce	Priority
None	CLP=0+1	Static	8	CLP=0+1	Static	8
NoCLPNoSCR	CLP=0+1	Static	8	CLP=0+1	Static	8
CLPNoTagNoSCR	CLP=0+1	Static	8	CLP=0	Static	8
CLPTagNoSCR	CLP=0+1	Congestion 3	8	CLP=0	Congestion 2	8
NoCLPSCR	CLP=0+1	Static	8	CLP=0+1	Static	8
CLPNoTagSCR	CLP=0+1	Static	8	PCR: CLP=0+1 SCR/MBS: CLP=0	Static	8
CLPTagSCR	CLP=0+1	Congestion 3	8	PCR: CLP=0+1 SCR/MBS: CLP=0	Congestion 2	8

Available Bit Rate (ABR)

Policing and Enforcement in Each Leaky Bucket for Class of Service 4 (ABR)

Traffic Descriptor Specified	Leaky Bucket 1 (GCRA A)			Leaky Bucket 2 (GCRA B)		
	Police	Enforce	Priority	Police	Enforce	Priority
None	CLP=0+1	Congestion 2	10	CLP=0+1	Congestion 2	10
NoCLPNoSCR	CLP=0+1	Congestion 2	10	CLP=0+1	Congestion 2	10
CLPNoTagNoSCR	CLP=0+1	Congestion 2	10	CLP=0	Congestion 2	10
CLPTagNoSCR	CLP=0+1	Congestion 2	10	CLP=0	Congestion 2	10
NoCLPSCR	CLP=0+1	Congestion 2	10	CLP=0+1	Congestion 2	10
CLPNoTagSCR	CLP=0+1	Congestion 2	10	PCR: CLP=0+1 SCR/MBS: CLP=0	Congestion 2	10
CLPTagSCR	CLP=0+1	Congestion 2	10	PCR: CLP=0+1 SCR/MBS: CLP=0	Congestion 2	10

Unspecified Bit Rate (UBR)

Policing and Enforcement in Each Leaky Bucket for Unspecified Class of Service (UBR)

Traffic Descriptor Specified	Leaky Bucket 1 (GCRA A)			Leaky Bucket 2 (GCRA B)		
	Police	Enforce	Priority	Police	Enforce	Priority
None	CLP=0+1	Congestion 2	15	CLP=0+1	Congestion 2	15
NoCLPNoSCR	CLP=0+1	Congestion 2	15	CLP=0+1	Congestion 2	15
CLPNoTagNoSCR	CLP=0+1	Congestion 2	15	CLP=0	Congestion 2	15
CLPTagNoSCR	CLP=0+1	Congestion 2	15	CLP=0	Congestion 2	15
NoCLPSCR	CLP=0+1	Congestion 2	15	CLP=0+1	Congestion 2	15
CLPNoTagSCR	CLP=0+1	Congestion 2	15	PCR: CLP=0+1 SCR/MBS: CLP=0	Congestion 2	15
CLPTagSCR	CLP=0+1	Congestion 2	15	PCR: CLP=0+1 SCR/MBS: CLP=0	Congestion 2	15

The ATM Menu

User Interface commands for configuring and monitoring CSM modules are in the ATM menu. The ATM menu displays as shown below:

Command	ATM Management Menu
vap	View the list of atm ports configurations
map	Modify an atm port configuration
vvc	View virtual channel connections
cvc	Create a virtual channel connection
mvc	Modify a virtual channel connection
dvc	Delete a virtual channel connection
vva	View virtual atm addresses
cva	Create a virtual atm address
mva	Modify a virtual atm address
dva	Delete a virtual atm address
vlat	View ATM LANE LE_ARP table
vat	View ATM CIP Arp table
aat	Add static ATM Arp entry for CIP
dat	Delete static ATM Arp entry for CIP
vss	View ATM Service statistics
vls	View atm layer statistics table
vllrs	View atm layer rx error statistics table
vllts	View atm layer tx error statistics table
vcs	View atm connection statistics table
vcrs	View atm connection rx error statistics table
vcts	View atm connection tx error statistics table
vbwg	View the bandwidth group table
mbwg	Modify the bandwidth group table
vgptovc	View group to VC mapping table (Scaling)
vnac	View current number of atm connecns
vnapc	View current number of atm PTOMP connections
atmlsem	Enables or disables LEC debugs
cvpt	Create VP Tunnel
dvpt	Delete VP Tunnel
mvpt	Modify VP Tunnel
lvpt	List VP Tunnel(s)
svvc	View the Soft PVC Connections
scvc	Create Soft PVC Connection
masrt	Modify entries in ATM Service Registry Table
mclk	Modify CSM clock configuration
vclka	View CSM clock configuration of all ports on the system
vclk	View CSM clock configuration on configured ports only
mcst	Modify CSM clock switching time
vcac	View CSM Port Auto Configuration information
mcac	Modify CSM Port Auto Configuration Parameters
imce	Enable Intelligent Multicast feature
imcr	Disable Intelligent Multicast feature
imci	Display Gain with Intelligent Multicast Enabled
imcd	Display Intelligent Multicast tree
vcst	Display Port & Connection Statistics

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

This menu contains commands that can be used with ATM uplink modules (ASM modules for the OmniSwitch and ASXs for the Omni Switch/Router), the Frame-to-Cell Switching module (FCSM module), and Cell Switching Modules (CSM modules). The commands in the menu operate differently for ASM, FCSM, and CSM modules.

Several of the commands can be used only with ATM access and FCSM modules and are not available for CSM modules. ATM address commands (**vva**, **cva**, **mva**, and **dva**), Classical IP commands (**vat**, **aat**, **dat**), the LAN Emulation command (**vlat** and **atmlsem**), and the traffic shaping commands (**vbwg** and **mbwg**) are used only with ATM access and FCSM modules since they control ATM uplink, or access, connections. In addition, the informational commands **vss**, **vlts**, **vcts**, **vps**, **vpis**, and **vgptovc** are available only for ATM access and FCSM modules.

This chapter describes basic ATM menu commands as they apply to CSM modules. The commands are different when used with ATM access modules or with FCSM internal ports. See Chapter 33, “Managing ATM Access Modules,” for information on how these commands apply to ATM access modules (ASMs and ASXs) and FCSM modules. For special information on how FCSM ports are handled by ATM menu commands see *FCSM Modules in ATM Menu Commands* on page 41-28.

◆ **Note** ◆

The commands for ATM clocking on CSM modules (**mclk**, **vclka**, **vclk**, and **mcst**) are described in Chapter 45, “Clocking ATM Networks.”

For more advanced ATM commands as they apply to CSM modules, see Chapter 42, “Advanced CSM Management.” This chapter contains the documentation for Soft PVC commands (**svvc** and **scvc**), Virtual Path (VP) tunneling commands (**cvpt**, **dvpt**, **mvpt**, and **lvpt**), ATM layer statistics commands (**vls** and **vlrs**), ATM connection statistics commands (**vcs** and **vcrs**), intelligent multicast replication commands (**imce**, **imcr**, **imci**, and **imcd**), and the **masrt** command, which is used to configure LANE Configuration Server (LECS) ATM addresses on a CSM. Additionally, the **vcst** command can be used to display port and connection statistics for CSM modules.

◆ **Important Note** ◆

For Release 4.4 and later, CSM-ABT Traffic Shaping is supported in CLI (Command Line Interface) mode, but not in UI (User Interface) mode. See Chapter 42, “Advanced CSM Management,” and the *Text-Based Configuration CLI Reference Guide* for information about this feature.

FCSM Modules in ATM Menu Commands

The FCSM module, which serves as a link between the frame bus and cell matrix, contains an “internal” logical port that is functionally the same as an ATM access port. You can obtain statistics on this port and configure ATM services on this port. The FCSM logical port will display as port 1 for the slot in which the FCSM port is installed. For example, if the FCSM is installed in slot 3, then its uplink port will display as port **3/1**.

Half of this internal port 1 on the FCSM module is a CSM port. The CSM half of the port is functionally the same as an OC-3c/STM-1 (FCSM I) port or OC-12c/STM-4c (FCSM II) port, and is directly connected to the ASM half of the port. LAN traffic comes in on the ASM half of this internal port and enters the cell switching fabric on the CSM half of the port.

ATM menu commands that display statistics will show information on the ASM half of the FCSM port and on the CSM half. When viewing these commands, keep in mind that these displays reveal information on two halves of the same port.

The following table summarizes the functions of each FCSM port:

FCSM Ports

	Port 1 (FCSM I)	Port 1 (FCSM II)	Port 2 (FCSM I)
ASM half	ATM Services Port	ATM Services Port and Management Data (ILMI, UNI signaling, PNNI)	Management Data (ILMI, UNI signaling, PNNI)
CSM half	Connects ATM Service Port to Cell Matrix	Connects ATM Service Port to Cell Matrix and Management Data (ILMI, UNI signaling, PNNI)	Management Data (ILMI, UNI signaling, PNNI)

The Second FCSM I Port

Both the ASM half of the port and the CSM half of Port 1 on the FCSM module are user-configurable. In some command displays, you may also note that there is a *second* FCSM port on the FCSM I. (The FCSM II has only one internal port.) If the FCSM I were installed in slot 2, this second port would display as port **2/2**.

This second internal port also contains an ATM access half and a CSM half. It is used to pass control signals. Unlike the first FCSM I port, this second port is only partially configurable (i.e., SAR and frame buffer sizes only). Virtual channels will by default be set up on this second port for signaling and ILMI. If PNNI is enabled on this port, then an additional channel will be set up for PNNI.

Modifying a Port Configuration

You can use the **map** command to alter CSM port configuration settings. Ports are configured with default settings until you modify them using the **map** command. To use this command, enter **map** followed by the slot and port number of the CSM port you want to modify. For example, to change settings for port 3 on the CSM module in slot 3, you would enter:

```
map 3/3
```

A screen similar to the following displays:

```
Slot 3 Port 3 Configuration

1) Description (30 chars max)      : CSM PORT
2) ESI (12 hex-chars)             : 000000000000
   NetPrefix (3903488001bc900001017dee30)
3) Max VPI bits (1..11)           : 2
4) Max VCI bits (1..11)           : 10
5) I/F Type { Pub UNI (1), Priv UNI (2),
   PNNI (3), IISP netw (4),
   IISP user (5)                   : Private
6) Phy Protocol {SONET (1), SDH (2): SONET
7) Signaling Ver
   {3.0 (1), 3.1 (2), 4.0 (3) }    : 3.1
8) ILMI Enable { False (1), True (2) } : True
80) CSM Port Auto Cfg
   { Enable (1), Disable (2) }    : Enable
81) ILMI Polling {Off (1), On (2) } : On
9) Timing Mode {Local (1), Loop (2) } : Local
90) Local { Osc (1), Bus (2) }    : Osc
14) Signaling Status (Disable (1)
   Enable (2)                       : Enable
15) Phy Loopback {none (0), diag (1),
   line (2) }                       : None
16) Bandwidth Overbooking Factor
   {0.0=Disable CAC;
   1.0=No Over Booking (default);
   Valid: >= 0.0}                  : 1.0
```

Enter (option=value/save/cancel) :

You change a value in the field by entering the line number for the variable you want to change, an equal sign (=), and the new value for the variable. (Please note that the values for variables 5-9 are represented by option numbers.) For example, to change the **Signaling Ver** field variable to “3.0,” you would enter a 7 (the line number for **Signaling Ver**), an equal sign, and the option number for the new value, as follows:

```
7=1
```

When you are done entering all new values, type **save** at the colon prompt (:) and all new parameters will be saved. If you want to cancel your changes, enter **cancel**. The variables in the **map** command screen are explained in the following sections.

Description

A textual description of this CSM port. The description may be up to 30 characters long. This identifier will be used in displays for other software commands.

ESI

The 20-octet hex ATM address for this CSM port.

Max VPI bits

The maximum number of bits that can be used for Virtual Path Identifiers (VPIs) created on this CSM port. The CSM-U+ supports 0 to 6 bits per VPI (the default is 4 bits) and the CSM-A25-12 and CSM-A25-24W support up to 9 bits per VPI; all other CSM modules support up to 12 bits per VPI. This setting affects the maximum number of Virtual Paths that can be configured on this port. The maximum number of Virtual Paths is $2^n - 1$ where n is the **Max VPI Bits**. For example, if the **Max VPI Bits** is 4, then the maximum number of Virtual Paths on this port will be 15.

◆ Note ◆

The total bits available for VPIs and VCIs is 14 on the CSM-U+, 9 on the CSM-A25-12 and CSM-A25-24W for VPIs or for VPI/VCIs, and 12 on all other CSM modules for VPIs or for VPI/VCIs. You can specify how many bits are allotted for VPIs and how many are for VCIs, but the total must be 14 on the CSM-U+, 9 on the CSM-A25-12 and CSM-A25-24W, and 12 on all other CSM modules.

Max VCI bits

The maximum number of bits that can be used for Virtual Channel Identifiers (VCIs) created on this CSM port. The CSM-U+ supports 8 to 14 bits per VCI (the default is 10) and the CSM-A25-12 and CSM-A25-24W support up to 9 bits per VCI; all other CSM modules support up to 12 bits per VCI. This setting affects the maximum number of Virtual Channels that can be configured on this port. The maximum number of Virtual Channels is $2^n - 1$ where n is the **Max VCI Bits**. For example, if the **Max VCI Bits** is 8, then the maximum number of Virtual Channels on this port will be 256.

I/F Type

Specifies the type of ATM interface that this CSM port supports. The options are as follows:

- Pub UNI** Public UNI. This ATM port will be used for connections to public ATM service carrier switches, such as those used by Telcos.
- Priv UNI** Private UNI. The port is used for private UNI uplinks. Such a port would connect either directly to an ATM workstation, LAN switch, or ATM attached router.
- PNNI 1.0** Private Network-to-Network Interface (PNNI). The port will support PNNI version 1.0 ATM routing, which includes support for a single-peer group mapping.

◆ Important Note ◆

If your software version is prior to 4.1, then you *must* reboot the switch when you change the **I/F Type** from **PNNI 1.0** to **Pub UNI**.

IISP Interim Interswitch Signaling Protocol. Typically, an IISP port would be part of an intermediate ATM node that did not support the PNNI routing protocol. It is used primarily for establishing static routes using the IISP protocol. The two types of IISP ports are network (**IISP netw**) and user (**IISP user**). See Chapter 47, “Managing IISP and PNNI Routes” for further information.

◆ Important Note ◆

If you want to configure and connect two IISP ports having PNNI and ILMI 4.0 capabilities, you must disable CSM port auto configuration and manually configure the ports instead. According to the ATM Forum ILMI 4.0, the two IISP ports will configure themselves as PNNI if you do not disable port auto configuration in this instance. For more information, see Chapter 47, “Managing IISP and PNNI Static Routes.”

Phy Protocol

The type of physical media standard used for this port. In North America, ATM broadband services are delivered over Synchronous Optical Network (SONET) facilities. SONET is a high-speed fiber optic system that uses Synchronous Transfer Level 1 (STS-1).

Outside North America, ATM broadband services use Synchronous Digital Hierarchy (SDH). SDH is a high-speed fiber optic system that uses Synchronous Transfer Mode (STM-1). The OmniSwitch supports both SONET and SDH fiber systems. You select the system with which you want this port to be compatible.

Signaling Ver

The version of the User-to-Network Interface (UNI) used on this port. The switch is compliant with ATM Forum UNI specifications version 3.0 and 3.1. If you have installed the software for multiple-peer group PNNI, then you can also set the signaling version to 4.0.

ILMI Enable

Indicates whether or not you want to enable the Integrated Local Management Interface (ILMI) on this port. Normally, you want to enable ILMI to allow the switch to discover attached ATM End Systems (ESs). If you disable ILMI, then you must configure a static route between this port and all attached ESs. If you want to enable ILMI, select the **True** option. If you want to disable ILMI, select the **False** option.

CSM Port Auto Configuration. Indicates whether or not you want to enable auto configuration on this port.

ILMI Polling. The ILMI status messages sent out at regular intervals (about every 3-5 seconds) from this port. If you want to enable ILMI polling, select the **On** option. If you want to disable ILMI polling, select the **Off** option. The default value for **ILMI Polling** is **On**.

Timing Mode

The clock source from which modules derive their timing. Two transmit timing modes are available: **local timing** and **loop timing**.

Local Timing. For local timing mode, you set which source a port is to use to drive its transmit data. The options are:

- The local oscillator (**Osc**). Using the local oscillator (located on the CSM module) will provide the backplane with a Stratum 4-level clock.
- The bus backplane (**Bus**). You can select either the 8 kHz or 19 MHz bus, depending upon the port type. Select this option if you are planning to provide a single reference clock across the network.

Loop Timing. Typically implemented with public network connections. In loop timing, the reference clock is derived from the receive data, then fed back out with the transmit data.

Signaling Status

Indicates whether or not you want to enable the Service-Specific Connection Oriented Protocol (SSCOP). SSCOP operates on the ATM control plane and is a peer-to-peer protocol that helps set up connections, detect errors in connection, and correct connection errors.

Phy Loopback

The loopback configuration for this port. In live network situations, use the **none** option, which is the default. The other two loopback configurations, **diag** and **line**, are intended mainly for debugging or test situations. The following provides more detail on the three loopback configurations:

None	No loopback occurs between receive and transmission paths.
Diag	Interface transmission path is connected to receive path at the connectors. The port receives its own transmission rather than the signal coming over the cable.
Line	The interface receive path is looped to the transmission path at the connectors. The signal on the receive connector is not passed into the UNI and processed.

Bandwidth Overbooking Factor (CAC & Call Overbooking)

The Call Overbooking feature for this port (default = No Overbooking). When Overbooking is enabled, available bandwidth on a CSM virtual port can be calculated to reduce or increase cell loss probability on a logical or physical link. This feature can help minimize traffic congestion and optimize access to network resources for different QoS classes. To enable this feature, specify a value greater than **0.0**. (Note that extremely high values will be discarded, and the previous setting will be retained.) This value can also be changed to **0.0**, to disable Connection Admission Control (CAC). The factory default setting is used for normal port operation without enabling Bandwidth Overbooking.

0.0	Disables CAC (Connection Admission Control).
1.0	No Overbooking - normal port operation (default).
Valid >= 0.0	Specifying a value between 0.0 and 1.0 underbooks the port's maximum physical capacity (for use with highly loss-sensitive bursty traffic). Values greater than 1.0 enable Overbooking (to increase port capacity utilization, depending on bandwidth resource availability).

Creating a Permanent Virtual Circuit

The **cvc** command allows you to create a Permanent Virtual Circuit (PVC) for a physical port and logical VPI or VPI/VCI that you specify. It contains several suboptions for configuring multicast virtual circuits and traffic contract parameters. This section is divided into several subprocedures, all of which are part of the **cvc** command. The subprocedures are as follows:

- Setting Up Basic VC Parameters
- Setting Up Multicast Virtual Circuits
- Configuring Traffic Parameters
- Configuring Statistics and Priority Parameters

You cannot configure Switched Virtual Circuits (SVCs) or Soft PVCs through the **cvc** command. SVCs are set up automatically by the ATM network and Soft PVCs are configured through the **scvc** command. See Chapter 42, “Advanced CSM Management,” for information on configuring soft PVCs.

Setting Up Basic VC Parameters

To begin setting up the virtual circuit, enter **cvc** followed by the slot number, a slash (*/*), and the port number where you want to set up the virtual circuit. After the slot and port number, leave a space, then specify the Virtual Path Identifier (VPI), a slash (*/*), and then the Virtual Channel Identifier (VCI). (You do not have to include the VCI if you are setting up a Virtual Path only.) For example, the following command specifies a virtual circuit with a VCI of 100, and VPI of 2 on the first port on the module in slot 5:

```
cvc 5/1 2/100
```

Note that these values indicate the *input* port and *input* VPI/VCI for this virtual circuit on this OmniSwitch. Output parameters are specified later through **cvc** screen options.

The following message displays for a moment:

```
creating csm connection, please wait .....
```

The initial message will be followed by a screen of options similar to the following:

```
Slot 4 Port 1 Connection VPI 0 VCI 256 Configuration
Available bandwidth: Tx=353208 Rx=353208
1) Description (30 chars max)           : Connection 256
2) Outgoing Slot (1-9)                 : 4
3) Outgoing Port (1-08)                : 1
4) Outgoing VPI (1-0015)               : 0
5) Outgoing VCI (1-0255)               : 256

6) Channel Type { vc-nni(3), vc-uni(4) } : VC-UNI
7) Transport Priority { CBR(1), CBR_PRS(2), VBR_RT(3), : UBR
   VBR_NRT(4), ABR(5), UBR(6) }
8) Multicast Enable { disable(0), enable(1) } : Disabled
10) AAL5 Discard Continue { disable(0), enable(1) } : Disabled

11) Traffic Parameters
13) Advanced Parameters

Enter (option=value/save/cancel) :
```

You make changes by entering the line number for the option you want to change, an equal sign (=), and then the value for the new parameter. When you are done entering all new values, type **save** at the colon prompt (:) and all new parameters will be saved. The following sections describe the options you can alter through this menu.

1) Description

A textual description of this virtual circuit. You can use up to 30 characters to describe a virtual circuit. For example, if this VC will be used primarily to carry traffic for multimedia workstations, you may want to describe it as "Building #1 VC."

2) Outgoing Slot

The slot number for the module on which output traffic is forwarded along the virtual circuit path.

3) Outgoing Port

The port number on which output traffic is forwarded along the virtual circuit path.

4) Outgoing VPI

The Virtual Path Identifier (VPI) on which output traffic is forwarded along the virtual circuit path.

5) Outgoing VCI

The Virtual Channel Identifier (VCI) on which output traffic is forwarded along the virtual circuit path. This field only displays if you are setting up a Virtual Channel Connection; a VCI is not required if you are setting up just a Virtual Path.

6) Channel Type

The type of connection supported by this channel. Normally, this circuit will connect to a user device, such as an ATM workstation, or to another ATM switch, such as an OmniSwitch. When connected directly to a user device, this connection would be considered a UNI connection (option 4). When connected to another ATM switch, this connection would be considered an NNI connection (option 3).

7) Transport Priority

Indicates the type of traffic and its priority on this connection. Some traffic types require higher priority than others because any disruption in the connection will cause unacceptable results. For example, a circuit emulating a private digital line requires a continuous flow of traffic. Circuit emulation requires Constant Bit Rate (CBR) transport and is given a higher priority than other less sensitive traffic. On the other hand, data connections can tolerate some delay in the connection. Data traffic usually requires Unspecified Bit Rate (UBR) transport. UBR is the default value for this option.

When you set this option, the Class of Service and Priority level of the circuit are automatically selected in **cvc** submenus. The following transport values are available:

CBR (1)	Constant Bit Rate
CBR_PRS (2)	Constant Bit Rate with Primary Reference Source
VBR_RT (3)	Variable Bit Rate, Real Time
VBR_NRT (4)	Variable Bit Rate, Non-Real Time
ABR (5)	Available Bit Rate
UBR (6)	Unspecified Bit Rate

The numbering on the screen indicates the priority level of the traffic except in the case of the two CBR traffic types: **CBR_PRS (2)** is given a higher priority than standard **CBR traffic (1)**.

8) Multicast Enable

Enables multicast, or point-to-multipoint, virtual circuits on this primary virtual circuit. If you enable multicast support, you will receive additional prompts to indicate the identifier values (VPI or VPI/VCI) for multicast virtual circuits. Multicast virtual circuits are leaves of the primary, or root, virtual circuit. In addition, multicast virtual circuits inherit QoS and traffic parameters from the root virtual circuit. See *Point-to-Multipoint Virtual Circuits* on page 41-6 for more information on the multicast virtual circuits. The steps for setting up individual point-to-multipoint virtual circuit are described later in *Configuring Point-to-Multipoint Virtual Circuits* on page 41-38.

10) AAL5 Discard

Indicates how AAL5 PDU cells are discarded. Configuration of this option varies, depending on the following two factors:

1. The **Transport Priority** value entered in option 7. CBR, CBR_PRS, and VBR_RT traffic types do not carry AAL5 PDU cells and are therefore not configurable for AAL5 Discard. See 7) *Transport Priority* on page 41-35 for available traffic types.
2. The IOP chip version on the CSM board where you are creating a virtual circuit. The IOP (Input Output Processor) chip is a cell routing engine on CSM boards. IOP1, the older chip version does not support Early Packet Discard (EPD) and Partial Packet Discard (PPD). IOP2, the newer chip version, supports EPD and PPD for UBR, VBR_NRT, and ABR traffic types. (See *CSMs with the IOP2 ASIC* on page 41-15 for a list of CSMs with the IOP2 ASIC.)

You can view AAL5 Discard configurations on a virtual circuit through the **vcc** command. The following describes the possible displays for the AAL5 Discard field:

- If an older chip version (IOP1) is installed, option 10 displays as follows for all **Transport Priority** values:

10) AAL5 Discard Continue {disable (0), enable (1)} : disabled

Enabling AAL5 Discard (which also enables “Partial Packet Discard”) increases overall frame throughput for AAL5 traffic during times of congestion. The default for this option is disabled.

- If a newer chip version (IOP2) is installed and UBR, VBR_NRT, or ABR is the **Transport Priority** traffic type entered in option 7, the screen displays as follows:

10) AAL5 Discard { Disable (0), EPD (1), PPD (2) } :EPD

Descriptions of these options are as follows:

◆ Important Note ◆

Policing (which is described in *Cell Loss Priority (CLP) and Policing* on page 41-14) will fail if Early Packet Discard (EPD) or Partial Packet Discard (PPD) is enabled. See *Policing and AAL5 Discarding* on page 41-15 to change the default setting for AAL5 discards on CSMs with the IOP2 ASIC from EPD to disabled.

Disable (0). Enter **0** to randomly discard cells associated with AAL5 PDU during congestion conditions. Cells are marked when the GCRA contract is violated.

EPD (1). Enter **1** to enable EPD (Early Packet Discard). EPD allows the switch to selectively discard cells associated with AAL5 PDU during congestion conditions. In this mode, the cells of the whole packet are either passed or discarded. At congestion time, if the first cell of a packet has already passed, then the rest of the packet will be passed. When congestion ends, the first cell of a new packet will be passed. Cells are marked when the GCRA contract has been violated.

PPD (2). Enter **2** to enable PPD (Partial Packet Discard). PPD allows the switch to selectively discard cells associated with AAL5 PDU during congestion conditions. In this mode, the cells of the rest of the packet—except for the very last cell—are discarded. When congestion ends, the first cell of a new packet will be passed. Cells are marked when the GCRA contract is violated.

- If a newer chip version (IOP2) is installed and VBR_RT, CBR, or CBR_PRS is the **Transport Priority** traffic type entered in option 7, the screen displays as follows:

10) AAL5 Discard : Disabled

CBR, CBR_PRS, and VBR_RT traffic types do not carry AAL5 PDU cells and are therefore not configurable for AAL5 Discard. The **AAL5 Discard** option for these traffic types remains at the default value of **disabled**.

11) Traffic Parameters

This option enters a screen of suboptions for configuring traffic descriptors and Quality of Service parameters. This screen and its options are described later in *Configuring Traffic Parameters* on page 41-40.

13) Advanced Parameters

This option enters a screen of suboptions for configuring the priority level for this circuit and for controlling statistics output. This screen and its options are described later in *Configuring Statistics and Priority Parameters* on page 41-45.

Configuring Point-to-Multipoint Virtual Circuits

While configuring a virtual circuit through the **cvc** command, you can configure multicast circuits to be associated with the primary circuit. Multicast circuits are leaves of the root virtual circuit and inherit its traffic properties. Cells on the root circuit are copied to all leaf circuits you specify. See *Point-to-Multipoint Virtual Circuits* on page 41-6 for descriptive information on point-to-multipoint connections.

Option 8 in the **cvc** command allows you to set up point-to-multipoint virtual circuits. Follow these steps:

1. At the bottom of the main **cvc** screen, you will find the following prompt.

Enter (option=value/save/cancel) :

Enter **8=1** at this prompt to enable multicast support on this virtual circuit. The **cvc** screen re-displays with an additional option under the **Multicast Enable** option, as follows.

Enter (option=value/save/cancel) : 8=1

Slot 5 Port 1 Connection VPI 2 VCI 100 Configuration

Available bandwidth: Tx=353209 Rx=353209

```

1) Description (30 chars max)      : Connection 100
2) Outgoing Slot (1-9)             : 5
3) Outgoing Port (1-64)           : 1
4) Outgoing VPI (1-0015)          : 2
5) Outgoing VCI (1-0255)          : 100

6) Channel Type { vc-nni(3), vc-uni(4) }      : VC-UNI
7) Transport Priority { CBR(1), CBR_PRS(2), VBR_RT(3), VBR_NRT(4), ABR(5), UBR(6) } : CBR
8) Multicast Enable { disable(0), enable(1) } : enable
   20) Add/Delete Multicast { add(1), delete(2) }
      Slot Port VPI VCI   Slot Port VPI VCI
      -----
10) AAL5 Discard Continue { disable(0), enable(1) } : disable

11) Traffic Parameters
13) Advanced Parameters

```

Enter (option=value/save/cancel) :

2. Enter **20=1** at the **Enter** prompt to add a virtual circuit. When adding leaves to the root, define the branching point on the switch closest to the leaves so as to maximize network resources.
3. The following prompt displays:

Enter (slot/port/vpi/vci) to add :

Enter the slot, port, VPI, and VCI (if applicable) for this leaf virtual circuit. Separate each identifier with a slash and do not include a space between any of the identifiers. For example, to create a leaf virtual circuit with a VPI of 2 and a VCI of 200 on port 1 of the module in slot 5, you would enter:

5/1/2/200

- Press <Enter>. The **cvc** screen re-displays with information on the virtual circuit you just added. The following shows a sample of what you may see:

```

8) Multicast Enable { disable(0), enable(1) }           : enable
20) Add/Delete Multicast { add(1), delete(2) }
   Slot Port VPI VCI   Slot Port VPI VCI
   -----
   5   1   8   7
  
```

- Continue adding multicast connections by repeating steps 2 through 4. The maximum number of multicast circuits is 8000 per CSM-155 module and 16,000 per CSM-622 module.

◆ Note ◆

You can improve the performance of point-to-multi-point connections on OC-3 modules with intelligent multicast replication, which is described in Chapter 42, “Advanced CSM Management.”

Configuring Traffic Parameters

The **cvc** command contains a sub-option for configuring traffic parameters, such as traffic descriptors and Quality of Service (QoS) parameters. Option 11 on the main **cvc** screen provides the link to this submenu. Enter **11** at the **Enter** prompt at the bottom of the main **cvc** screen and you will see the following screen of sub-options:

Slot 5 Port 1 Connection VPI 2 VCI 200 Configuration

Available bandwidth: Tx=353208 Rx=353208

- 1) Requested Tx QoS Class { Unspecified(0), Class1(1), Class2(2), Class3(3), Class4(4)} : Unspecified
- 2) Requested TX Best Effort { False (1), True (2) } : True
- 3) Requested Tx Traffic Descriptor Type { None(1), NoCLP NoSCR(2), CLPNoTagNoSCR(3), CLPNoTagNoSCR(4), NoCLPSCR(5), CLPNoTagSCR(6), CLPNoTagSCR(7) } : NoCLP NoSCR
- 20) Peak Cell Rate (cells/sec) for CLP=0+1 : 353208
- 4) Requested Rx QoS Class : Unspecified
- 5) Requested RX Best Effort { False (1), True (2) } : True
- 6) Requested Rx Traffic Descriptor Type : NoCLP NoSCR
- 30) Peak Cell Rate (cells/sec) for CLP=0+1 : 353208
- 7) Bi-directional Traffic Params { Off (1), On (2) } : On

Enter (option=value/save/cancel) :

The following sections describe the options on this screen.

1) Requested Tx QoS Class

The Quality of Service (QoS) for cells transmitted (from source to destination) on this VPI or VPI/VCI. The QoS can be Unspecified (0), Class 1 (1), Class 2 (2), Class 3 (3), or Class 4 (4). Each of these five classes is described in *Quality of Service (QoS)* on page 41-10 and they are listed below. The QoS Class that you select affects the priority of this Virtual Circuit and the Generic Cell Rate Algorithm (GCRA) used to police traffic. See *The ATM Menu* on page 41-26 for more information on the interaction of QoS and GCRA.

- Unspecified** Best Effort for data traffic (UBR)
- Class 1** Circuit Emulation, Constant Bit Rate Traffic (CBR)
- Class 2** Variable Bit Rate for Real Time Audio and Video Traffic (rt-VBR)
- Class 3** VBR for Connection-Oriented Protocols Such as Frame Relay (nrt-VBR)
- Class 4** Available Bit Rate for Connectionless Data Protocols Such as IP (ABR)

2) Requested Tx Best Effort

Indicates whether to use the Peak Cell Rate (PCR) setting—specified later in this procedure—to determine the amount of bandwidth allocated or to use all available bandwidth. Setting this field to **True** specifies this circuit to use all available bandwidth. Setting this field to **False** specifies the circuit to use the PCR to determine the amount of bandwidth; if bandwidth is not available to support the PCR then this connection will be disabled.

3) Requested Tx Traffic Descriptor Type

The traffic descriptor bundle to be used with this Class of Service. The traffic descriptor bundle you choose here determines which traffic parameters you will specify. The traffic parameters will include the Peak Cell Rate (PCR) and may also include the Sustained Cell Rate (SCR) and Maximum Burst Size (MBS). Each traffic descriptor bundle available is described in *Traffic Contract Descriptors* on page 41-16.

The traffic descriptor along with the Class of Service you choose determines the Generic Cell Rate Algorithm (GCRA), or “leaky bucket,” that will be used to police this connection. See *The ATM Menu* on page 41-26 for more information on the relationship between Class of Service, traffic descriptors, and GCRA. The following traffic descriptor bundles and prompts are available:

None No traffic enforcement imposed. No prompts for any traffic parameters.

NoCLPNoSCR Prompts for the Peak Cell Rate (PCR). Option 20 will display as follows:

```
3) Requested Tx Traffic Descriptor Type { None (1),           : NoCLP NoSCR
    NoCLPNoSCR (2), CLPNoTagNoSCR (3) CLPtagNoSCR (4),
    NoCLPSCR (5), CLPNo tagSCR (6), CLPtagSCR (7) }
20) Peak Cell Rate (cells/sec) for CLP=0+1                 : 3
```

The PCR will be checked on the aggregate of CLP=0 and CLP=1 traffic. Both the minimum and default setting for PCR is 3 cells per second.

CLPNoTagNoSCR Prompts for the Peak Cell Rate (PCR). Options 20 and 21 will display as follows:

```
3) Requested Tx Traffic Descriptor Type { None (1),           : CLP NoTag
NoSCR
    NoCLPNoSCR (2), CLPNoTagNoSCR (3) CLPtagNoSCR (4),
    NoCLPSCR (5), CLPNo tagSCR (6), CLPtagSCR (7) }
20) Peak Cell Rate (cells/sec) for CLP=0+1                 : 3
21) Peak Cell Rate (cells/sec) for CLP=0                   : 3
```

The PCR will be checked on the aggregate of CLP=0 and CLP=1 (CLP=0+1) traffic and separately on CLP=0 traffic. The default setting for PCR on CLP=0+1 traffic is 3 cells per second. The default setting for PCR on CLP=0 traffic is 3 cells per second.

CLPtagNoSCR Prompts for the Peak Cell Rate (PCR). Options 20 and 21 will display as follows:

```
3) Requested Tx Traffic Descriptor Type { None (1),           : CLP_Tag_NoSCR
    NoCLPNoSCR (2), CLPNoTagNoSCR (3) CLPtagNoSCR (4),
    NoCLPSCR (5), CLPNo tagSCR (6), CLPtagSCR (7) }
20) Peak Cell Rate (cells/sec) for CLP=0+1                 : 3
21) Peak Cell Rate (cells/sec) for CLP=0                   : 3
```

The PCR will be checked on the aggregate of CLP=0 and CLP=1 (CLP=0+1) traffic and separately on CLP=0 traffic. The default setting for PCR on CLP=0+1 traffic is 3 cells per second. The default setting for PCR on CLP=0 traffic is 3 cells per second.

NoCLPSCR Prompts for the Peak Cell Rate (PCR), Sustained Cell Rate (SCR), and Maximum Burst Size (MBS). Options 20, 21, and 22 displays as follows:

```
3) Requested Tx Traffic Descriptor Type { None (1),           : NoCLP SCR
    NoCLPNoSCR (2), CLPNoTagNoSCR (3) CLPTagNoSCR (4),
    NoCLPSCR (5), CLPNo tagSCR (6), CLPTagSCR (7) }
20) Peak Cell Rate (cells/sec) for CLP=0+1                 : 3
21) Sustaining Cell Rate (cells/sec) for CLP=0+1           : 2
22) Maximum Burst Size                                     : 1
```

The PCR will be checked on the aggregate of CLP=0 and CLP=1 (CLP=0+1) traffic. The default setting for PCR is 3 cells per second. The SCR will be checked on the aggregate of CLP=0 and CLP=1 traffic. Both the minimum value and the default setting for SCR is 2 cells per second. SCR must be less than PCR. The MBS will be checked on the aggregate of CLP=0+1 traffic. The MBS default setting is 1 cell.

CLPNoTagSCR Prompts for the Peak Cell Rate (PCR), Sustained Cell Rate (SCR), and Maximum Burst Size (MBS). Options 20, 21, and 22 will display as follows:

```
3) Requested Tx Traffic Descriptor Type { None (1),           : CLP NoTag SCR
    NoCLPNoSCR (2), CLPNoTagNoSCR (3) CLPTagNoSCR (4),
    NoCLPSCR (5), CLPNo tagSCR (6), CLPTagSCR (7) }
20) Peak Cell Rate (cells/sec) for CLP=0+1                 : 3
21) Sustaining Cell Rate (cells/sec) for CLP=0             : 2
22) Maximum Burst Size (cells) for CLP=0                   : 1
```

The PCR will be checked on the aggregate of CLP=0 and CLP=1 (CLP=0+1) traffic. The default setting for PCR is 3 cells per second. The SCR will be checked on CLP=0 traffic. The default setting for SCR is 2 cells per second. The MBS will be checked on CLP=0 traffic; the MBS default setting is 1 cell.

CLPTagSCR Prompts for the Peak Cell Rate (PCR), Sustained Cell Rate (SCR), and Maximum Burst Size (MBS).

```
3) Requested Tx Traffic Descriptor Type { None (1),           : CLP Tag SCR
    NoCLPNoSCR (2), CLPNoTagNoSCR (3) CLPTagNoSCR (4),
    NoCLPSCR (5), CLPNo tagSCR (6), CLPTagSCR (7) }
20) Peak Cell Rate (cells/sec) for CLP=0+1                 : 3
21) Sustaining Cell Rate (cells/sec) for CLP=0             : 2
22) Maximum Burst Size (cells) for CLP=0                   : 1
```

The PCR will be checked on the aggregate of CLP=0 and CLP=1 (CLP=0+1) traffic. The default setting for PCR is 3 cells per second. The SCR will be checked on CLP=0 traffic. The default setting for SCR is 2 cells per second. The MBS will be checked on CLP=0 traffic. The MBS default setting is 1 cell.

The following sections describe the traffic parameter prompts that display after you select a traffic descriptor bundle.

Peak Cell Rate

The following is a sample prompt display:

20) Peak Cell Rate (cells/sec) for CLP=0+1 : 3

In this field, you specify the Peak Cell Rate (PCR), in cells per second allowed on this VPI or VPI/VCI. The PCR is the fastest cell rate allowed on the connection. The switch will use this parameter as part of the traffic contract for this virtual circuit. A cell rate above the rate you indicate here will denote a violation of the traffic contract and the leaky bucket algorithm will determine which enforcement action to take. Note that the PCR will be enforced on CLP=0+1 or CLP=0 cell flows; this prompt will indicate which cell flow is checked.

Sustaining Cell Rate

The following is a sample prompt display:

21) Sustaining Cell Rate (cells/sec) for CLP=0+1 : 2

In this field, you specify the Sustaining Cell Rate (SCR), in cells per second allowed on this VPI or VPI/VCI. The SCR is highest average cell rate allowed on the circuit. The switch will use the parameter as part of the traffic contract for this virtual circuit. An average cell rate above the rate you indicate here will denote a violation of the traffic contract and the leaky bucket algorithm will determine which enforcement action to take. Note that the SCR will be enforced on CLP=0+1 or CLP=0 cell flows; this prompt indicates which cell flow is checked.

Maximum Burst Rate

The following is a sample prompt display:

22) Maximum Burst Rate (cells) for CLP=0+1 : 1

In this field, you specify the Maximum Burst Size (MBS), in cells allowed on this VPI or VPI/VCI. The MBS is the largest single burst of cells allowed on the connection. The switch will use this parameter as part of the traffic contract for this virtual circuit. A burst size above the value you indicate here will denote a violation of the traffic contract and the leaky bucket algorithm will determine which enforcement action to take. Note that the MBS will be enforced on CLP=0+1 or CLP=0 cell flows; this prompt indicates which cell flow is checked.

4) Requested Rx QoS Class

The Quality of Service (QoS) for cells received from the destination at the source on this VPI or VPI/VCI. The QoS can be Unspecified (0), Class 1 (1), Class 2 (2), Class 3 (3), or Class 4 (4). Each of these five classes is described in *Quality of Service (QoS)* on page 41-10 and they are listed below. The QoS Class that you select affects the priority of this Virtual Circuit and the Generic Cell Rate Algorithm (GCRA) used to police traffic. See *The ATM Menu* on page 41-26 for more information on the interaction of QoS and GCRA.

Unspecified	Best Effort for data traffic (UBR)
Class 1	Circuit Emulation, Constant Bit Rate Traffic (CBR)
Class 2	Variable Bit Rate for Audio and Video Traffic (rt-VBR)
Class 3	VBR for Connection-Oriented Protocols Such as Frame Relay (nrt-VBR)
Class 4	Available Bit Rate for Connectionless Data Protocols Such as IP (ABR)

5) Requested Rx Best Effort

Indicates whether to use the Peak Cell Rate (PCR) setting—specified later in this procedure—to determine the amount of bandwidth allocated or to use all available bandwidth. Setting this field to **True** specifies this circuit to use all available bandwidth. Setting this field to **False** specifies the circuit to use the PCR to determine the amount of bandwidth; if bandwidth is not available to support the PCR then this connection will be disabled.

6) Requested Rx Traffic Descriptor Type

The traffic descriptor bundle to be used with this Class of Service. The traffic descriptor bundle you choose here determines which traffic parameters you will specify. The traffic parameters will include the Peak Cell Rate (PCR) and may also include the Sustained Cell Rate (SCR) and Maximum Burst Size (MBS). Each traffic descriptor bundle available is described in *Traffic Contract Descriptors* on page 41-16. In addition, please refer to 3) *Requested Tx Traffic Descriptor Type* on page 41-41 for information on the traffic descriptor options included in this software option.

7) Bi-directional Traffic Params

Indicates whether you want to use the same traffic parameters for the transmit and receive sides of this virtual circuit. If you enter a **Yes** in this field then the Tx traffic parameters (fields 1 to 3) will match the Rx traffic parameters (fields 4 to 6).

Configuring Statistics and Priority Parameters

The **cvc** command contains a sub-option for configuring the Priority level and the statistics that display for this connection. Option 13 on the main **cvc** screen provides the link to this submenu. Enter **13** at the **Enter** prompt at the bottom of the main **cvc** screen and you will see the following screen of sub-options:

```

Slot 5 Port 1 Connection VPI 2 VCI 200 Configuration
    Available bandwidth: Tx=353209 Rx=353209
    1) User Priority (0-15)                : 4
    2) CDV (10us-10000us)                : 1000
    
```

Enter (option=value/save/cancel) :

The options in this screen are described below.

User Priority

The priority level assigned to this virtual circuit. This priority is used to decide which virtual circuit's traffic is discarded first in a situation where congestion occurs. The priority level for a virtual circuit can range from 0 to 15, with 0 being the highest priority and 15 being the lowest. A default value is supplied for User Priority based on the type of traffic you specified under the **Traffic Priority** option on the main **cvc** screen (Option 7). The following defaults are supplied for each traffic type:

Traffic Type and Priority

Traffic Type	Default Priority Level
CBR	4
VBR	8
ABR	8
UBR	15

You can fine tune these priorities through this option. For example, some CBR circuits can be given higher priority than other CBR circuits by assigning a User Priority of 1, 2, or 3 rather than CBR default of 4.

CDV

Cell Delay Variation in microseconds. Also referred to as "jitter," this value is the change that occurs in cell spacing from the time cells leave one node and arrive at another node.

Configuring a Cell Switch for Switched Virtual Circuits (SVCs)

Follow the steps below to configure an OmniSwitch with CSMs for Switched Virtual Circuits (SVCs).

◆ Important Note ◆

If your ATM edge devices use UNI Signaling version 4.0, you must use the image files for Multiple-Peer Group (MPG) PNNI (**cell_mpg.img**, **sonet.img** and **asm_mpg.img** on an MPM-1G or MPM-III, or **cell_mpg.img**, **sonet.img** and **asmc_mpg.img** on an MPM-C.) See Chapter 46, “Configuring and Managing PNNI,” for more information on MPG PNNI.

1. Enter **map** followed by the slot number of the CSM port, a slash (*/*), and the port number of the CSM port. For example, to configure CSM Port 3 in Slot 3, enter

```
map 3/3
```

at the system prompt. A screen similar to the following will be displayed.

Slot 3 Port 3 Configuration

```
1) Description (30 chars max)      : CSM PORT
2) ESI (12 hex-chars)              : 000000000000
   NetPrefix (3903488001bc900001017dee30)
3) Max VPI bits (1..11)            : 2
4) Max VCI bits (1..11)            : 10
5) I/F Type { Pub UNI (1), Priv UNI (2),
   PNNI (3), IISP netw (4),
   IISP user (5)                    : Private
6) Phy Protocol {SONET (1), SDH (2): SONET
7) Signaling Ver
   {3.0 (1), 3.1 (2), 4.0 (3) }      : 3.1
8) ILMI Enable { False (1), True (2) } : True
80) CSM Port Auto Cfg
   { Enable (1), Disable (2) } : Enable
81) ILMI Polling {Off (1), On (2) } : On
9) Timing Mode {Local (1), Loop (2) } : Local
90) Local { Osc (1), Bus (2) }      : Osc
14) Signaling Status (Disable (1)
   Enable (2)                        : Enable
15) Phy Loopback {none (0), diag (1),
   line (2) }                        : None
16) Bandwidth Overbooking Factor
   {0.0=Disable CAC;
   1.0=No Over Booking (default);
   Valid: >= 0.0}                   : 1.0
```

Enter (option=value/save/cancel) :

2. Enter any necessary changes to the port's configuration. When you are finished, enter

```
save
```

at the **map** command prompt.

A screen similar to the following will be displayed.

```
Slot 2 Port 1 Configuration
1) Description (30 chars max)      : CSM PORT
2) ESI (12 hex-chars)             : 000000000000
   NetPrefix (3903488001bc900001017dee30)
3) Max VPI bits (1..11)           : 2
4) Max VCI bits (1..11)           : 10
5) I/F Type { Pub UNI (1), Priv UNI (2),
   PNNI (3), IISP netw (4),
   IISP user (5)                   : Private
6) Phy Protocol {SONET (1), SDH (2): SONET
7) Signaling Ver
   {3.0 (1), 3.1 (2), 4.0 (3)}     : 3.1
8) ILMI Enable { False (1), True (2) } : True
80) CSM Port Auto Cfg
   { Enable (1), Disable (2) }     : Enable
81) ILMI Polling {Off (1), On (2) } : On
9) Timing Mode {Local (1), Loop (2) } : Local
90) Local { Osc (1), Bus (2) }     : Osc
14) Signaling Status (Disable (1)
   Enable (2)                       : Enable
```

Enter (option=value/save/cancel) :

7. Enter

```
14=2
```

at the **map** command prompt.

8. Enter any necessary changes to the internal port's configuration. When you are finished, enter

```
save
```

at the **map** command prompt.

9. You must now configure a route property, or template, that describes route characteristics with the **prpadd** command. (See Chapter 47, "Managing IISP and PNNI Routes," for more information on the **prpadd** command.) The syntax for this command is as follows.

```
prpadd <slot>/<port>/[<virtual tunnel instance>]
```

(The **<virtual tunnel instance>** option is a unique value assigned to each virtual tunnel on a CSM module port.) For example, to set up a static route property on CSM Port 3 in Slot 3, enter

```
prpadd 3/3
```

at the system prompt.

A screen similar to the following will be displayed.

Route Property Configuration for Slot 3 Port 3

- 1) Internal or exterior (i or e) [i]: Unspecified
- 2) Scope (1-104) [80]: Unspecified
- 3) VP Capable (t or f) [t]: Unspecified
- 4) VPI : Unspecified
- 5) E.164 Address : Unspecified

6) Topology State Parameter Configuration Menu

7) Associated Transit Network Configuration Menu

To configure a parameter, type "item = value" (as in 1=i)
 To quit out of configuration, type "quit"
 To save the configured info, type "save"

->

10. You must now add route addresses to one of the pre-configured route properties with the **pradd** command. (See Chapter 47, "Managing IISP and PNNI Routes," for more information on the **pradd** command.) The syntax for this command is as follows.

pradd <slot>/<port>[/<virtual tunnel instance>]

(The **<virtual tunnel instance>** option is a unique value assigned to each virtual tunnel on a CSM module port.) For example, to add route address to the route properties you configured in Step 6, follow Steps **a** through **e** on the following page.

- a.** To add route addresses to CSM Port 3 in Slot 3, for example, enter

pradd 3/3

at the system prompt. A screen similar to the following will be displayed.

Currently there are 3 route configurations for this port as follows:

Rt	Slot/ Port	Int/ Ext	Scope	Admin Weight Metrics		# Route Prefixes	
1	3/3	Int	104	CBR	In:5000	Out:0	0
				rtVBR	In:0	Out:2000	
				nrtVBR	In:0	Out:0	
				ABR	In:0	Out:0	
				UBR	In:0	Out:0	

Do you wish to add to this property? (y)

- b.** Enter a **y** at this prompt to begin adding route addresses. If more than one route property exists, then you will be prompted to enter the route number for which you want to add addresses. Route numbers are listed in the left-most column of the table.

The following prompt displays:

1) Number of routes (0-20) : Unspecified

To configure a parameter, type "item = value" (as in 1=2)
 To abort out of configuration, type "quit"
 To return to the route property parameters menu, type "return"

->

- c.** Enter the number of address you to configure for this static route property by entering a **1**, an equal sign (=) and then the number of addresses to add. Up to 20 route prefixes may be added to a route property.

Configuring a Cell Switch for Switched Virtual Circuits (SVCs)

For example, to specify two (2) addresses for this static route property, enter

1=2

at the prompt. A screen similar to the following will be displayed.

```
Route Address Configuration for Routes on Slot 3 Port 3:
1) Number of routes (0-20)                : 2
   Address Prefix (a)                      Prefix bit-length (b)
=====
2)                                         0
3)                                         0

To configure a parameter, type "item = value" (as in 1=2)
To quit out of configuration, type "quit"
To save the configuration, type "save"
```

- d.** Enter parameters for the first address. Start each specification with a **2**, followed by the letter of the parameter (**a** or **b**), an equal sign (=), and then the value of the parameter. For example, to enter an address prefix of **1** and an Length of **75**, you would enter:

-> 2a=4700040006345623000047000400063456230000, 2b=75

Be sure to separate each parameter specification by a comma (,).

- e.** Repeat Step **d** for other addresses you want to add. The second address specification should start with a 3, the third address starts with a 4, and so on.
- f.** Enter

save

at the **pradd** prompt to save your settings.

Configuring VP Switching

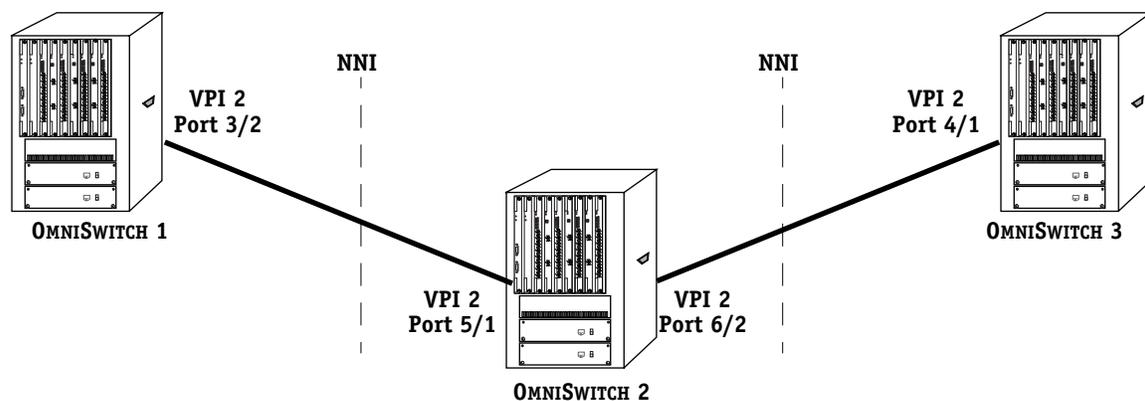
You can set up virtual path (VP) switching on an OmniSwitch with the **cvc** command by configuring separate incoming and outgoing ports. In addition, you can set up a VP with incoming and outgoing ports on separate switching modules.

You can configure VP switching on any CSM module. For example, you can configure an incoming port on a CSM-AB-IMA submodule and an outgoing port on a CSM-155 module. However, you *cannot* configure VP switching on an ATM access module.

◆ Note ◆

When configuring VP switching, you need to consider the range of VPIs supported by the CSM ports used. For example, if one CSM port supports VPIs 0 to 2 and the other CSM port supports VPIs 0 to 4, then you must use only VPIs 0 to 2.

As shown in the figure below, OmniSwitch 2 has been configured for VP switching. CSM port 5/1 on OmniSwitch 2 has been configured as the incoming port and CSM port 6/2 has been configured as the outgoing port.



VP Switching on an NNI Connection

Follow the steps below to configure a switch for VP switching.

1. Enter **cvc** followed by the slot number of the incoming port, a slash (/), the port number of the incoming port, and the VPI number. For example, to configure VP switching on incoming VPI No. 2 on Slot 5, Port 1, enter

```
cvc 5/1 2
```

A screen similar to the following will be displayed.

Slot 5 Port 1 Connection VPI 2 VCI 100 Configuration

Available bandwidth: Tx=353209 Rx=353209

- 1) Description (30 chars max) : Connection 100
- 2) Outgoing Slot (1-9) : 5
- 3) Outgoing Port (1-08) : 1
- 4) Outgoing VPI (1-0015) : 2
- 5) Outgoing VCI (1-0255) : 100

- 6) Channel Type { vc-nni(3), vc-uni(4) } : VC-UNI
- 7) Transport Priority { CBR(1), CBR_PRS(2), VBR_RT(3), VBR_NRT(4), ABR(5), UBR(6) } : UBR
- 8) Multicast Enable { disable(0), enable(1) } : disable
- 10) AAL5 Discard Continue { disable(0), enable(1) } : enable

- 11) Traffic Parameters
- 13) Advanced Parameters

Enter (option=value/save/cancel) :

2. Enter **2**, followed by **=**, and followed by the slot number to set the outgoing slot. For example, to set the outgoing slot to 6, enter

2=6

at the prompt.

3. Enter **3**, followed by **=**, and followed by the port number to set the outgoing port. For example, to set the outgoing port to 2, enter

3=2

at the prompt.

4. Enter **4**, followed by **=**, and followed by the VPI number to set the outgoing VPI. For example, to set the outgoing VPI to 2, enter

4=2

at the prompt.

5. Enter

6=2

at the prompt to set the channel type to NNI.

6. Enter

save

at the system prompt to save your settings.

Modifying a Virtual Circuit

You can modify any parameters for a virtual circuit that you previously configured. The **mvc** command enables you to modify a virtual circuit, including soft PVCs. It uses the same screens and allows you to change the same parameters as the **cvc** and **scvc** commands. Use of **mvc** is essentially the same as the corresponding configuration command (**cvc** or **scvc**).

To begin modifying a virtual circuit, enter **mvc** followed by the slot number, a slash (/), and the port number for the input virtual circuit. After the slot and port number, leave a space, then specify the Virtual Path Identifier (VPI), a slash (/), and then the Virtual Channel Identifier (VCI). (Do not include the VCI if you are modifying a Virtual Path only.) For example, the following command specifies to modify a virtual circuit with a VCI of 7 and a VPI of 6 on the first port on the module in slot 5:

```
mvc 5/1 6/7
```

For more information on the **mvc** screens and parameters, see *Creating a Permanent Virtual Circuit* on page 41-33 for PVCs and Chapter 42, "Advanced CSM Management" for soft PVCs.

Deleting a Virtual Circuit

You can delete a virtual circuit using the **dvc** command. When you delete the circuit, the VPI or VPI/VCI parameters are deleted and any reserved bandwidth is released.

To delete a virtual path or virtual channel enter **dvc** followed by the slot number of the CSM module where the circuit was set up, the physical port number for the circuit, and the VPI and/or VCI of the circuit. For example, if wanted to delete virtual channel 7 on virtual path 4 and port 1 of the CSM module in slot 5, you would enter:

```
dvc 5/1 4/7
```

Note that there is a space between the slot/port specification and the VPI/VCI specification. You can also specify to delete just a virtual path. In this case, you would simply leave out the VCI at the end of the command. For example, to delete Virtual Path 3 on port 1 on the CSM module in slot 5, you would enter:

```
dvc 5/1 3
```

Again note that there is a space between the slot/port numbers and the VPI.

After you specify to delete a circuit, you will receive a message asking you to confirm the deletion:

```
Remove CSM Slot 5 Port 1 Connection VPI 7 VCI 7 (n)? :
```

Stop the deletion by pressing **<Enter>** or entering **N** at this prompt. A message similar to the following displays:

```
CSM Slot 5 Port 1 Connection VPI 7 VCI 7 not removed
```

Confirm the deletion by entering a **Y** at the confirmation prompt. The VPI or VCI will be removed and a message similar to the following displays:

```
Removing CSM Slot 5 Port 1 Connection VPI 7 VCI 7, please wait...
```

```
CSM Slot 5 Port 1 Connection VPI 7 VCI 7 removed
```

CSM Port Auto Configuration

Auto configuration allows you to directly connect an X-Cell CSM port to another switch's ATM port without requiring manual configuration. When you enable auto configuration procedures on a specified port, the port automatically configures the interface type and signaling version of a connected peer port. User interface commands to configure and view CSM auto port configuration parameters are described in the sections that follow.

Modifying CSM Port Auto Configuration

The **mcac** command allows you to modify port auto configuration parameters on a single CSM port, a specified list of CSM ports, all ports on a single CSM board, or all CSM ports in an OmniSwitch chassis. To modify all CSM ports in a switch, enter the **mcac** command at the system prompt. A screen similar to the following displays:

CSM Port Auto Configuration Parameters

- 1) **CSM Auto Configuration { Enable (1), Disable (2) } : Enable**
- 2) **Trigger CSM Auto Configuration By
{ Physical Link Up(1), Logic Link Up(2), Both(3) } : Both**
- 3) **Default Interface Type { Pub UNI(1), Pri UNI(2),
PNNI(3), IISP netw(4), IISP user(5) } : Private UNI**
- 4) **Default Sig Version { 3.0(1), 3.1(2), 4.0 (3) } : 3.1**

Enter (option=value/save/cancel) :

You change a value in the field by entering the line number for the variable you want to change, an equal sign (=), and then the option number for the new value. For example, if you wanted to change the **Default Sig Version** field variable to 3.0, you would enter a 4 (the line number for **Default Sig Version**), an equal sign, and then the option number for the new value as follows:

4=1

When you are done entering all new values, type **save** at the colon prompt (:) and all new parameters will be saved. If you want to cancel your changes, enter **cancel**. The following sections describe the options you can alter through the **mcac** command.

CSM Auto Configuration

This option enables or disables auto configuration on the port(s) you are modifying. In Release 4.1 and later, the default for auto configuration is **disabled**; however, if you load new software on your switch, it will not disable auto configuration if it is already enabled.

◆ Note ◆

A redundant ATM uplink may be incorrectly configured if port auto configuration was initially enabled but then became disabled. If your primary ATM uplink goes down, then you should verify the ATM uplink's port configuration through the **vap** command.

Trigger CSM Auto Configuration By

This option sets up the conditions for triggering auto configuration procedures. Possible values are as follows:

Physical link up. Physical link up refers to the physical connectivity established with another port. Physical connectivity, indicated by a green light on the CSM link LED, occurs when the cable from another switch is plugged into the specific port or when a connected switch turns on. If you choose this option, auto configuration procedures will be triggered only once, after the physical link connectivity is established. ILMI trap messages from a peer port (i.e., a logical link up) will not trigger auto configuration.

Logical link up. Logical link up refers to the ILMI trap messages sent from a peer port. Trap messages are sent whenever a peer port changes its operating parameters or resets itself. Trap messages trigger ILMI auto configuration procedures in the peer port. The logical link up option will enable a port to dynamically adapt to the changes of its peer port. For example, if an ATM access port is connected to a CSM port and the user changes the ATM access port UNI version from 3.0 to 3.1, the CSM port will detect the change and automatically switch its UNI version to 3.1.

◆ Note ◆

Non-ILMI 4.0 implementation or vendor specific implementations might send out erroneous traps. In such cases, you may want to disable the logical link up in order to avoid de-stabilizing CSM ports.

Both. This is the default value for this option. If you choose this option, auto configuration procedures will be triggered in both Physical Link Up and Logical Link Up situations described above.

Default Interface Type

This option sets up the default interface type used on this port(s) if auto configuration procedures cannot determine the interface type. The default setting is private Network-to-Node Interface (PNNI), unless otherwise configured by the user. If auto configuration procedures cannot determine the interface type, the port(s) will support the default interface type specified in this menu.

◆ Important Note ◆

In Release 4.1 and later, changing the interface type will take place immediately after you save your changes. You do not need to reboot the switch.

Default Sig Version

This option sets up the default signaling version used on this port(s) if auto configuration procedures cannot determine the signaling version. The default setting is 3.1, unless otherwise configured by the user. If auto configuration procedures cannot determine the interface type, the port(s) will support the default signaling version specified in this menu.

◆ Important Note ◆

In Release 4.1 and later, changing the signaling version will take place immediately after you save your changes. You do not need to reboot the switch.

Modifying One or More CSM Boards

The **mcac** command allows you to modify port auto configuration information on one or more CSM boards. To modify port auto configuration information on a single board, you enter the **mcac** command along with the slot number for the CSM board, as follows:

```
mcac <slot>
```

where **<slot>** is the slot number where the CSM board is installed. For example, if you wanted to modify information on the board in slot 4, you would enter:

```
mcac 4
```

This specification allows you to modify all the ports on the board in slot 4. Additionally, if you wanted to modify port auto configuration information on more than one CSM board, you would enter the **mcac** command followed by a list of the slot numbers for which you want to view information as follows:

```
mcac <slot list>
```

where **<slot list>** is a list of the slots for the CSM boards on which you want to modify port auto configuration information. Use the **<slot>/<port>** format and separate the slot range with the tilde sign (~). For example, if you wanted to modify the boards in slots 3 through 5, you would enter:

```
mcac 3~5
```

This specification allows you to modify all the ports in boards 3 through 5. If you wanted to modify a list of non-consecutive slots, separate slot specifications with a comma, as follows:

```
mcac 3,5,7
```

You may use both syntaxes in your slot list, as follows:

```
mcac 3,5~7
```

Note that there are no spaces between slot specifications.

Modifying One or More Ports

The **mcac** command allows you to modify port auto configuration information on one or more CSM ports. To modify a single port, you enter the **mcac** command along with the slot number for the CSM board and the port number for which you want to receive information, as follows:

```
mcac <slot>/<port>
```

where **<slot>** is the slot number where the CSM board is installed and **<port>** is the port number on the CSM board. For example, if you wanted to modify information for port 1 on the CSM module in slot 4, you would enter:

```
mcac 4/1
```

Additionally, if you wanted to modify port auto configuration for more than one port, you would enter the **mcac** command followed by a list of the port numbers for which you want to modify, as follows:

```
mcac <port list>
```

where **<port list>** is a list of CSM ports on which you want to modify port auto configuration information. Use the **<slot>/<port>** format and separate the range of port specifications with the tilde sign (~). For example, if you wanted to modify ports 2 through 7 in slot 4, you would enter:

```
vcac 4/2~4/7
```

If the ports you modify are not all on the same CSM board, use the **<slot>/<port>** and separate port specifications with a comma. The following is an example of a port list specification of ports on different CSM boards:

```
vcac 3/1,3/7,4/3
```

Note that there are no spaces between port specifications.

You may also view information on the specific instance number for a single port on a CSM board by entering:

```
mcac <slot>/<port> <instance>
```

where **<slot>** is the slot number where the CSM board is installed, **<port>** is the port number on the CSM board, and **<instance>** is the instance number of the port. Note that there is a space separating **<slot>/<port>** and instance number. For example, if you wanted to view basic information for instance 2 on port 1, in slot 3, you would enter:

```
mcac 3/1 2
```

Viewing CSM Port Auto Configuration

The **vcac** command allows you to view auto configuration information on a single CSM port, a specified list of CSM ports, all ports on a single CSM board, or all CSM ports in an OmniSwitch chassis. To view all CSM ports in a switch, enter the **vcac** command at the system prompt. The following is a sample display.

ATM Port Table

Abs Port	Slot	Port	Inst	Enable Auto Cfg	Trigger Auto Cfg	Current I/F Type	Current Sig Ver	Default I/F Type	Default Sig Ver
64	2	1	0	Enabled	Phy&Logic	Pri UNI	UNI3.0	Pri UNI	UNI3.1
72	2	2	0	Enabled	Phy&Logic	Pri UNI	UNI3.0	Pri UNI	UNI3.1
192	4	1	0	Enabled	Phy&Logic	PNNI	----	Pri UNI	UNI3.1
200	4	2	0	Disabled	Phy&Logic	Pri UNI	UNI3.0	Pri UNI	UNI3.1
208	4	3	0	Enabled	Phy&Logic	Pri UNI	UNI3.0	Pri UNI	UNI3.1
216	4	4	0	Enabled	Phy&Logic	Pri UNI	UNI3.0	Pri UNI	UNI3.1
224	4	5	0	Enabled	Phy&Logic	Pri UNI	UNI3.0	Pri UNI	UNI3.1
232	4	6	0	Enabled	Phy&Logic	Pri UNI	UNI3.0	Pri UNI	UNI3.1
240	4	7	0	Enabled	Phy&Logic	Pri UNI	UNI3.0	Pri UNI	UNI3.1
248	4	8	0	Enabled	Phy&Logic	Pri UNI	UNI3.0	Pri UNI	UNI3.1

Abs Port	Auto Cfg	Peer UNI Typ	Peer Dev Typ	Peer Uni Ver	Peer NNI Sig	Peer ILMI Ver
64	Cfg Done	Private	User	UNI3.0	Unsupported	ILMI4.0
72	Idle	n/a	n/a	n/a	n/a	n/a
192	Idle	n/a	n/a	n/a	n/a	n/a
200	Idle	n/a	n/a	n/a	n/a	n/a
208	Idle	n/a	n/a	n/a	n/a	n/a
216	Idle	n/a	n/a	n/a	n/a	n/a
224	Idle	n/a	n/a	n/a	n/a	n/a
232	Idle	n/a	n/a	n/a	n/a	n/a
240	Idle	n/a	n/a	n/a	n/a	n/a
248	Idle	n/a	n/a	n/a	n/a	n/a

Abs Port. An internal port assignment used by CSM software to identify ports. You might use this number for the sake of comparison when viewing displays for PNNI-specific commands, which are found in the PNNI sub-menu. Additionally, the absolute port number may be used for tracing auto configuration debugging messages.

Slot/Port. Indicates the CSM module and the port for which auto configuration is provided. Each row in the table gives information for a single CSM port.

Inst. Indicates the instance of the virtual UNI/NNI on this particular CSM port. A physical CSM port has an instance of zero. Any virtual ports configured through VP tunneling will have an instance that is greater than zero.

Enable Auto Cfg. Indicates whether or not you want to enable auto configuration on this port.

Trigger Auto Cfg. Indicates whether auto configuration of this port is triggered by a physical link up, a logical link up, or both. Physical link up refers to the physical layer connection established by a plugged in cable or a switch re-boot. Logical link up refers to situations such as a peer port re-setting or logical link connectivity (ILMI) being re-established. A logical link connection is indicated by an ILMI trap message from a peer port. The physical connection should always be up during a logical link up.

Current I/F Type. Specifies the type of ATM interface that this port supports. The options are described below:

Pub UNI Public UNI. This port will be used for connections to public ATM service carrier switches, such as those used by Telcos.

Priv UNI Private UNI. This port is used for private UNI uplinks. Such a port would connect either directly to an ATM workstation, LAN switch, or ATM attached router.

PNNI 1.0 Private Network-to-Network Interface (PNNI). The port will support PNNI version 1.0 ATM routing, which includes support for a single-peer group mapping.

◆ **Important Note** ◆

If your software version is prior to 4.1, then you *must* reboot the switch when you change the **I/F Type** from **PNNI 1.0** to **Pub UNI**.

IISP Interim Interswitch Signaling Protocol. Typically an IISP port would be part of an intermediate ATM node that did not support the PNNI routing protocol. It is used primarily for establishing static routes using the IISP protocol. See Chapter 47, “Managing IISP and PNNI Static Routes” for further information.

◆ **Important Note** ◆

If you want to configure and connect two IISP ports having PNNI and ILMI 4.0 capabilities, you must disable CSM port auto configuration and manually configure the ports instead. According to the ATM Forum ILMI 4.0, the two IISP ports will configure themselves as PNNI if you do not disable port auto configuration in this instance,. For more information, see Chapter 47, “Managing IISP and PNNI Static Routes.”

Current Sig Ver. The version of the User-to-Network Interface (UNI) used on this port. OmniSwitch is compliant with ATM Forum UNI specifications versions 3.0 and 3.1. If you have installed the software for multiple peer group PNNI, then you can also set the signalling version to 4.0. You select which version your ATM network supports.

Default I/F Type. Specifies the default type of ATM interface that this port supports if auto configuration procedures cannot determine the interface type. The default setting is private Network-to-Node Interface (PNNI), unless otherwise configured by the user.

Default Sig Ver. The default version used on this port if auto configuration procedures cannot determine the signaling version. The default setting is private User-to-Network Interface (pri UNI) 3.1, unless otherwise configured by the user.

Auto Cfg Status. Indicates the status of auto configuration on this port. An **Idle** status means that auto configuration on this port is not active. A **Done** status means that auto configuration procedures on this port have completed. An **In progress** status means that auto configuration is currently running.

Peer UNI Typ. The type of the ATM User-to-Network Interface (UNI) used on the peer port. The two possible types are private and public.

Peer Dev Typ. The type of device used on the peer port. The two possible device types are User or Network.

Peer UNI Ver. The version of the ATM User-to-Network Interface used on the peer port. The version number corresponds to the ATM Forum Specification with which this UNI implementation complies. The OmniSwitch is compliant with UNI versions 3.0 and 3.1. If you have installed the software for multiple peer group PNNI, then you can configure CSM modules for UNI signalling specification 4.0.

Peer NNI Sig. The version of the Network-to-Network interface (NNI) used on the peer port.

Peer ILMI Ver. The version (4.0) of the Integrated Local Management Interface (ILMI) used on the peer port.

Information on the Ports for One or More CSM Boards

To view **vcac** port auto configuration information on one or more CSM boards, you enter the **vcac** command along with the slot number for the CSM board, as follows:

vcac <slot>

where **<slot>** is the slot number where the CSM board is installed. For example, if you wanted to view information on the board in slot 4, you would enter:

vcac 4

This command displays a screen similar to the following:

Abs Port	Slot	Port	Inst	Enable Auto Cfg	Trigger Auto Cfg	Current I/F Type	Current Sig Ver	Default I/F Type	Default Sig Ver
192	4	1	0	Enabled	Phy&Logic	PNNI	---	Pri UNI	UNI3.1
200	4	2	0	Disabled	Phy&Logic	Pri Uni	Uni3.0	Pri Uni	UNI 3.1
208	4	3	0	Disabled	Phy&Logic	Pri Uni	Uni3.0	Pri Uni	UNI 3.1
216	4	4	0	Disabled	Phy&Logic	Pri Uni	Uni3.0	Pri Uni	UNI 3.1
224	4	5	0	Disabled	Phy&Logic	Pri Uni	Uni3.0	Pri Uni	UNI 3.1
232	4	6	0	Disabled	Phy&Logic	Pri Uni	Uni3.0	Pri Uni	UNI 3.1
240	4	7	0	Disabled	Phy&Logic	Pri Uni	Uni3.0	Pri Uni	UNI 3.1
248	4	8	0	Disabled	Phy&Logic	Pri Uni	Uni3.0	Pri Uni	UNI 3.1

Abs Port	Auto Cfg Status	Peer UNI Typ	Peer Dev Typ	Peer Uni Ver	Peer NNI Sig	Peer ILMI Ver
192	Idle	n/a	n/a	n/a	n/a	n/a
200	Idle	n/a	n/a	n/a	n/a	n/a
208	Idle	n/a	n/a	n/a	n/a	n/a
216	Idle	n/a	n/a	n/a	n/a	n/a
224	Idle	n/a	n/a	n/a	n/a	n/a
232	Idle	n/a	n/a	n/a	n/a	n/a
240	Idle	n/a	n/a	n/a	n/a	n/a
248	Idle	n/a	n/a	n/a	n/a	n/a

Additionally, if you wanted to view auto configuration information on more than one CSM board, you would enter the **vcac** command followed by a list of the slot numbers for which you want to view information as follows:

vcac <slot list>

where **<slot list>** is a list of the slots for the CSM boards on which you want to view port auto configuration information. If you wanted to view a range of consecutive slots, separate the slot range with the tilde sign (~), as follows:

vcac 3~5

If you wanted to view a list of non-consecutive slots, separate slot specifications with a comma, as follows:

vcac 3,5,7

You may use both syntaxes in your slot list, as follows:

vcac 3,5~7

Note that there are no spaces between slot specifications.

Descriptions of the columns included in the above display are described earlier in *Viewing Virtual Connections* on page 41-82.

Information on One or More Single Ports

To view port auto configuration information on one or more single CSM ports, you enter the **vcac** command along with the slot number for the CSM board and the port number for which you want to receive information, as follows:

vcac <slot>/<port>

where **<slot>** is the slot number where the CSM board is installed and **<port>** is the port number on the CSM board. For example, if you wanted to view information for port 1 on the CSM module in slot 4, you would enter:

vcac 4/1

This command displays a screen similar to the following:

Abs Port	Slot	Port	Inst	Enable Auto Cfg	Trigger Auto Cfg	Current I/F Type	Current Sig Ver	Default I/F Type	Default Sig Ver
192	4	1	0	Enabled	Phy&Logic	PNNI	----	Pri UNI	UNI3.1

Abs Port	Auto Cfg Status	Peer UNI Typ	Peer Dev Typ	Peer Uni Ver	Peer NNI Sig	Peer ILMI Ver
192	Idle	n/a	n/a	n/a	n/a	n/a

Additionally, if you wanted to view more than one port, you would enter the **vcac** command followed by a list of the port numbers for which you want to receive information, as follows:

vcac <port list>

where **<port list>** is a list of CSM ports on which you want to view port auto configuration information. Use the **<slot>/<port>** format and separate port specifications by a comma, as follows:

vcac 3/1,3/7,4/3

If you wanted to view a range of consecutive ports in the same module, separate the port range with the tilde sign (~), as follows:

vcac 3/1~3/7

You may use both syntaxes, as follows:

vcac 3/1~3/7,4/3

Note that there are no spaces between port specifications.

Descriptions of the columns included in the above display are described earlier in *Viewing Virtual Connections* on page 41-82.

Information on One Virtual Instance

To view auto configuration information on a single virtual UNI/NNI instance, you enter the **vcac** command along with the slot number for the CSM board, the port number, and the **Inst** number for the UNI/NNI instance on which you want information, as follows:

```
vcac <slot>/<port> <instance>
```

where **<slot>** is the slot number where the CSM board is installed, **<port>** is the port number on the CSM board, and **<instance>** is the virtual UNI/NNI instance on the physical port. Note that there is a space separating **<slot>/<port>** and **<instance>**. For example, if you wanted to view information for the board in slot 3, port 1, instance 2, you would enter:

```
vcac 3/1 2
```

Note that there is a space between the port specification and the instance number. This command displays a screen similar to the following:

Abs	Enable	Trigger	Current	Current	Default	Default			
Port	Auto Cfg	Auto Cfg	I/F Type	Sig Ver	I/F Type	Sig Ver			
192	4	1	1	Enabled	Phy&Logic	PNNI	----	Pri UNI	UNI3.1

Abs	Auto Cfg	Peer	Peer	Peer	Peer	Peer
Port	Status	UNI Typ	Dev Typ	Uni Ver	NNI Sig	ILMI Ver
192	Idle	n/a	n/a	n/a	n/a	n/a

Descriptions of the columns included in this display are described earlier in *Viewing Virtual Connections* on page 41-82.

Viewing Port Configurations

The **vap** command allows you to view basic information on a single CSM port, all ports on a single CSM board, or all CSM ports in an OmniSwitch chassis. In addition, it will also display information on ATM access ports (if present) and the internal FCSM ports. The following is a sample display.

ATM Port Table

Slot	Port	ATM Port Description	Conn Type	Tran Type	Media Type	UNI Typ	Max VCC
2	1	ATM PORT	SVC	--	--	Pri	1023 10
2	2	ATM PORT	PVC	--	--	Pri	1023 10
5	1	ATM PORT	SVC	STS12	Multi	Pri	1023 10
6	1	ATM PORT	SVC	STS3c	Multi	Pri	1023 10

Slot	Port	Loopback Cfg	Tx Clk Source
2	1	NoLoop	LocalTiming
2	2	NoLoop	LocalTiming
5	1	NoLoop	LocalTiming
6	1	NoLoop	LocalTiming

Slot	Port	ATM Network Prefix	End System Identifier	Sig Ver	Sig VCI	ILMI Enable	ILMI VCI	ILMI Poll
2	1	3903488001bc90000101dbd400	0020da98e910	3.0	5	True	16	Off
2	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	1	3903488001bc90000101dbcfa0	0020dace0660	3.1	5	True	16	Off
5	1	00000000000000000000000000000000	0020dab344f0	3.0	5	True	16	Off

Status

Slot	Port	Sscop Up	Sscop Down	Up	Dn	Status
2	1	WED SEP 29 10:03:37 2001	WED SEP 29 10:03 :32 2001	2	1	Up
2	2	-----	-----	0	0	Down
5	1	WED SEP 29 10:10:53 2001	WED SEP 29 10:10 :46 2001	50	49	Up
6	1	-----	-----	0	0	Down

Slot	Port	Ilmi Up	Ilmi Down	Up	Dn	Status
2	1	WED SEP 29 10:03:30 2001	-----	1	0	Up
2	2	-----	-----	0	0	Down
5	1	WED SEP 29 10:02:51 2001	-----	1	0	Up
6	1	-----	-----	0	0	Down

Slot	Port	Phy Up	Phy Down	Up	Dn	Status
2	1	WED SEP 29 10:02:11 2001	-----	1	0	Enb (SVC)
2	2	WED SEP 29 10:01:46 2001	-----	1	0	Enb (CTL)
5	1	WED SEP 29 10:02:25 2001	-----	1	0	Enb (PVC)
6	1	-----	-----	0	0	Dis (R)

Slot	Port	Tx SegSz	Rx Seg Sz	Tx Buff Sz	Rx Buff Sz
2	1	16384	16384	4600	4600
2	2	8192	8192	8192	8192
5	1	131072	131072	4600	4600
6	1	131072	131072	4600	4600

Slot	Port	Primary	Secondary	FailOver	Reason of Last Failover
5	1	Active	Inactive	0	

— Output continues on next page —

Viewing Port Configurations

CSM Port Table

Slot	Port	CSM Port Description	Tran Type	Media Type	Intrf Type	Uni Ver	#Bits VPI VCI
2	1	CSM PORT	STS3c	Multi	PrUNI	3.0 2	10
2	2	CSM PORT	STS3c	Multi	PrUNI	3.0 2	10
3	1	CSM PORT	STS3c	Multi	PNNI	---	2 10
3	2	CSM PORT	STS3c	Multi	PNNI	---	2 10
3	3	CSM PORT	STS3c	Multi	PNNI	---	2 10
3	4	CSM PORT	STS3c	Multi	PrUNI	3.0 2	10
3	5	CSM PORT	STS3c	Multi	PrUNI	3.0 2	10
3	6	CSM PORT	STS3c	Multi	PrUNI	3.0 2	10
3	7	CSM PORT	STS3c	Multi	PNNI	---	2 10
3	8	CSM PORT	STS3c	Multi	PrUNI	3.0 2	10
4	1	CSM PORT	STS3c	Multi	PrUNI	3.1 2	10
4	2	CSM PORT	STS3c	Multi	PrUNI	3.1 2	10
4	3	CSM PORT	STS3c	Multi	PrUNI	3.0 2	10
4	4	CSM PORT	STS3c	Multi	PrUNI	3.0 2	10
4	5	CSM PORT	STS3c	Multi	PrUNI	3.0 2	10
4	6	CSM PORT	STS3c	Multi	PrUNI	3.0 2	10
4	7	CSM PORT	STS3c	Multi	PrUNI	3.0 2	10
4	8	CSM PORT	STS3c	Multi	PrUNI	3.0 2	10

Slot	Port	MaxPhyBW	Port Bandwidth OverBookFactor	Port Residual BWs	
				RX	TX
2	1	1412830	1.00	1412831	1412831
2	2	353208	1.00	353209	353209
3	1	353208	1.00	353208	353208
3	2	353208	1.00	353208	353208
3	3	353208	1.00	353208	353208
3	4	353208	1.00	353208	353208
3	5	353208	1.00	353208	353208
3	6	353208	1.00	353208	353208
3	7	353208	1.00	353208	353208
3	8	353208	1.00	353208	353208
4	1	353208	1.00	353209	353209
4	2	353208	1.00	353208	353208
4	3	353208	1.00	353208	353208
4	4	353208	1.00	353208	353208
4	5	353208	1.00	353208	353208
4	6	353208	1.00	353208	353208
4	7	353208	1.00	353208	353208
4	8	353208	1.00	353208	353208

Slot	Port	ATM Address	Max	Max	Cfgd	Cfgd
			VPCs	VCCs	VPCs	VCI
2	1	3903488001bc9000010176fd600020da0000c000	3	1022	0	3
2	2	3903488001bc9000010176fd600020da0000c800	3	1022	0	9
3	1	3903488001bc9000010176fd600020da0000d000	3	1022	0	0
3	2	3903488001bc9000010176fd600020da0000d800	3	1022	0	2
3	3	3903488001bc9000010176fd600020da0000e000	3	1022	0	11
3	4	3903488001bc9000010176fd600020da0000e800	3	1022	0	0
3	5	3903488001bc9000010176fd600020da0000f000	3	1022	0	0
3	6	3903488001bc9000010176fd600020da0000f800	3	1022	0	0
3	7	3903488001bc9000010176fd600020da00010000	3	1022	0	0
3	8	3903488001bc9000010176fd600020da00010800	3	1022	0	0
4	1	3903488001bc9000010176fd600020da00011000	3	1022	0	0
4	2	3903488001bc9000010176fd600020da00011800	3	1022	0	0
4	3	3903488001bc9000010176fd600020da00012000	3	1022	0	0
4	4	3903488001bc9000010176fd600020da00012800	3	1022	0	0
4	5	3903488001bc9000010176fd600020da00013000	3	1022	0	0
4	6	3903488001bc9000010176fd600020da00013800	3	1022	0	0
4	7	3903488001bc9000010176fd600020da00014000	3	1022	0	0
4	8	3903488001bc9000010176fd600020da00016000	3	1022	0	0

— Output continues on next page —

Slot	Port	Sscop Up	Sscop Down	Up	Dn	Status
2	1	WED SEP 29 10:03:37 2001	WED SEP 29 10:03:24 2001	2	1	Up
2	2	-----	-----	0	0	Down
3	1	-----	-----	0	0	Down
3	2	-----	-----	0	0	Down
3	3	WED SEP 29 10:03:21 2001	-----	1	0	Up
3	4	-----	-----	0	0	Down
3	5	-----	-----	0	0	Down
3	6	-----	-----	0	0	Down
3	7	-----	-----	0	0	Down
3	8	-----	-----	0	0	Down
4	1	-----	-----	0	0	Down
4	2	-----	-----	0	0	Down
4	3	-----	-----	0	0	Down
4	4	-----	-----	0	0	Down
4	5	-----	-----	0	0	Down
4	6	-----	-----	0	0	Down
4	7	-----	-----	0	0	Down
4	8	-----	-----	0	0	Down

Slot	Port	Ilmi Up	Ilmi Down	Up	Dn	Status
2	1	WED SEP 29 10:03:30 2001	-----	1	0	Up
2	2	-----	-----	0	0	Down
3	1	-----	-----	0	0	Down
3	2	-----	-----	0	0	Down
3	3	-----	-----	0	0	Down
3	4	-----	-----	0	0	Down
3	5	-----	-----	0	0	Down
3	6	-----	-----	0	0	Down
3	7	-----	-----	0	0	Down
3	8	-----	-----	0	0	Down
4	1	-----	-----	0	0	Down
4	2	-----	-----	0	0	Down
4	3	-----	-----	0	0	Down
4	4	-----	-----	0	0	Down
4	5	-----	-----	0	0	Down
4	6	-----	-----	0	0	Down
4	7	-----	-----	0	0	Down
4	8	-----	-----	0	0	Down

— Output continues on next page —

Viewing Port Configurations

Slot	Port	Phy Up	Phy Down	Up	Dn	Status
2	1	WED SEP 29 10:03:18 2001	-----	1	0	En
2	2	WED SEP 29 10:03:18 2001	-----	1	0	En
3	1	-----	WED SEP 29 10:03:18 2001	0	1	Dis
3	2	-----	WED SEP 29 10:03:19 2001	0	1	Dis
3	3	WED SEP 29 10:03:19 2001	-----	1	0	En
3	4	-----	WED SEP 29 10:03:21 2001	0	1	Dis
3	5	-----	WED SEP 29 10:03:21 2001	0	1	Dis
3	6	-----	WED SEP 29 10:03:21 2001	0	1	Dis
3	7	-----	WED SEP 29 10:03:21 2001	0	1	Dis
3	8	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	1	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	2	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	3	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	4	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	5	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	6	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	7	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	8	-----	WED SEP 29 10:03:21 2001	0	1	Dis

ILMI						
Slot	Port	Mode	Phy Protocol	Signaling	Enable/ Poll	CSM Port Auto Cfg
2	1	Normal	SONET	Enb	Enable/Off	Enabled
2	2	Normal	SONET	Enb	Enable/Off	Enabled
3	1	Normal	SONET	Enb	Enable/On	Enabled
3	2	Normal	SONET	Enb	Enable/On	Enabled
3	3	Normal	SONET	Enb	Enable/On	Enabled
3	4	Normal	SONET	Enb	Enable/On	Enabled
3	5	Normal	SONET	Enb	Enable/On	Enabled
3	6	Normal	SONET	Enb	Enable/On	Enabled
3	7	Normal	SONET	Enb	Enable/On	Enabled
3	8	Normal	SONET	Enb	Enable/On	Enabled
4	1	Normal	SONET	Enb	Enable/On	Enabled
4	2	Normal	SONET	Enb	Enable/On	Enabled
4	3	Normal	SONET	Enb	Enable/On	Enabled
4	4	Normal	SONET	Enb	Enable/On	Enabled
4	5	Normal	SONET	Enb	Enable/On	Enabled
4	6	Normal	SONET	Enb	Enable/On	Enabled
4	7	Normal	SONET	Enb	Enable/On	Enabled
4	8	Normal	SONET	Enb	Enable/On	Enabled

— Output continues on next page —

Clock Source				
Slot	Port	Timing Mode	Configured Source	Current Source
3	1	Local	Oscillator	Oscillator
3	2	Local	Oscillator	Oscillator
3	3	Local	Oscillator	Oscillator
3	4	Local	Oscillator	Oscillator
3	5	Local	Oscillator	Oscillator
3	6	Local	Oscillator	Oscillator
3	7	Local	Oscillator	Oscillator
3	8	Local	Oscillator	Oscillator
4	1	Local	Oscillator	Oscillator
4	2	Local	Oscillator	Oscillator
4	3	Local	Oscillator	Oscillator
4	4	Local	Oscillator	Oscillator
4	5	Local	Oscillator	Oscillator
4	6	Local	Oscillator	Oscillator
4	7	Local	Oscillator	Oscillator
4	8	Local	Oscillator	Oscillator

Cell Error Statistics				
Slot	Port	Cell Count	Correctable Cell Count	Uncorrectable Cell Count
3	1	0	0	0
3	2	0	0	0
3	3	358	0	0
3	4	0	0	0
3	5	0	0	0
3	6	0	0	0
3	7	0	0	0
3	8	0	0	0
4	1	0	0	0
4	2	0	0	0
4	3	0	0	0
4	4	0	0	0
4	5	0	0	0
4	6	0	0	0
4	7	0	0	0
4	8	0	0	0

The columns under the **ATM Port Table** heading include information on ATM access module ports and FCSM internal ports. An FCSM includes two internal ports. The first port is user-configurable; half of this port is the same as an ATM access port and half is a CSM OC-3c/STM-1 port. The second FCSM port is not user-configurable; it is used for communication between the frame bus and cell matrix. The second FCSM port also has an ATM access half and a CSM half. Descriptions of these columns can be found in Chapter 33, "Managing ATM Access Modules."

Descriptions of the CSM part of the display are as follows.

Slot/Port. The slot within the chassis and the port on that module for which information will be displayed. This command displays information for a single port in one row.

CSM Port Description. A description of this port entered during port configuration using the **map** command. The port description can be up to 30 characters long.

Tran Type. The type of ATM port. This type will either be an OC-3c/STM-1 port (**STS-3c**) or an OC-12c/STM-4c port (**STS-12c**).

Media Type. The type of fiber cable used on this port. The type will either be multimode (**Multi**) or single mode (**Single**).

Intrf Type. The type of ATM logical connection used to service this port. The UNI type will be Private (**PrUNI**), Public (**PbUNI**), Interim Inter-Switch Protocol (**IISP**), or Private Network-to-Network Interface (**PNNI**). These options are explained in the section, *Modifying a Port Configuration* on page 41-29.

UNI Ver. The version used for the ATM User-to-Network Interface. The version number corresponds to the ATM Forum Specification with which this UNI implementation complies. The OmniSwitch is compliant with UNI versions 3.0 and 3.1. If you have installed the software for multiple peer group PNNI, then you can also set the signaling version to 4.0.

VPI Bits. The number of bits used for the Virtual Path Identifiers (VPIs) set up on this ATM port. CSM-U+ ports support 0 to 6 bits (the default is 4) and the CSM-A25-12 and CSM-A25-24W support up to 9 bits per VPI; all other CSM ports can support up to 12 bits. The number of VPI bits is set through the **map** command.

VCI Bits. The number of bits used for the Virtual Channel Identifiers (VCIs) set up on this ATM port. CSM-U+ ports support 8 to 14 bits (the default is 10) and the CSM-A25-12 and CSM-A25-24W support up to 9 bits per VCI; all other CSM ports can support up to 12 bits. The number of VCI bits is set through the **map** command.

Port Bandwidth Overbook Factor. The maximum available bandwidth and OverBooking Factor defined for this CSM port. The Overbooking Factor is specified through the **map** command.

Max Phy BW. The maximum physical bandwidth available on this port (bps). In order for maximum available bandwidth to be monitored and calculated by the switch, Overbooking must be enabled through the **map** command (default = **1.0** - No Overbooking).

OverBook Factor. The Call OverBooking Factor specified for this port through the **map** command (default = **1.0** - No Overbooking; normal port operation). Underbooking can be enabled by specifying a **Bandwidth Overbooking Factor** between **0.0** and **1.0**. Overbooking can be enabled by specifying a value greater than **1.0**. (Note that unusually high values will be discarded, and the previous value will be retained.) By specifying a value of **0.0**, Connection Admission Control (CAC) will be disabled.

Rx Port Residual BWs. The amount of residual bandwidth available on the receiving port.

Tx Port Residual BWs. The amount of residual bandwidth available on the sending port

ATM Address. The ATM address defined for this CSM port. This address is defined through the **map** command.

Max VPCs. The maximum number of Virtual Path Connections supported on this port. The maximum number depends on the number of bits specified for the VPI under **VPI Bits**. For example, if the number of bits for VPIs is 4, then the maximum number of VPCs will be 15. If you selected the **VPI Bits** to be 2, then the maximum number of VPCs would be 3.

Max VCCs. The maximum number of Virtual Channel Connections supported by this port per Virtual Path. The maximum number depends on the number of bits specified for the VCI under **VCI Bits**. For example, if the number of bits for VCIs is 8, then the maximum number of VCCs will be 254. If you selected the **VCI Bits** to be 10, then the maximum number of VCCs would be 1022.

Cfgd VPCs. The number of Virtual Path Connections (VPCs) configured on this CSM port. VPCs are configured through the **cvc** and **scvc** commands.

Cfgd VCCs. The number of Virtual Channel Connections (VCCs) on this CSM port. VCCs are configured through the **cvc** and **scvc** commands. This value includes non-user-configured switched virtual circuits (SVCs).

The following column headings fall under the table heading labeled **Status**.

SSCOP. The current state of the Service-Specific Connection Oriented Protocol (SSCOP). SSCOP operates on the ATM control plane and is a peer-to-peer protocol that helps set up connections and provides a reliable transport mechanism for signaling. The **Sscop Up** and **Sscop Down** columns will indicate the last time SSCOP last came up and went down, respectively. The **Up** and **Down** columns will indicate the number of times SSCOP came up and went down, respectively. The SSCOP **Status** column will indicate Up or Down.

ILMI. The Integrated Local Management Interface (ILMI) enabled on this port. The **Ilmi Up** and **Ilmi Down** columns will indicate the last time ILMI last came up and went down, respectively. The **Up** and **Down** columns will indicate the number of times ILMI came up and went down, respectively. The ILMI **Status** column will indicate Up or Down.

PHY. The operational status of the port. The **Phy Up** and **Phy Down** columns will indicate the last time PHY last came up and went down, respectively. The **Up** and **Down** columns will indicate the number of times PHY came up and went down, respectively. The PHY **Status** column will indicate whether the port is **Enabled** or **Disabled**. The port will be enabled if the port is connected on this end and the far end. If there is a disconnection at either end, then the operational status will be **Disabled**.

Mode. The port mode used for the IOP ASIC on this CSM module. This mode will be **Normal**. Other modes will be supported in later releases.

Phy Protocol. The type of physical media standard used for this port. In North America ATM broadband services are delivered over Synchronous Optical Network (SONET) facilities. Outside North America, ATM broadband services use Synchronous Digital Hierarchy (SDH).

Signaling. Indicates whether or not the Service-Specific Connection Protocol (SSCOP) is enabled. SSCOP

ILMI Enable. Indicates whether the Integrated Local Management Interface (ILMI) is enabled on this port.

CSM Port Auto Cfg. Indicates whether or not auto port configuration is enabled on this port.

The columns under the **Clock Source** heading include information on the clocking source for all CSM ports on the system.

Timing Mode. This field has two options: **Loop** and **Local**. **Loop**, means the port is deriving its clocking directly from the receive data. **Local**, means the port is deriving its clocking from the bus.

Configured Source. Indicates that the current source for the port is either its local oscillator (the default setting), or one of the buses.

Current Source. Indicates that the configured source for the port is either its local oscillator (the default setting), or one of the buses.

◆ **Note** ◆

If Configured Source and Current Source are different, it is a probable indicator that the port's configured source has failed.

The columns under the **Cell Error Statistics** heading include information on the RX Cell Statistics for the SUNI chip installed on all CSM ports in the system.

Cell Count. Indicates the total number of cells received on the CSM port.

Correctable Cell Count. Indicates the number of cells received with 1-bit HCS error on the CSM port.

Uncorrectable Cell Count. Indicates the number of cells received with more than 1-bit HCS errors.

Information on the Ports for One CSM Board

To view information on all CSM ports in a single CSM board, you enter the **vap** command along with the slot number for the CSM board, as follows:

vap <slot>

where **<slot>** is the slot number where the CSM board is installed. For example, if you wanted to obtain status information for the board in slot 4, you would enter:

vap 4

Viewing Port Configurations

This command displays a screen similar to the following:

CSM Port Table						
Slot	Port	CSM Port Description	Tran Type	Media Type	Intrf Type	Uni Ver VPI VCI
4	1	CSM PORT	STS3c	Multi	PrUNI	3.1 2 10
4	2	CSM PORT	STS3c	Multi	PrUNI	3.1 2 10
4	3	CSM PORT	STS3c	Multi	PrUNI	3.0 2 10
4	4	CSM PORT	STS3c	Multi	PrUNI	3.0 2 10
4	5	CSM PORT	STS3c	Multi	PrUNI	3.0 2 10
4	6	CSM PORT	STS3c	Multi	PrUNI	3.0 2 10
4	7	CSM PORT	STS3c	Multi	PrUNI	3.0 2 10
4	8	CSM PORT	STS3c	Multi	PrUNI	3.0 2 10

Slot	Port	MaxPhyBW	Port Bandwidth OverBookFactor	Port Residual BWs RX	TX
4	1	1412830	1.00	1412831	1412831
4	2	353208	1.00	353209	353209
4	3	353208	1.00	353208	353208
4	4	353208	1.00	353208	353208
4	5	353208	1.00	353208	353208
4	6	353208	1.00	353208	353208
4	7	353208	1.00	353208	353208
4	8	353208	1.00	353208	353208

Slot	Port	ATM Address	Max VPCs	Max VCCs	Cfgd VPCs	Cfgd VCI
4	1	3903488001bc9000010176fd600020da00011000	3	1022	0	0
4	2	3903488001bc9000010176fd600020da00011800	3	1022	0	3
4	3	3903488001bc9000010176fd600020da00012000	3	1022	0	1
4	4	3903488001bc9000010176fd600020da00012800	3	1022	0	0
4	5	3903488001bc9000010176fd600020da00013000	3	1022	0	0
4	6	3903488001bc9000010176fd600020da00013800	3	1022	0	0
4	7	3903488001bc9000010176fd600020da00014000	3	1022	0	0
4	8	3903488001bc9000010176fd600020da00016000	3	1022	0	0

Slot	Port	Sscop Up	Sscop Down	Up	Dn	Status
4	1	-----	-----	0	0	Down
4	2	-----	-----	0	0	Down
4	3	-----	-----	0	0	Down
4	4	-----	-----	0	0	Down
4	5	-----	-----	0	0	Down
4	6	-----	-----	0	0	Down
4	7	-----	-----	0	0	Down
4	8	-----	-----	0	0	Down

Slot	Port	Ilmi Up	Ilmi Down	Up	Dn	Status
4	1	-----	-----	0	0	Down
4	2	-----	-----	0	0	Down
4	3	-----	-----	0	0	Down
4	4	-----	-----	0	0	Down
4	5	-----	-----	0	0	Down
4	6	-----	-----	0	0	Down
4	7	-----	-----	0	0	Down
4	8	-----	-----	0	0	Down

Slot	Port	Phy Up	Phy Down	Up	Dn	Status
4	1	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	2	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	3	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	4	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	5	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	6	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	7	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	8	-----	WED SEP 29 10:03:21 2001	0	1	Dis

— Output continues on next page —

Slot	Port	Mode	Phy Protocol	Signaling	ILMI	
					Enable/ Poll	CSM Port Auto Cfg
4	1	Normal	SONET	Enb	Enable/On	Enabled
4	2	Normal	SONET	Enb	Enable/On	Enabled
4	3	Normal	SONET	Enb	Enable/On	Enabled
4	4	Normal	SONET	Enb	Enable/On	Enabled
4	5	Normal	SONET	Enb	Enable/On	Enabled
4	6	Normal	SONET	Enb	Enable/On	Enabled
4	7	Normal	SONET	Enb	Enable/On	Enabled
4	8	Normal	SONET	Enb	Enable/On	Enabled

Clock Source

Slot	Port	Timing Mode	Configured Source	Current Source
4	1	Local	Oscillator	Oscillator
4	2	Local	Oscillator	Oscillator
4	3	Local	Oscillator	Oscillator
4	4	Local	Oscillator	Oscillator
4	5	Local	Oscillator	Oscillator
4	6	Local	Oscillator	Oscillator
4	7	Local	Oscillator	Oscillator
4	8	Local	Oscillator	Oscillator

Cell Error Statistics

Slot	Port	Cell Count	Correctable Cell Count	Uncorrectable Cell Count
4	1	0	0	0
4	2	0	0	0
4	3	0	0	0
4	4	0	0	0
4	5	0	0	0
4	6	0	0	0
4	7	0	0	0
4	8	0	0	0

Descriptions of the columns included in this display are described earlier in *Viewing Port Configurations* on page 41-63.

Information of One Port

To view information on a single CSM port, you enter the **vap** command along with the slot number for the CSM board and the port number for which you want to receive information, as follows:

vap <slot>/<port>

where **<slot>** is the slot number where the CSM board is installed and **<port>** is the port number on the CSM board. For example, if you wanted to view basic information for port 1 on the CSM module in slot 4, you would enter:

vap 4/1

This command displays a screen similar to the following:

```

CSM Port Table

Slot Port      CSM Port Description      Tran Media Intrf Uni #Bits
==== =====
4   1   CSM PORT                  STS3c Multi PrUNI 3.1 2 10

Slot Port      MaxPhyBW      Port Bandwidth
OverBookFactor      Port Residual BWs
RX              TX
==== =====
4   1   1412830      1.00          1412831      1412831

Slot Port      ATM Address      Max Max Cfgd Cfgd
VPCs VCCs VPCs VCI
==== =====
4   1   3903488001bc9000010176fd600020da00011000 3 1022 0 0

Slot Port      Sscop Up      Sscop Down      Up Dn Status
==== =====
4   1   -----      -----          0 0 Down

Slot Port      Ilmi Up      Ilmi Down      Up Dn Status
==== =====
4   1   -----      -----          0 0 Down

Slot Port      Phy Up      Phy Down      Up Dn Status
==== =====
4   1   -----      WED SEP 29 10:03:21 2001 0 1 Dis

ILMI
----- CSM Port
Slot Port      Mode      Phy Protocol      Signaling      Enable/ Poll      Auto Cfg
==== =====
4   1   Normal      SONET      Enb      Enable/On      Enabled

Clock Source
-----
Slot Port      Timing Mode      Configured      Current
Source      Source
==== =====
4   1   Local      Oscillator      Oscillator

Cell Error Statistics
-----
Slot Port      Cell Count      Correctable      Uncorrectable
Cell Count      Cell Count
==== =====
4   1   0      0      0
    
```

Descriptions of the columns included in this display are described earlier in *Viewing Port Configurations* on page 41-63.

Viewing SSCOP, ILMI, and PHY

You can view general and detailed Service-Specific Connection Oriented Protocol (SSCOP), Integrated Local Management Interface (ILMI), and Physical information on all CSM ports in a switch, a single CSM board, and individual ports. The **vap** command is used to provide this information.

Viewing SSCOP, ILMI, and PHY Information on All Ports

To view SSCOP, ILMI, and PHY information on all CSM ports in a switch, you enter the **vap** command along with the following parameters:

```
vap sip
```

where **s** indicates SSCOP, **i** indicates ILMI, and **p** indicates PHY. This command displays a screen similar to the following:

CSM Port Table						
Slot	Port	SScop Up	SScop Down	Up	Dn	Status
2	1	WED SEP 29 10:03:37 2001	WED SEP 29 10:03:24 2001	2	1	Up
2	2	-----	-----	0	0	Down
3	1	-----	-----	0	0	Down
3	2	-----	-----	0	0	Down
3	3	WED SEP 29 10:03:21 2001	-----	1	0	Up
3	4	-----	-----	0	0	Down
3	5	-----	-----	0	0	Down
3	6	-----	-----	0	0	Down
3	7	-----	-----	0	0	Down
3	8	-----	-----	0	0	Down
4	1	-----	-----	0	0	Down
4	2	-----	-----	0	0	Down
4	3	-----	-----	0	0	Down
4	4	-----	-----	0	0	Down
4	5	-----	-----	0	0	Down
4	6	-----	-----	0	0	Down
4	7	-----	-----	0	0	Down
4	8	-----	-----	0	0	Down

Slot	Port	Ilmi Up	Ilmi Down	Up	Dn	Status
2	1	WED SEP 29 10:03:30 2001	-----	1	0	Up
2	2	-----	-----	0	0	Down
3	1	-----	-----	0	0	Down
3	2	-----	-----	0	0	Down
3	3	-----	-----	0	0	Down
3	4	-----	-----	0	0	Down
3	5	-----	-----	0	0	Down
3	6	-----	-----	0	0	Down
3	7	-----	-----	0	0	Down
3	8	-----	-----	0	0	Down
4	1	-----	-----	0	0	Down
4	2	-----	-----	0	0	Down
4	3	-----	-----	0	0	Down
4	4	-----	-----	0	0	Down
4	5	-----	-----	0	0	Down
4	6	-----	-----	0	0	Down
4	7	-----	-----	0	0	Down
4	8	-----	-----	0	0	Down

— Output continues on next page —

Viewing Port Configurations

Slot	Port	Phy Up	Phy Down	Up	Dn	Status
2	1	WED SEP 29 10:03:18 2001	-----	1	0	En
2	2	WED SEP 29 10:03:18 2001	-----	1	0	En
3	1	-----	WED SEP 29 10:03:18 2001	0	1	Dis
3	2	-----	WED SEP 29 10:03:19 2001	0	1	Dis
3	3	WED SEP 29 10:03:19 2001	-----	1	0	En
3	4	-----	WED SEP 29 10:03:21 2001	0	1	Dis
3	5	-----	WED SEP 29 10:03:21 2001	0	1	Dis
3	6	-----	WED SEP 29 10:03:21 2001	0	1	Dis
3	7	-----	WED SEP 29 10:03:21 2001	0	1	Dis
3	8	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	1	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	2	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	3	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	4	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	5	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	6	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	7	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	8	-----	WED SEP 29 10:03:21 2001	0	1	Dis

Cell Error Statistics

Slot	Port	Cell Count	Correctable Cell Count	Uncorrectable Cell Count
3	1	0	0	0
3	2	0	0	0
3	3	358	0	0
3	4	0	0	0
3	5	0	0	0
3	6	0	0	0
3	7	0	0	0
3	8	0	0	0
4	1	0	0	0
4	2	0	0	0
4	3	0	0	0
4	4	0	0	0
4	5	0	0	0
4	6	0	0	0
4	7	0	0	0
4	8	0	0	0

Additionally, you may enter the parameters for SSCOP, ILMI, and PHY in any order and combination. For example, if you wanted to view only the ILMI and PHY, you would enter the **vap** command along with the respective parameters as follows:

vap ip

or

vap pi

This command displays a screen similar to the following:

CSM Port Table

Slot	Port	Ilmi Up	Ilmi Down	Up	Dn	Status
2	1	WED SEP 29 10:03:30 2001	-----	1	0	Up
2	2	-----	-----	0	0	Down
3	1	-----	-----	0	0	Down
3	2	-----	-----	0	0	Down
3	3	-----	-----	0	0	Down
3	4	-----	-----	0	0	Down
3	5	-----	-----	0	0	Down
3	6	-----	-----	0	0	Down
3	7	-----	-----	0	0	Down
3	8	-----	-----	0	0	Down
4	1	-----	-----	0	0	Down
4	2	-----	-----	0	0	Down
4	3	-----	-----	0	0	Down
4	4	-----	-----	0	0	Down
4	5	-----	-----	0	0	Down
4	6	-----	-----	0	0	Down
4	7	-----	-----	0	0	Down
4	8	-----	-----	0	0	Down

Slot	Port	Phy Up	Phy Down	Up	Dn	Status
2	1	WED SEP 29 10:03:18 2001	-----	1	0	En
2	2	WED SEP 29 10:03:18 2001	-----	1	0	En
3	1	-----	WED SEP 29 10:03:18 2001	0	1	Dis
3	2	-----	WED SEP 29 10:03:19 2001	0	1	Dis
3	3	WED SEP 29 10:03:19 2001	-----	1	0	En
3	4	-----	WED SEP 29 10:03:21 2001	0	1	Dis
3	5	-----	WED SEP 29 10:03:21 2001	0	1	Dis
3	6	-----	WED SEP 29 10:03:21 2001	0	1	Dis
3	7	-----	WED SEP 29 10:03:21 2001	0	1	Dis
3	8	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	1	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	2	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	3	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	4	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	5	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	6	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	7	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	8	-----	WED SEP 29 10:03:21 2001	0	1	Dis

Cell Error Statistics

Slot	Port	Cell Count	Correctable Cell Count	Uncorrectable Cell Count
3	1	0	0	0
3	2	0	0	0
3	3	358	0	0
3	4	0	0	0
3	5	0	0	0
3	6	0	0	0
3	7	0	0	0
3	8	0	0	0
4	1	0	0	0
4	2	0	0	0
4	3	0	0	0
4	4	0	0	0
4	5	0	0	0
4	6	0	0	0
4	7	0	0	0
4	8	0	0	0

Descriptions of the columns included in the two displays above are described earlier in *Viewing Port Configurations* on page 41-63.

Viewing SSCOP, ILMI, and PHY Information on One CSM Board

To view SSCOP, ILMI, and PHY information on a single CSM board in a switch, you enter the **vap** command along with the slot number for the CSM board and the following parameters:

vap <slot> sip

where **<slot>** is the slot number where the CSM board is installed, **s** indicates SSCOP, **i** indicates ILMI, and **p** indicates PHY. For example, if you wanted to view SSCOP, ILMI, and PHY information for the board in slot 4, you would enter:

vap 4 sip

This command displays a screen similar to the following:

CSM Port Table									
Slot	Port	CSM Port Description	Tran Type	Media Type	Intrf Type	Uni Ver	#Bits VPI	VCI	
4	1	CSM PORT	STS3c	Multi	PrUNI	3.1	2	10	
4	2	CSM PORT	STS3c	Multi	PrUNI	3.1	2	10	
4	3	CSM PORT	STS3c	Multi	PrUNI	3.0	2	10	
4	4	CSM PORT	STS3c	Multi	PrUNI	3.0	2	10	
4	5	CSM PORT	STS3c	Multi	PrUNI	3.0	2	10	
4	6	CSM PORT	STS3c	Multi	PrUNI	3.0	2	10	
4	7	CSM PORT	STS3c	Multi	PrUNI	3.0	2	10	
4	8	CSM PORT	STS3c	Multi	PrUNI	3.0	2	10	

Slot	Port	ATM Address	Max VPCs	Max VCCs	Cfgd VPCs	Cfgd VCCs
4	1	3903488001bc90000101dbd4000020da0000c000	3	1022	0	0
4	2	3903488001bc90000101dbd4000020da0000c800	3	1022	0	0
4	3	3903488001bc90000101dbd4000020da0000d000	3	1022	0	0
4	4	3903488001bc90000101dbd4000020da0000d800	3	1022	0	0
4	5	3903488001bc90000101dbd4000020da0000e000	3	1022	0	0
4	6	3903488001bc90000101dbd4000020da0000e800	3	1022	0	0
4	7	3903488001bc90000101dbd4000020da0000f000	3	1022	0	0
4	8	3903488001bc90000101dbd4000020da0000f800	3	1022	0	0

Slot	Port	Sscop Up	Sscop Down	Up	Dn	Status
4	1	-----	-----	0	0	Down
4	2	-----	-----	0	0	Down
4	3	-----	-----	0	0	Down
4	4	-----	-----	0	0	Down
4	5	-----	-----	0	0	Down
4	6	-----	-----	0	0	Down
4	7	-----	-----	0	0	Down
4	8	-----	-----	0	0	Down

Slot	Port	Ilmi Up	Ilmi Down	Up	Dn	Status
4	1	-----	-----	0	0	Down
4	2	-----	-----	0	0	Down
4	3	-----	-----	0	0	Down
4	4	-----	-----	0	0	Down
4	5	-----	-----	0	0	Down
4	6	-----	-----	0	0	Down
4	7	-----	-----	0	0	Down
4	8	-----	-----	0	0	Down

— Output continues on next page —

Slot	Port	Phy Up	Phy Down	Up	Dn	Status
4	1	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	2	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	3	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	4	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	5	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	6	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	7	-----	WED SEP 29 10:03:21 2001	0	1	Dis
4	8	-----	WED SEP 29 10:03:21 2001	0	1	Dis

ILMI						
Slot	Port	Mode	Phy Protocol	Signaling	Enable/ Poll	CSM Port Auto Cfg
4	1	Normal	SONET	Enb	Enable/On	Enabled
4	2	Normal	SONET	Enb	Enable/On	Enabled
4	3	Normal	SONET	Enb	Enable/On	Enabled
4	4	Normal	SONET	Enb	Enable/On	Enabled
4	5	Normal	SONET	Enb	Enable/On	Enabled
4	6	Normal	SONET	Enb	Enable/On	Enabled
4	7	Normal	SONET	Enb	Enable/On	Enabled
4	8	Normal	SONET	Enb	Enable/On	Enabled

Clock Source				
Slot	Port	Timing Mode	Configured Source	Current Source
4	1	Local	Oscillator	Oscillator
4	2	Local	Oscillator	Oscillator
4	3	Local	Oscillator	Oscillator
4	4	Local	Oscillator	Oscillator
4	5	Local	Oscillator	Oscillator
4	6	Local	Oscillator	Oscillator
4	7	Local	Oscillator	Oscillator
4	8	Local	Oscillator	Oscillator

Cell Error Statistics				
Slot	Port	Cell Count	Correctable Cell Count	Uncorrectable Cell Count
4	1	0	0	0
4	2	0	0	0
4	3	0	0	0
4	4	0	0	0
4	5	0	0	0
4	6	0	0	0
4	7	0	0	0
4	8	0	0	0

Additionally, you may enter the parameters for SSCOP, ILMI, and PHY in any order and combination. For example, if you wanted to view the statistics for only SSCOP and ILMI for a single board, you would enter the **vap** command along with the slot number and the respective parameters as follows:

vap <slot> si

or

vap <slot> is

Descriptions of the columns included in the display above are described earlier in *Viewing Port Configurations* on page 41-63.

Viewing SSCOP, ILMI, and PHY Information on One Port

To view SSCOP, ILMI, and PHY information on a single CSM port, you enter the **vap** command along with the slot number for the CSM board, the port number for which you want to receive information, and the following parameters:

vap <slot>/<port> sip

where **<slot>** is the slot number where the CSM board is installed, **<port>** is the port number on the CSM board, **s** indicates SSCOP, **i** indicates ILMI, and **p** indicates PHY. For example, if you wanted to view SSCOP, ILMI, and PHY information for port 8 on the CSM module in slot 4, you would enter:

vap 4/8 sip

This command displays a screen similar to the following:

```

CSM Port Table
Slot Port      CSM Port Description      Tran Media Intrf Uni #Bits
==== ==      =====
4   8          CSM PORT                STS3c Multi PrUNI 3.0 2 10

Slot Port      ATM Address                Max Max Cfgd Cfgd
==== ==      =====
4   8          3903488001bc90000101dbd4000020da0000f800 3 1022 0 0

CSM Port Table
Slot Port      Sscop Up      Sscop Down      Up Dn Status
==== ==      =====
4   8          -----
-----
0 0 Down

Slot Port      Ilmi Up      Ilmi Down      Up Dn Status
==== ==      =====
4   8          -----
-----
0 0 --

Slot Port      Phy Up      Phy Down      Up Dn Status
==== ==      =====
4   8          -----
WED FEB 17 16:00:10 1999 0 1 Dis

ILMI
Slot Port      Mode      Phy Protocol      Signaling      Enable/ Poll      CSM Port
==== ==      =====
4   8          Normal      SONET      Enb      Enable/On      Enabled

Clock Source
-----
Slot Port      Timing Mode      Configured      Current
==== ==      =====
4   8          Local      Oscillator      Oscillator

Cell Error Statistics
-----
Slot Port      Cell Count      Correctable      Uncorrectable
==== ==      =====
4   8          0      0      0
    
```

Additionally, you may enter the parameters for SSCOP, ILMI, and PHY in any order and combination. For example, if you wanted to view the statistics for only SSCOP and PHY for a single CSM port, you would enter the **vap** command along with the slot number, the port number for which you want to receive information, and the respective parameters as follows:

```
vap <slot>/<port> sp
```

or

```
vap <slot>/<port> ps
```

Descriptions of the columns included in this display are described earlier in *Viewing Port Configurations* on page 41-63.

Viewing Virtual Connections

The **vvc** command allows you to view information on all virtual circuits in an OmniSwitch chassis. The **vvc** display is comprised of two parts. The first part of the display provides information on all VPI/VCI associated with a given FCSM internal logical port or ATM access port. The second part displays information on all VPIs and VPI/VCI associated with a given CSM port.

Information on All Virtual Circuits in a Switch

To view status information on all CSM virtual circuits in a switch, you enter the **vvc** command without any parameters as follows:

```
vvc
```

The following is a sample of the output from the first part of the display for FCSM and ATM access modules ports. Descriptions of the columns included in this display can be found in Chapter 33, "Managing ATM Access Modules."

```

ATM Connections

Slot  Port  VPI  VCI  Connection Description      Conn  Circuit  Operational
=====  =====  =====  =====  =====  =====  =====  =====
2    2    0    100  Connection 0/100  VCC   PVC   LocalUp End2endUnknown
2    2    0    1018 Connection 0/1018 VCC   PVC   LocalUp End2endUnknown
2    2    0    1019 Connection 0/1019 VCC   PVC   LocalUp End2endUnknown
2    2    0    1021 Connection 0/1021 VCC   PVC   LocalUp End2endUnknown
2    2    0    1022 Connection 0/1022 VCC   PVC   LocalUp End2endUnknown

+ ==> PVC Connections
# ==> MPLS Connections
* ==> SVC Connections which cannot be modified by the user
@ ==> Soft PVC Connections
& ==> Control Connections

```

```

CSM Connections

Incoming      Outgoing
-----
Slot  Port  VPI  VCI  Slot  Port  VPI  VCI  Connection Description      Chan  Transport
=====  =====  =====  =====  =====  =====  =====  =====  =====  =====
2    1    0    5    2    2    0    1022 Connection 5      VC  UNI  UBR  &
2    1    0    16   2    2    0    1021 Connection 16     VC  UNI  UBR  &
2    1    0    18   2    2    0    1020 Connection 18     VC  UNI  UBR  &
2    1    0    100  3    1    0    100  Connection 100    VC  UNI  UBR  +
2    2    0    1017  3    1    0    18   Connection 1017   VC  UNI  UBR  &
2    2    0    1018  3    1    0    16   Connection 1018   VC  UNI  UBR  &
2    2    0    1019  3    1    0    5    Connection 1019   VC  UNI  UBR  &
2    2    0    1020  2    1    0    18   Connection 1020   VC  UNI  UBR  &
2    2    0    1021  2    1    0    16   Connection 1021   VC  UNI  UBR  &
2    2    0    1022  2    1    0    5    Connection 1022   VC  UNI  UBR  &
3    1    0    5    2    2    0    1019 Connection 5      VC  UNI  UBR  &
3    1    0    16   2    2    0    1018 Connection 16     VC  UNI  UBR  &
3    1    0    18   2    2    0    1017 Connection 18     VC  UNI  UBR  &
3    1    0    100  2    1    0    100  Connection 100    VC  UNI  UBR  +

```

The **vvc -v** command variable provides a verbose option, which appears similar to the display shown below:

ATM Connections

Slot	Port	VPI	VCI	Connection Description	Conn Type	Circuit Type	Operational Status
2	1	0	100	Connection 0/100	VCC	PVC	LocalUp End2endUnknown
2	2	0	1018	Connection 0/1018	VCC	PVC	LocalUp End2endUnknown
2	2	0	1019	Connection 0/1019	VCC	PVC	LocalUp End2endUnknown
2	2	0	1021	Connection 0/1021	VCC	PVC	LocalUp End2endUnknown
2	2	0	1022	Connection 0/1022	VCC	PVC	LocalUp End2endUnknown

Slot	Port	VPI	VCI	Port Status	Tx Max Frame Sz	Rx Max Frame Sz
2	1	0	100	UP	8192	8192
2	2	0	1018	UP	8192	8192
2	2	0	1019	UP	8192	8192
2	2	0	1021	UP	8192	8192
2	2	0	1022	UP	8192	8192

Actual Tx Traffic Information

Slot	Port	VPI	VCI	Tx Traffic Descrip Type	Peak Cell Rate	Tx QoS	Best Effort
2	1	0	100	NoCLP NoSCR	353208	Uns	True
2	2	0	1018	NoCLP NoSCR	353208	Uns	True
2	2	0	1019	NoCLP NoSCR	353208	Uns	True
2	2	0	1021	NoCLP NoSCR	353208	Uns	True
2	2	0	1022	NoCLP NoSCR	353208	Uns	True

— Output continues on next page —

Viewing Virtual Connections

Actual Rx Traffic Information

Slot	Port	VPI	VCI	Rx Traffic Descrip Type	Peak Cell Rate	Rx QoS	Best Effort
2	2	0	100	NoCLP NoSCR	353208	Uns	True
2	2	0	1018	NoCLP NoSCR	353208	Uns	True
2	2	0	1019	NoCLP NoSCR	353208	Uns	True
2	2	0	1021	NoCLP NoSCR	353208	Uns	True
2	2	0	1022	NoCLP NoSCR	353208	Uns	True

+ ==> PVC Connections
 # ==> MPLS Connections
 * ==> SVC Connections which cannot be modified by the user
 @ ==> Soft PVC Connections
 & ==> Control Connections

CSM Connections

Incoming				Outgoing				Connection	Chan	Transport
Slot	Port	VPI	VCI	Slot	Port	VPI	VCI	Description	Type	Priority
2	1	0	5	2	2	0	1022	Connection 5	VC UNI	UBR &
2	1	0	16	2	2	0	1021	Connection 16	VC UNI	UBR &
2	1	0	18	2	2	0	1020	Connection 18	VC UNI	UBR &
2	1	0	100	3	1	0	100	Connection 100	VC UNI	UBR +
2	2	0	1017	3	1	0	18	Connection 1017	VC UNI	UBR &
2	2	0	1018	3	1	0	16	Connection 1018	VC UNI	UBR &
2	2	0	1019	3	1	0	5	Connection 1019	VC UNI	UBR &
2	2	0	1020	2	1	0	18	Connection 1020	VC UNI	UBR &
2	2	0	1021	2	1	0	16	Connection 1021	VC UNI	UBR &
2	2	0	1022	2	1	0	5	Connection 1022	VC UNI	UBR &
3	1	0	5	2	2	0	1019	Connection 5	VC UNI	UBR &
3	1	0	16	2	2	0	1018	Connection 16	VC UNI	UBR &
3	1	0	18	2	2	0	1017	Connection 18	VC UNI	UBR &
3	1	0	100	2	1	0	100	Connection 100	VC UNI	UBR +

— Output continues on next page —

Slot	Port	VPI	VCI	Port Status	User Pri.	Statistics Mode
2	1	0	5	UP	15	CntGcra, PsCell
2	1	0	16	UP	15	CntGcra, PsCell
2	1	0	18	UP	15	CntGcra, PsCell
2	1	0	100	UP	15	CntGcra, PsCell
2	2	0	1017	UP	15	CntGcra, PsCell
2	2	0	1018	UP	15	CntGcra, PsCell
2	2	0	1019	UP	15	CntGcra, PsCell
2	2	0	1020	UP	15	CntGcra, PsCell
2	2	0	1021	UP	15	CntGcra, PsCell
2	2	0	1022	UP	15	CntGcra, PsCell
3	1	0	5	UP	15	CntGcra, PsCell
3	1	0	16	UP	15	CntGcra, PsCell
3	1	0	18	UP	15	CntGcra, PsCell
3	1	0	100	UP	15	CntGcra, PsCell

Tx Traffic Information

Slot	Port	VPI	VCI	Tx Traffic Descrip Type	Peak Cell Rate	Sustain Cell Rate	Maximum Burst Sz	Tx QoS	Best Effort
2	1	0	5	NoCLP NoSCR	589			Uns	True
2	1	0	16	NoCLP NoSCR	589			Uns	True
2	1	0	18	NoCLP NoSCR	589			Uns	True
2	1	0	100	NoCLP NoSCR	353208			Uns	True
2	2	0	1017	NoCLP NoSCR	589			Uns	True
2	2	0	1018	NoCLP NoSCR	589			Uns	True
2	2	0	1019	NoCLP NoSCR	589			Uns	True
2	2	0	1020	NoCLP NoSCR	589			Uns	True
2	2	0	1021	NoCLP NoSCR	589			Uns	True
2	2	0	1022	NoCLP NoSCR	589			Uns	True
3	1	1	5	NoCLP NoSCR	589			Uns	True
3	1	1	16	NoCLP NoSCR	589			Uns	True
3	1	0	18	NoCLP NoSCR	589			Uns	True
3	1	0	100	NoCLP NoSCR	353208			Uns	True

— Output continues on next page —

Viewing Virtual Connections

Rx Traffic Information

Slot	Port	VPI	VCI	Rx Traffic Descrip Type	Peak Cell Rate	Sustain Cell Rate	Maximum Burst Sz	Rx QoS	Best Effort
2	1	0	5	NoCLP NoSCR	589			Uns	True
2	1	0	16	NoCLP NoSCR	589			Uns	True
2	1	0	18	NoCLP NoSCR	589			Uns	True
2	1	0	100	NoCLP NoSCR	353208			Uns	True
2	2	0	1017	NoCLP NoSCR	589			Uns	True
2	2	0	1018	NoCLP NoSCR	589			Uns	True
2	2	0	1019	NoCLP NoSCR	589			Uns	True
2	2	0	1020	NoCLP NoSCR	589			Uns	True
2	2	0	1021	NoCLP NoSCR	589			Uns	True
2	2	0	1022	NoCLP NoSCR	589			Uns	True
3	1	0	5	NoCLP NoSCR	589			Uns	True
3	1	0	16	NoCLP NoSCR	589			Uns	True
3	1	0	18	NoCLP NoSCR	589			Uns	True
3	1	0	100	NoCLP NoSCR	353208			Uns	True

Multicast

Slot	Port	VPI	VCI	gcra a enf mode	gcra b enf mode	grp id	enable	ingrs / egrss
2	1	0	5	dx all	dx all	4095	disable	ingress
2	1	0	16	dx all	dx all	4095	disable	ingress
2	1	0	18	dx all	dx all	4095	disable	ingress
2	1	0	100	no cong dx clpl	no cong dx clpl	4095	disable	ingress
2	2	0	1017	dx all	dx all	4095	disable	ingress
2	2	0	1018	dx all	dx all	4095	disable	ingress
2	2	0	1019	dx all	dx all	4095	disable	ingress
2	2	0	1020	dx all	dx all	4095	disable	ingress
2	2	0	1021	dx all	dx all	4095	disable	ingress
2	2	0	1022	dx all	dx all	4095	disable	ingress
3	1	0	5	dx all	dx all	4095	disable	ingress
3	1	0	16	dx all	dx all	4095	disable	ingress
3	1	0	18	dx all	dx all	4095	disable	ingress
3	1	0	100	no cong dx clpl	no cong dx clpl	4095	disable	ingress

— Output continues on next page —

Slot	Port	VPI	VCI	AAL5 Discard	Cdv	Bidir Traffic
2	1	0	5	Disabled	1000	On
2	1	0	16	Disabled	1000	On
2	1	0	18	Disabled	1000	On
2	1	0	100	Disabled	1000	On
2	2	0	1017	Disabled	1000	On
2	2	0	1018	Disabled	1000	On
2	2	0	1019	Disabled	1000	On
2	2	0	1020	Disabled	1000	On
2	2	0	1021	Disabled	1000	On
2	2	0	1022	Disabled	1000	On
3	1	0	5	Disabled	1000	On
3	1	0	16	Disabled	1000	On
3	1	0	18	Disabled	1000	On
3	1	0	100	Disabled	1000	On

The legend at the top of the CSM port display indicates the symbols used to differentiate the four virtual circuit types. A symbol is placed after the **Transport Priority** column to indicate whether the circuit is a Permanent Virtual Circuit (PVC) configured through the **cvc** command (+), a Multi Protocol Label Switching (MPLS) (#), a Switched Virtual Circuit (SVC) configured dynamically by the ATM network (*), a soft PVC configured through the **scvc** command (@), or a management connection (&).

◆ **Note** ◆

MPLS is not supported in the current release.

Port Status. Indicates the FCSM/ASM/CSM physical port status (up=enabled, down=disabled).

User Pri., Statistics Mode. These variables are described earlier in *Configuring Statistics and Priority Parameters* on page 41-45.

Tx Traffic Information, Rx Traffic Information. These variables are described earlier in *Configuring Statistics and Priority Parameters* on page 41-45. Note that for SVCs, the Peak Cell Rate (PCR) is incorrectly displayed as 1; PVCs display the actual configured PCR value.

gcra a mode, gcra b mode. The type of algorithm used for the Generic Cell Rate Algorithm (GCRA), or “leaky bucket,” with this virtual circuit. By default, this column will read **no cong dx clp1**, meaning that only CLP=1 cells will be discarded.

Multicast grp id. The group identification number for this multicast virtual circuit. This number is not user-configurable and is used internally by the switch.

Multicast enable. Indicates whether multicast leaf virtual circuits are associated with this root virtual circuit.

Multicast ingres/egress. Indicates whether this is the ingress or egress point for this multicast virtual circuit.

AAL5 Discard. Indicates how AAL5 PDU cells are discarded during times of congestion. Possible values are as follows:

Disabled. During congestion conditions, cells associated with AAL5 PDU are randomly discarded. Cells are marked when the GCRA contract is violated.

EPD. Early Packet Discard. The switch selectively discards cells associated with AAL5 PDU during congestion conditions. In this mode, the cells of the whole packet are either passed or discarded. At congestion time, if the first cell of a packet has already passed, then the rest of the packet will be passed. When congestion ends, the first cell of a new packet will be passed. Cells are marked when the GCRA contract has been violated.

PPD. Partial Packet Discard. The switch selectively discards cells associated with AAL5 PDU during congestion conditions. In this mode, the cells of the rest of the packet—except for the very last cell—are discarded. When congestion ends, the first cell of a new packet will be passed. Cells are marked when the GCRA contract is violated.

Cdv. Indicates Cell Delay Variation in microseconds. For information about this setting, see *Configuring Statistics and Priority Parameters* on page 41-45.

Bidirectional Traffic. Indicates the status (**on** or **off**) of bidirectional traffic parameters for the transmit and receive sides of this virtual circuit. For information on changing this setting, see *Configuring Traffic Parameters* on page 41-40.

Information on the Ports for One CSM Virtual Circuit

To view status information on virtual circuits in a single CSM board, you enter the **vvv** command along with the slot number for the CSM board, as follows:

```
vvv <slot>
```

where **<slot>** is the slot number where the CSM board is installed. For example, if you wanted to view status information for the board in slot 3, you would enter:

```
vvv 3
```

This command displays a screen similar to the following:

```
+ ==> PVC Connections
# ==> MPLS Connections
* ==> SVC Connections which cannot be modified by the user
@ ==> Soft PVC Connections
& ==> Control Connections
```

CSM Connections

Incoming				Outgoing				Connection Description	Chan Type	Transport Priority
Slot	Port	VPI	VCI	Slot	Port	VPI	VCI			
3	2	0	402	7	3	0	32	fesm_con	VC UNI	UBR @
3	2	0	405	5	3	0	33	csm_conn	VC UNI	UBR @
3	3	0	5	5	2	0	1019	Connection 5	VC UNI	UBR &
3	3	0	16	5	2	0	1018	Connection 16	VC UNI	UBR &
3	3	0	18	5	2	0	1017	Connection 18	VC UNI	UBR &
3	3	0	32	5	2	1	402		VC UNI	UBR *
3	3	0	33	5	2	1	405		VC UNI	UBR *
3	3	0	34	5	3	1	401		VC UNI	UBR *
3	3	0	35	5	3	1	403		VC UNI	UBR *
3	3	1	36	5	3	1	404		VC UNI	UBR *
3	3	1	401	5	3	0	34	Connection 401	VC UNI	UBR @
3	3	1	403	5	3	0	35	Connection 403	VC UNI	UBR @
3	3	1	404	5	3	0	36	csm_conn	VC UNI	UBR @

Viewing Virtual Connections

The **vcv -v** command variable provides a verbose option, which appears similar to the display shown below:

For example, if you wanted to use the verbose option to view status information for the CSM module in slot 3, you would enter:

vcv 3 -v

This command displays a screen similar to the following:

```
+ ==> PVC Connections
# ==> MPLS Connections
* ==> SVC Connections which cannot be modified by the user
@ ==> Soft PVC Connections
& ==> Control Connections
```

CSM Connections

Incoming				Outgoing				Connection Description	Chan Type	Transport Priority
Slot	Port	VPI	VCI	Slot	Port	VPI	VCI			
3	2	0	402	7	3	0	32	fesm_con	VC UNI	UBR @
3	2	0	405	5	3	0	33	csm_conn	VC UNI	UBR @
3	3	0	5	5	2	0	1019	Connection 5	VC UNI	UBR &
3	3	0	16	5	2	0	1018	Connection 16	VC UNI	UBR &
3	3	0	18	5	2	0	1017	Connection 18	VC UNI	UBR &
3	3	0	32	5	2	1	402		VC UNI	UBR *
3	3	0	33	5	2	1	405		VC UNI	UBR *
3	3	0	34	5	3	1	401		VC UNI	UBR *
3	3	0	35	5	3	1	403		VC UNI	UBR *
3	3	1	36	5	3	1	404		VC UNI	UBR *
3	3	1	401	5	3	0	34	Connection 401	VC UNI	UBR @
3	3	1	403	5	3	0	35	Connection 403	VC UNI	UBR @
3	3	1	404	5	3	0	36	csm_conn	VC UNI	UBR @

Slot	Port	VPI	VCI	Port Status	User Pri.	Statistics Mode
3	2	1	402	UP	15	CntGcra, PsCell
3	2	1	405	UP	15	CntGcra, PsCell
3	3	0	5	UP	15	CntGcra, PsCell
3	3	0	16	UP	15	CntGcra, PsCell
3	3	0	18	UP	15	CntGcra, PsCell
3	3	0	32	UP	15	CntGcra, PsCell
3	3	0	33	UP	15	CntGcra, PsCell
3	3	0	34	UP	15	CntGcra, PsCell
3	3	0	35	UP	15	CntGcra, PsCell
3	3	0	36	UP	15	CntGcra, PsCell
3	3	0	401	UP	15	CntGcra, PsCell
3	3	0	403	UP	15	CntGcra, PsCell
3	3	0	404	UP	15	CntGcra, PsCell

Tx Traffic Information

Slot	Port	VPI	VCI	Tx Traffic		Peak Cell Rate	Sustain Cell Rate	Maximum Burst Sz	Tx QoS	Best Effort
				Descrip	Type					
3	2	1	402	NoCLP	NoSCR	1000			Uns	True
3	2	1	405	NoCLP	NoSCR	1000			Uns	True
3	3	0	5	NoCLP	NoSCR	589			Uns	True
3	3	0	16	NoCLP	NoSCR	589			Uns	True
3	3	0	18	NoCLP	NoSCR	589			Uns	True
3	3	0	32	NoCLP	NoSCR	353207			Uns	True
3	3	0	33	NoCLP	NoSCR	353207			Uns	True
3	3	0	34	NoCLP	NoSCR	353207			Uns	True
3	3	0	35	NoCLP	NoSCR	353207			Uns	True
3	3	0	36	NoCLP	NoSCR	353207			Uns	True
3	3	1	401	NoCLP	NoSCR	1000			Uns	True
3	3	1	403	NoCLP	NoSCR	1000			Uns	True
3	3	1	404	NoCLP	NoSCR	1000			Uns	True

— Output continues on next page —

Rx Traffic Information

Slot	Port	VPI	VCI	Rx Traffic Descrip Type	Peak Cell Rate	Sustain Cell Rate	Maximum Burst Sz	Rx QoS	Best Effort
3	2	1	402	NoCLP NoSCR	1000			Uns	True
3	2	1	405	NoCLP NoSCR	1000			Uns	True
3	3	0	5	NoCLP NoSCR	589			Uns	False
3	3	0	16	NoCLP NoSCR	589			Uns	False
3	3	0	18	NoCLP NoSCR	589			Uns	False
3	3	0	32	NoCLP NoSCR	353207			Uns	True
3	3	0	33	NoCLP NoSCR	353207			Uns	True
3	3	0	34	NoCLP NoSCR	353207			Uns	True
3	3	0	35	NoCLP NoSCR	353207			Uns	True
3	3	0	36	NoCLP NoSCR	353207			Uns	True
3	3	1	401	NoCLP NoSCR	1000			Uns	True
3	3	1	403	NoCLP NoSCR	1000			Uns	True
3	3	1	404	NoCLP NoSCR	1000			Uns	True

Multicast

Slot	Port	VPI	VCI	gkra a enf mode	gkra b enf mode	grp id	enable	ingrs / egrss
3	2	1	402	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	2	1	405	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	5	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	16	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	18	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	32	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	33	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	34	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	35	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	36	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	1	401	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	1	403	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	1	404	no cong dx clpl	no cong dx clpl	4095	disable	ingress

Slot	Port	VPI	VCI	AAL5 Discard	Cdv	Bidir Traffic
3	2	1	402	Disabled	1000	On
3	2	1	405	Disabled	1000	On
3	3	0	5	Disabled	1000	On
3	3	0	16	Disabled	1000	On
3	3	0	18	Disabled	1000	On
3	3	0	32	Disabled	1000	On
3	3	0	33	Disabled	1000	On
3	3	0	34	Disabled	1000	On
3	3	0	35	Disabled	1000	On
3	3	0	36	Disabled	1000	On
3	3	1	401	Disabled	1000	On
3	3	1	403	Disabled	1000	On
3	3	1	404	Disabled	1000	On

Descriptions of the columns included in this display are described earlier in *Viewing Virtual Connections* on page 41-82.

Information on One Port

To view status information on virtual circuits in a single CSM port, you enter the **vc** command along with the slot number for the CSM board and the port number for which you want to receive information, as follows:

```
vc <slot>/<port>
```

where **<slot>** is the slot number where the CSM board is installed and **<port>** is the port number on the CSM board. For example, if you wanted to view status information for port 3 on the CSM module in slot 3, you would enter:

```
vc 3/3
```

This command displays a screen similar to the following:

```
+ ==> PVC Connections
# ==> MPLS Connections
* ==> SVC Connections which cannot be modified by the user
@ ==> Soft PVC Connections
& ==> Control Connections
```

CSM Connections												
Incoming				Outgoing				Connection Description	Chan Type	Transport		
Slot	Port	VPI	VCI	Slot	Port	VPI	VCI			Priority		
3	3	0	5	5	2	0	1019	Connection 5	VC UNI	UBR	&	
3	3	0	16	5	2	0	1018	Connection 16	VC UNI	UBR	&	
3	3	0	18	5	2	0	1017	Connection 18	VC UNI	UBR	&	
3	3	0	32	5	2	1	402		VC UNI	UBR	*	
3	3	0	33	5	2	1	405		VC UNI	UBR	*	
3	3	0	34	5	3	1	401		VC UNI	UBR	*	
3	3	0	35	5	3	1	403		VC UNI	UBR	*	
3	3	0	36	5	3	1	404		VC UNI	UBR	*	
3	3	1	401	5	3	0	34	Connection 401	VC UNI	UBR	@	
3	3	1	403	5	3	0	35	Connection 403	VC UNI	UBR	@	
3	3	1	404	5	3	0	36	csm_conn	VC UNI	UBR	@	

The **vvv -v** command variable provides a verbose option, which appears similar to the display shown below:

For example, if you wanted to use the verbose option to view status information for port 3 on the CSM module in slot 3, you would enter:

vvv 3/3 -v

This command displays a screen similar to the following:

```

+ ==> PVC Connections
# ==> MPLS Connections
* ==> SVC Connections which cannot be modified by the user
@ ==> Soft PVC Connections
& ==> Control Connections
    
```

CSM Connections

Incoming				Outgoing				Connection Description	Chan Type	Transport Priority
Slot	Port	VPI	VCI	Slot	Port	VPI	VCI			
3	3	0	5	5	2	0	1019	Connection 5	VC UNI UBR	&
3	3	0	16	5	2	0	1018	Connection 16	VC UNI UBR	&
3	3	0	18	5	2	0	1017	Connection 18	VC UNI UBR	&
3	3	0	32	5	2	1	402		VC UNI UBR	*
3	3	0	33	5	2	1	405		VC UNI UBR	*
3	3	0	34	5	3	1	401		VC UNI UBR	*
3	3	0	35	5	3	1	403		VC UNI UBR	*
3	3	0	36	5	3	1	404		VC UNI UBR	*
3	3	1	401	5	3	0	34	Connection 401	VC UNI UBR	@
3	3	1	403	5	3	0	35	Connection 403	VC UNI UBR	@
3	3	1	404	5	3	0	36	csm_conn	VC UNI UBR	@

Slot	Port	VPI	VCI	Port Status	User Pri.	Statistics Mode
3	3	0	5	UP	15	CntGcra, PsCell
3	3	0	16	UP	15	CntGcra, PsCell
3	3	0	18	UP	15	CntGcra, PsCell
3	3	0	32	UP	15	CntGcra, PsCell
3	3	0	33	UP	15	CntGcra, PsCell
3	3	0	34	UP	15	CntGcra, PsCell
3	3	0	35	UP	15	CntGcra, PsCell
3	3	0	36	UP	15	CntGcra, PsCell
3	3	1	401	UP	15	CntGcra, PsCell
3	3	1	403	UP	15	CntGcra, PsCell
3	3	1	404	UP	15	CntGcra, PsCell

Tx Traffic Information

Slot	Port	VPI	VCI	Tx Traffic		Peak Cell Rate	Sustain Cell Rate	Maximum Burst Sz	Tx QoS	Best Effort
3	3	0	5	NoCLP	NoSCR	589			Uns	False
3	3	0	16	NoCLP	NoSCR	589			Uns	False
3	3	0	18	NoCLP	NoSCR	589			Uns	False
3	3	0	32	NoCLP	NoSCR	353207			Uns	True
3	3	0	33	NoCLP	NoSCR	353207			Uns	True
3	3	0	34	NoCLP	NoSCR	353207			Uns	True
3	3	0	35	NoCLP	NoSCR	353207			Uns	True
3	3	0	36	NoCLP	NoSCR	353207			Uns	True
3	3	1	401	NoCLP	NoSCR	1000			Uns	True
3	3	1	403	NoCLP	NoSCR	1000			Uns	True
3	3	1	404	NoCLP	NoSCR	1000			Uns	True

— Output continues on next page —

Viewing Virtual Connections

Rx Traffic Information

Slot	Port	VPI	VCI	Rx Traffic Descrip Type	Peak Cell Rate	Sustain Cell Rate	Maximum Burst Sz	Rx QoS	Best Effort
3	3	0	5	NoCLP NoSCR	589			Uns	False
3	3	0	16	NoCLP NoSCR	589			Uns	False
3	3	0	18	NoCLP NoSCR	589			Uns	False
3	3	0	32	NoCLP NoSCR	353207			Uns	True
3	3	0	33	NoCLP NoSCR	353207			Uns	True
3	3	0	34	NoCLP NoSCR	353207			Uns	True
3	3	0	35	NoCLP NoSCR	353207			Uns	True
3	3	0	36	NoCLP NoSCR	353207			Uns	True
3	3	1	401	NoCLP NoSCR	1000			Uns	True
3	3	1	403	NoCLP NoSCR	1000			Uns	True
3	3	1	404	NoCLP NoSCR	1000			Uns	True

Multicast

Slot	Port	VPI	VCI	gcra a enf mode	gcra a enf mode	grp id	enable	ingrs / egrss
3	3	0	5	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	16	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	18	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	32	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	33	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	34	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	35	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	0	36	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	1	401	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	1	403	no cong dx clpl	no cong dx clpl	4095	disable	ingress
3	3	1	404	no cong dx clpl	no cong dx clpl	4095	disable	ingress

Slot	Port	VPI	VCI	AAL5 Discard	Cdv	Bidir Traffic
3	3	0	5	Disabled	1000	On
3	3	0	16	Disabled	1000	On
3	3	0	18	Disabled	1000	On
3	3	0	32	Disabled	1000	On
3	3	0	33	Disabled	1000	On
3	3	0	34	Disabled	1000	On
3	3	0	35	Disabled	1000	On
3	3	0	36	Disabled	1000	On
3	3	1	401	Disabled	1000	On
3	3	1	403	Disabled	1000	On
3	3	1	404	Disabled	1000	On

Descriptions of the columns included in this display are described earlier in *Viewing Virtual Connections* on page 41-82.

Information on One Virtual Path

To view status information on a single virtual path, you enter the **vcv** command along with the slot number for the CSM board, the port number, and the VPI number for the virtual path on which you want information, as follows:

```
vcv <slot>/<port> <vpi>
```

where **<slot>** is the slot number where the CSM board is installed, **<port>** is the port number on the CSM board, and **<vpi>** is the virtual path identifier. For example, if you wanted to view status information for the board in slot 3, port 3, VPI 0, you would enter:

```
vcv 3/3 0
```

This command displays a screen similar to the following:

```
+ ==> PVC Connections
# ==> MPLS Connections
* ==> SVC Connections which cannot be modified by the user
@ ==> Soft PVC Connections
& ==> Control Connections
```

CSM Connections

Incoming				Outgoing				Connection Description	Chan Type	Transport Priority
Slot	Port	VPI	VCI	Slot	Port	VPI	VCI			
3	1	0	5	2	2	0	1019	Connection 5	VC UNI	UBR &
3	1	0	16	2	2	0	1018	Connection 16	VC UNI	UBR &
3	1	0	18	2	2	0	1017	Connection 18	VC UNI	UBR &
3	1	0	32	2	2	1	402	Connection 32	VC UNI	UBR *
3	1	0	33	2	2	1	405	Connection 33	VC UNI	UBR *
3	1	0	34	2	3	1	401	Connection 34	VC UNI	UBR *
3	1	0	35	2	3	1	403	Connection 35	VC UNI	UBR *
3	1	0	36	2	3	1	404	Connection 36	VC UNI	UBR *

The **vcv -v** command variable provides a verbose option, which appears similar to the display shown below:

For example, if you wanted to use the verbose option to view status information for the CSM board in slot 3, port 3, VPI 0, you would enter:

```
vcv 3/3 0 -v
```

This command displays a screen similar to the following:

```
+ ==> PVC Connections
# ==> MPLS Connections
* ==> SVC Connections which cannot be modified by the user
@ ==> Soft PVC Connections
& ==> Control Connections
```

CSM Connections

Incoming				Outgoing				Connection Description	Chan Type	Transport Priority
Slot	Port	VPI	VCI	Slot	Port	VPI	VCI			
3	1	0	5	2	2	0	1019	Connection 5	VC UNI	UBR &
3	1	0	16	2	2	0	1018	Connection 16	VC UNI	UBR &
3	1	0	18	2	2	0	1017	Connection 18	VC UNI	UBR &
3	1	0	32	2	2	1	402	Connection 32	VC UNI	UBR *
3	1	0	33	2	2	1	405	Connection 33	VC UNI	UBR *
3	1	0	34	2	3	1	401	Connection 34	VC UNI	UBR *
3	1	0	35	2	3	1	403	Connection 35	VC UNI	UBR *
3	1	0	36	2	3	1	404	Connection 36	VC UNI	UBR *

— Output continues on next page —

Viewing Virtual Connections

Slot	Port	VPI	VCI	Port Status	User Pri.	Statistics Mode
3	1	0	5	UP	15	CntGcra, PsCell
3	1	0	16	UP	15	CntGcra, PsCell
3	1	0	18	UP	15	CntGcra, PsCell
3	1	0	32	UP	15	CntGcra, PsCell
3	1	0	33	UP	15	CntGcra, PsCell
3	1	0	34	UP	15	CntGcra, PsCell
3	1	0	35	UP	15	CntGcra, PsCell
3	1	0	36	UP	15	CntGcra, PsCell

Tx Traffic Information

Slot	Port	VPI	VCI	Tx Traffic Descrip Type	Peak Cell Rate	Sustain Cell Rate	Maximum Burst Sz	Tx QoS	Best Effort
3	1	0	5	NoCLP NoSCR	589			Uns	True
3	1	0	16	NoCLP NoSCR	589			Uns	True
3	1	0	18	NoCLP NoSCR	589			Uns	True
3	1	0	32	NoCLP NoSCR	353208			Uns	True
3	1	0	33	NoCLP NoSCR	353208			Uns	True
3	1	0	34	NoCLP NoSCR	353208			Uns	True
3	1	0	35	NoCLP NoSCR	353208			Uns	True
3	1	0	36	NoCLP NoSCR	353208			Uns	True

Rx Traffic Information

Slot	Port	VPI	VCI	Rx Traffic Descrip Type	Peak Cell Rate	Sustain Cell Rate	Maximum Burst Sz	Rx QoS	Best Effort
3	1	0	5	NoCLP NoSCR	589			Uns	True
3	1	0	16	NoCLP NoSCR	589			Uns	True
3	1	0	18	NoCLP NoSCR	589			Uns	True
3	1	0	32	NoCLP NoSCR	353208			Uns	True
3	1	0	33	NoCLP NoSCR	353208			Uns	True
3	1	0	34	NoCLP NoSCR	353208			Uns	True
3	1	0	35	NoCLP NoSCR	353208			Uns	True
3	1	0	36	NoCLP NoSCR	353208			Uns	True

— Output continues on next page —

										----- Multicast -----				
Slot	Port	VPI	VCI	gcra a enf mode			gcra a enf mode			grp id	enable	ingrs / egrss		
====	====	====	====	=====	=====	=====	=====	=====	=====	=====	=====	=====		
3	1	0	5	no	cong	dx	clpl	no	cong	dx	clpl	4095	disable	ingress
3	1	0	16	no	cong	dx	clpl	no	cong	dx	clpl	4095	disable	ingress
3	1	0	18	no	cong	dx	clpl	no	cong	dx	clpl	4095	disable	ingress
3	1	0	32	no	cong	dx	clpl	no	cong	dx	clpl	4095	disable	ingress
3	1	0	33	no	cong	dx	clpl	no	cong	dx	clpl	4095	disable	ingress
3	1	0	34	no	cong	dx	clpl	no	cong	dx	clpl	4095	disable	ingress
3	1	0	35	no	cong	dx	clpl	no	cong	dx	clpl	4095	disable	ingress
3	1	0	36	no	cong	dx	clpl	no	cong	dx	clpl	4095	disable	ingress

Slot	Port	VPI	VCI	AAL5 Discard	Cdv	Bidir Traffic
====	====	====	====	=====	=====	=====
3	1	0	5	Disabled	1000	On
3	1	0	16	Disabled	1000	On
3	1	0	18	Disabled	1000	On
3	1	0	32	Disabled	1000	On
3	1	0	33	Disabled	1000	On
3	1	0	34	Disabled	1000	On
3	1	0	35	Disabled	1000	On
3	1	0	36	Disabled	1000	On

Descriptions of the columns included in this display are described earlier in *Viewing Virtual Connections* on page 41-82.

Information on One Virtual Channel

To view status information on a single virtual channel, you enter the **vcv** command along with the slot number for the CSM board, the port number, the VPI number, and VCI number for the virtual path on which you want information, as follows:

vcv <slot>/<port> <vpi>/<vci>

where **<slot>** is the slot number where the CSM board is installed, **<port>** is the port number on the CSM board, **<vpi>** is the virtual path identifier, and **<vci>** is the virtual channel identifier. For example, if you wanted to view status information for the board in slot 3, port 3, VPI 0, and VCI 5, you would enter:

vcv 3/3 0/5

This command displays a screen similar to the following:

```
+ ==> PVC Connections
# ==> MPLS Connections
* ==> SVC Connections which cannot be modified by the user
@ ==> Soft PVC Connections
& ==> Control Connections
```

CSM Connections

Incoming				Outgoing				Connection Description	Chan Type	Transport Priority
Slot	Port	VPI	VCI	Slot	Port	VPI	VCI			
3	1	0	100	2	1	0	100	Connection 100	VC UNI	UBR +

The **vcv -v** command variable provides a verbose option, which appears similar to the display shown below:

For example, if you wanted to use the verbose option to view status information for the CSM board in slot 3, port 3, VPI 0, and VCI 5, you would enter:

vcv 3/3 0/5 -v

This command displays a screen similar to the following:

```
+ ==> PVC Connections
# ==> MPLS Connections
* ==> SVC Connections which cannot be modified by the user
@ ==> Soft PVC Connections
& ==> Control Connections
```

CSM Connections

Incoming				Outgoing				Connection Description	Chan Type	Transport Priority
Slot	Port	VPI	VCI	Slot	Port	VPI	VCI			
3	1	0	100	2	1	0	100	Connection 100	VC UNI	UBR &

Slot	Port	VPI	VCI	Port Status	User Pri.	Statistics Mode
3	1	0	100	UP	15	CntGcra, PsCell

Tx Traffic Information

Slot	Port	VPI	VCI	Tx Traffic Descrip Type		Peak Cell Rate	Sustain Cell Rate	Maximum Burst Sz	Tx QoS	Best Effort
3	1	0	100	NoCLP	NoSCR	353208			Uns	True

— Output continues on next page —

Rx Traffic Information														
Slot	Port	VPI	VCI	Rx Traffic		Peak	Sustain	Maximum	Rx	Best				
====	====	====	====	Descrip Type		Cell Rate	Cell Rate	Burst Sz	QoS	Effort				
====	====	====	====	=====	=====	=====	=====	=====	====	=====				
3	1	0	100	NoCLP	NoSCR	353208			Uns	True				
----- Multicast -----														
Slot	Port	VPI	VCI	gkra	a	enf	mode	gkra	a	enf	mode	grp id	enable	ingrs / egrss
====	====	====	====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====
3	1	0	100	no	cong	dx	clpl	no	cong	dx	clpl	4095	disable	ingress
Slot	Port	VPI	VCI	AAL5 Discard		Cdv	Bidir Traffic							
====	====	====	====	=====		=====	=====							
3	1	0	100	Disabled		1000	On							

Descriptions of the columns included in this display are described earlier in *Viewing Virtual Connections* on page 41-82.

Displaying the Number of ATM Connections on a Switch

You use the **vnac** command to display the total number of ATM connections on a switch. To use this command, enter:

vnac

at the system prompt. A screen similar to the following will be displayed:

Current number of atm connections = 0

To display the total number of Point-to-Multipoint connections on a switch, use the **vnapc** command. To use this command, enter:

vnapc

at the system prompt. A screen similar to the following will be displayed:

Current number of atm PTOMP connections = 0

42 Advanced CSM Management

This chapter covers the following advanced software features for CSMs:

Configuring and Monitoring Soft PVCs

Soft PVCs, like PVCs but unlike SVCs, must be configured by the user. Soft PVCs differ from PVCs because they do not use static routes. If a link fails, a Soft PVC will reroute its path and will not go down.

This chapter describes User Interface (UI) commands for Soft PVCs. The **scvc** command, which is described in *Creating a Soft PVC* on page 42-3, is used to configure Soft PVCs. The **svvc** command, which is described in *Viewing Soft PVCs* on page 42-21, is used to display Soft PVC parameters.

Configuring and Monitoring Virtual Path (VP) Tunneling

You can create multiple UNI or NNI instances on a CSM physical port through the use of virtual path (VP) tunneling (see *Virtual UNI/NNI Using Virtual Path (VP) Tunneling* on page 42-24). VP tunneling can be used in many applications, including extending a Private Network-to-Network Interface (PNNI) network over a public ATM network.

UI commands to create, modify, display, and delete VP tunnels are described in this chapter. The **cvpt** command, which is described in *Creating a VP Tunnel* on page 42-26, is used to create a VP tunnel. Information is also included on tunnel shaping for OC-3 daughtercards, including Priority and Bandwidth Limitation options for CSM-ABT-155F daughtercards. The **lvpt** command, which is used to display VP tunnel parameters, is described in *Displaying VP Tunnel Information* on page 42-30. The **mvpt** command, which is used to modify VP tunnel parameters, is described in *Modifying a VP Tunnel* on page 42-35. And the **dvpt** command, which is described in *Deleting a VP Tunnel* on page 42-35, is used to delete a VP tunnel.

Configuring a LECS ATM Address

The **masrt** command, which is used to configure a LANE Configuration Server (LECS) ATM address, is described in *Configuring a LECS ATM Address* on page 42-36.

Viewing ATM Layer Statistics

The **vls** command, which is described in *Viewing ATM Layer Statistics* on page 42-39, is used to display ATM layer statistics tables for CSM and ATM access ports. And the **vlrs** command, which is described in *Viewing ATM Layer Receive Error Statistics* on page 42-41, is used to display ATM layer receive error statistics for CSM and ATM access ports.

Viewing ATM Connection Statistics

The **vcs** command, described in *Viewing ATM Connection Statistics Table* on page 42-46, is used to display ATM connection statistics for CSM and ATM access ports. The **vcst** command, which is described in *Viewing CSM Port and Connection Statistics* on page 42-51, can be used to display port and connection statistics for a CSM port or for a connection on a specific port. And the **vcrs** command, which is described in *Viewing Connection Receive Error Statistics* on page 42-54, is used to display ATM receive connection statistics for CSM and ATM access ports.

Intelligent Multicast Replication

An overview of intelligent multicast replication is provided in *Intelligent Multicast Replication* on page 42-56. Descriptions of UI commands to enable, disable, display performance gain, and to display the intelligent multicast replication tree begin on page 42-59.

CSM-ABT Traffic Shaping

An overview of CSM Traffic Shaping is provided on *CSM-ABT Traffic Shaping* on page 42-64. Instructions on using CLI commands to activate, configure and apply CSM Traffic Shaping enforcement are provided in *Using the CLI to Configure CSM Traffic Shaping* on page 42-65. For examples of these commands, see *Traffic Shaping Configuration Examples* on page 42-67.

◆ Important Notes ◆

In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. Chapter 8, “The User Interface,” includes documentation on changing from CLI mode to UI mode.

For basic UI commands to configure CSM ports and to create and modify PVCs, see Chapter 41, “Managing Cell Switching Modules (CSMs).”

Soft PVCs

The OmniSwitch supports “soft PVCs.” Soft PVCs must be configured like standard PVCs, but they are brought up on-the-fly and use PNNI signaling like SVCs. Configuration data for soft PVCs is stored in flash memory; if the OmniSwitch is restarted, data for the soft PVCs still exists.

Creating a Soft PVC

The **scvc** command allows you to create a soft PVC for a physical port and logical VPI or VPI/VCI that you specify. The **scvc** command contains several suboptions for configuring multi-cast virtual circuits and traffic contract parameters. Many of the options in the **scvc** command are the same as those used in the **cvc** command. For example, traffic parameters, priority, and statistics control are configured the same in both commands. The central difference between configuring a PVC and a soft PVC is that a soft PVC requires destination port information.

To begin setting up a soft PVC, enter **scvc** followed by the slot number, a slash (/), and the port number where you want to set up the soft PVC. After the slot and port number, leave a space, then specify the Virtual Path Identifier (VPI), a slash (/), and then the Virtual Channel Identifier (VCI). (You do not have to include the VCI if you are setting up a Virtual Path only.) For example, the following command specifies a soft PVC with a VCI of 200, and VPI of 1 on the first port on the module in slot 5:

```
scvc 5/1 1/200
```

Note that these values indicate the *input* port and *input* VPI/VCI for the soft PVC on this OmniSwitch. Output parameters are specified later through **scvc** screen options.

The following message displays for a moment

```
creating csm connection, please wait .....
```

This initial message will be followed by a screen of options similar to the following:

```
Slot 5 Port 1 Connection VPI 1 VCI 200 Configuration
  Available bandwidth: Tx=353209 Rx=353209
 1) Description (30 chars max      : Connection 200
 2) End point Id (1..65535)       : 1
 3) Terminating ATM Address      : 00000000000000000000000000000000
 4) Other End VPI (0..4095)       : 1
 5) Other End VCI (0..65535)      : 1
 6) Channel Type { vc-nni(3), vc-uni(4) } : VC-UNI
 7) Transport Priority { CBR(1), CBR_PRS(2), VBR_RT(3), : UBR
   VBR_NRT(4), ABR(5), UBR(6) }
 8) Point to Multipoint { disable(0), enable(1) } : disabled
 9) Channel Redirect { not allowed(0), allowed(1) } : not allowed
10) AAL5 Discard Continue { disable(0), enable(1) } : enable

11) Traffic Parameters
13) Advanced Parameters
14) Target Selector Type { required(1), any(2) } : required
15) SoftPvc Retry parameters
16) Broadband Bearer Capability Parameters

Enter (option=value/save/cancel) :
```

You make changes by entering the line number for the option you want to change, an equal sign (=), and then the value for the new parameter. When you are done entering all new values, type **save** at the colon prompt (:) and all new parameters will be saved. The following sections describe the options you can alter through this menu.

1) Description

A textual description of this virtual circuit. You can use up to 30 characters to describe a virtual circuit. For example, if this soft PVC will be used primarily to carry traffic for multimedia workstations, you may want to describe the circuit as "Multimedia VC."

2) End point Id

An identification number used to keep track of the endpoints within a single soft PVC. This number is used for identification purposes only and does not affect VPI/VCI numbering.

3) Terminating ATM Address

The ATM address of the output port of the ATM switch at the other end of this soft PVC.

4) Other End VPI

The Virtual Path Identifier (VPI) used for this circuit on the ATM switch at the other end of this soft PVC connection. This VPI is not the same one you specified in the **scvc** command line; the VPI specified in the **scvc** command line is the input VPI used on this OmniSwitch. The **Other End VPI** is the VPI used at the destination end of this soft PVC. This field will not display if the **Target Selector Type** field is set to **Any**.

5) Other End VCI

The Virtual Channel Identifier (VCI) used for this circuit on the ATM switch at the other end of this soft PVC connection. This VCI is not the same one you specified in the **scvc** command line. The VCI specified in the **scvc** command line is the input VCI used on this OmniSwitch. The **Other End VCI** is the VCI used at the destination end of this soft PVC. This field will not display if you are not setting up a Virtual Channel Connection (VCC) or if the **Target Selector Type** field is set to **Any**.

6) Channel Type

The type of connection supported by this channel. Normally, this circuit will connect to a user device, such as an ATM workstation, or to another network switch, such as an OmniSwitch. When connected directly to a user device, this connection would be considered a UNI connection (option 4). When connected to another ATM switch, this connection would be considered an NNI connection (option 3).

7) Transport Priority

Indicates the type of traffic and its priority on this connection. Some traffic types require higher priority than others because any disruption in the connection will cause unacceptable results. For example, a circuit emulating a private digital line requires a continuous flow of traffic. Circuit emulation requires Continuous Bit Rate (CBR) transport and is given a higher priority than other less sensitive traffic. On the other hand, data connections can tolerate some delay in the connection. Data traffic usually requires Available Bit Rate (ABR) transport.

◆ Note ◆

This parameter is not available if you are running the multiple peer group version of the PNNI software (i.e., you are using the **cell_mpg.img** file instead of **cell.img**.) See *Configuring Transport Priority with the Multiple-Peer Group Software* on page 42-19 for more information.)

When you set this option, the Class of Service and priority level of the circuit are automatically selected in **scvc** submenus. The following options are available:

CBR	Continuous Bit Rate
CBR_PRS	Continuous Bit Rate with Primary Reference Source
VBR_RT	Variable Bit Rate, Real Time
VBR_NRT	Variable Bit Rate, Non-Real Time
ABR	Available Bit Rate
UBR	Unspecified Bit Rate

Screen numbering for **Transport Priority** indicates the priority level of traffic except in the case of the two CBR traffic types: CBR_PRS (option 2) is given a higher priority than standard CBR traffic (option 1).

8) Point to Multipoint

Enables multicast, or point-to-multipoint, soft PVCs on this primary virtual circuit. If you enable multicast support, you will receive additional prompts to indicate additional information for the multicast virtual circuits. Multicast virtual circuits are leaves of the primary, or root, virtual circuit. In addition, multicast virtual circuits inherit QoS and traffic parameters from the root virtual circuit. See Chapter 41, “Managing Cell Switching Modules (CSMs),” for more information on multicast circuits. The steps for setting up individual point-to-multipoint virtual circuits for soft PVCs are described later in *Configuring Point-to-Multipoint Soft PVCs* on page 42-15.

9) Channel Redirect

Indicates whether data in this channel will be redirected to another channel if this channel goes down.

10) AAL5 Discard Continue

Indicates how AAL5 PDU cells are discarded. Configuration of this option varies, depending on the following two factors:

1. The **Transport Priority** value entered in option 7. CBR, CBR_PRS, and VBR_RT traffic types do not carry AAL5 PDU cells and are therefore not configurable for AAL5 Discard. See 7) *Transport Priority* on page 42-4 for available traffic types.
2. The IOP chip version on the CSM board where you are creating a virtual circuit. The IOP (Input Output Processor) chip is a cell routing engine on CSM boards. IOP1, the older chip version does not support Early Packet Discard (EPD) and Partial Packet Discard (PPD). IOP2, the newer chip version, supports EPD and PPD for UBR, VBR_NRT, and ABR traffic types.

You can view AAL5 Discard configurations on a virtual circuit through the **vc** command. The following describes the possible displays for the AAL5 Discard field:

- If an older chip version (IOP1) is installed, option 10 displays as follows for all **Transport Priority** values:

10) AAL5 Discard Continue {disable (0), enable (1)} : disabled

Enabling AAL5 Discard (which also enables “Partial Packet Discard”) increases overall frame throughput for AAL5 traffic during times of congestion. The default for this option is disabled.

- If a newer chip version (IOP2) is installed and UBR, VBR_NRT, or ABR is the **Transport Priority** traffic type entered in option 7, the screen displays as follows:

10) AAL5 Discard { Disable (0), EPD (1), PPD (2)} :EPD

Descriptions of these options are as follows:

◆ **Important Note** ◆

Policing will fail if Early Packet Discard (EPD) or Partial Packet Discard (PPD) is enabled. See Chapter 41, “Managing Cell Switching Modules (CSMs),” to change the default setting for AAL5 discards on CSMs with the IOP2 ASIC from EPD to disabled.

Disable (0). Enter **0** to randomly discard cells associated with AAL5 PDU during congestion conditions. Cells are marked when the GCRA contract is violated.

EPD (1). Enter **1** to enable EPD (Early Packet Discard). EPD allows the switch to selectively discard cells associated with AAL5 PDU during congestion conditions. In this mode, the cells of the whole packet are either passed or discarded. At congestion time, if the first cell of a packet has already passed, then the rest of the packet will be passed. When congestion ends, the first cell of a new packet will be passed. Cells are marked when the GCRA contract has been violated.

PPD (2). Enter **2** to enable PPD (Partial Packet Discard). PPD allows the switch to selectively discard cells associated with AAL5 PDU during congestion conditions. In this mode, the cells of the rest of the packet—except for the very last cell—are discarded. When congestion ends, the first cell of a new packet will be passed. Cells are marked when the GCRA contract is violated.

- If a newer chip version (IOP2) is installed and VBR_RT, CBR, or CBR_PRS is the **Transport Priority** traffic type entered in option 7, the screen displays as follows:

10) AAL5 Discard : Disabled

CBR, CBR_PRS, and VBR_RT traffic types do not carry AAL5 PDU cells and are therefore not configurable for AAL5 Discard. The **AAL5 Discard** option for these traffic types remains at the default value of **disabled**.

11) Traffic Parameters

This option enters a screen of suboptions for configuring traffic descriptors and Quality of Service parameters. This screen and its options are described later in *Configuring Traffic Parameters* on page 42-8.

13) Advanced Parameters

This option enters a screen of suboptions for configuring the priority level for this circuit and for controlling statistics output. This screen and its options are described later in *Configuring Statistics and Priority Parameters* on page 42-14.

14) Target Selector Type

Indicates whether you want the destination ATM switch to choose the VPI and VPI/VCI values or if you want to specify these values manually. **Required** means that you must specify **Other End VPI** and/or **Other End VCI** values. **Any** means the destination switch will select the VPI and VPI/VCI values; when **Any** is selected, the **Other End VPI** and **Other End VCI** fields will not display.

15) SoftPvc Retry parameters

This option displays a screen of sub-options for soft PVC retry parameters, such as Retry Interval and Retry Threshold. This screen and its options are described later in *Configuring Soft PVC Retry Parameters* on page 42-18.

16) Broadband Bearer Capability Parameters

This option displays a screen of suboptions for additional soft PVCs parameters. This screen's options are described in *Configuring Broadband Bearer Capability Parameters* on page 42-18.

Configuring Traffic Parameters

The **scvc** command contains a sub-option for configuring traffic parameters, such as traffic descriptors and Quality of Service (QoS) parameters. Option 11 on the main **scvc** screen provides the link to this submenu. Enter **11** at the **Enter** prompt at the bottom of the main **scvc** screen and you will see the following screen of sub-options:

Slot 5 Port 1 Connection VPI 2 VCI 200 Configuration

Available bandwidth: Tx=353210 Rx=353210

- | | |
|---|---------------|
| 1) Requested Tx QoS Class { Unspecified(0), Class1(1), Class2(2), Class3(3), Class4(4) } | : Class 3 |
| 2) Requested TX Best Effort { False (1), True (2) } | : False |
| 3) Requested Tx Traffic Descriptor Type { None(1), NoCLPNoSCR(2), CLPNoTagNoSCR(3), CLPNoTagSCR(4), NoCLPSCR(5), CLPNoTagSCR(6), CLPNoTagSCR(7) } | : CLP Tag SCR |
| 20) Peak Cell Rate (cells/sec) for CLP=0+1 | : 3 |
| 21) Sustaining Cell Rate (cells/sec) for CLP=0 | : 2 |
| 22) Maximum Burst Rate (cells) for CLP=0 | : 1 |
| 4) Requested Rx QoS Class | : Class 3 |
| 5) Requested RX Best Effort { False (1), True (2) } | : False |
| 6) Requested Rx Traffic Descriptor Type | : CLP Tag SCR |
| 30) Peak Cell Rate (cells/sec) for CLP=0+1 | : 3 |
| 31) Sustaining Cell Rate (cells/sec) for CLP=0 | : 2 |
| 32) Maximum Burst Rate (cells) for CLP=0 | : 1 |
| 7) Bi-directional Traffic Params { Off (1), On (2) } | : On |

Enter (option=value/save/cancel) :

The following sections describe the options on this screen.

1) Requested Tx QoS Class

The Quality of Service (QoS) for cells transmitted (from source to destination) on this VPI or VPI/VCI. The QoS can be Unspecified (0), Class 1 (1), Class 2 (2), Class 3 (3), or Class 4 (4). Each of these five classes is described in Chapter 41, “Managing Cell Switch Modules (CSMs),” and they are listed below. The QoS Class that you select affects the priority of this Virtual Circuit and the Generic Cell Rate Algorithm (GCRA) used to police traffic. See Chapter 41, “Managing Cell Switch Modules (CSMs),” for more information on the interaction of QoS and GCRA.

- | | |
|--------------------|---|
| Unspecified | Best Effort for data traffic (UBR) |
| Class 1 | Circuit Emulation, Constant Bit Rate Traffic (CBR) |
| Class 2 | Variable Bit Rate for Real Time Audio and Video Traffic (rt-VBR) |
| Class 3 | VBR for Connection-Oriented Protocols Such as Frame Relay (nrt-VBR) |
| Class 4 | Available Bit Rate for Connectionless Data Protocols Such as IP (ABR) |

2) Requested Tx Best Effort

Indicates whether to use the Peak Cell Rate (PCR) setting—specified later in this procedure—to determine the amount of bandwidth allocated or to use all available bandwidth. Setting this field to **True** specifies this circuit to use all available bandwidth. Setting this field to **False** specifies the circuit to use the PCR to determine the amount of bandwidth; if bandwidth is not available to support the PCR then this connection will be disabled.

3) Requested Tx Traffic Descriptor Type

The traffic descriptor bundle to be used with this Class of Service. The traffic descriptor bundle you choose here determines which traffic parameters you will specify. The traffic parameters will include the Peak Cell Rate (PCR) and may also include the Sustained Cell Rate (SCR) and Maximum Burst Size (MBS). Each traffic descriptor bundle available is described in Chapter 41, “Managing Cell Switch Modules (CSMs).”

The traffic descriptor along with the Class of Service you choose determines the Generic Cell Rate Algorithm (GCRA), or “leaky bucket,” that will be used to police this connection. See Chapter 41, “Managing Cell Switch Modules (CSMs),” for more information on the relationship between Class of Service, traffic descriptors, and GCRA. The following traffic descriptor bundles and prompts are available:

None No traffic enforcement imposed. No prompts for any traffic parameters.

NoCLPNoSCR Prompts for the Peak Cell Rate (PCR). Option 20 will display as follows:

```
3) Requested Tx Traffic Descriptor Type { None (1),           : NoCLP NoSCR
    NoCLPNoSCR (2), CLPNoTagNoSCR (3) CLPtagNoSCR (4),
    NoCLPSCR (5), CLPNo tagSCR (6), CLPtagSCR (7) }
20) Peak Cell Rate (cells/sec) for CLP=0+1                 : 3
```

The PCR will be checked on the aggregate of CLP=0 and CLP=1 traffic. Both the minimum and default setting for PCR is 3 cells per second.

CLPNoTagNoSCR Prompts for the Peak Cell Rate (PCR). Options 20 and 21 will display as follows:

```
3) Requested Tx Traffic Descriptor Type { None (1),           : CLP NoTag
NoSCR
    NoCLPNoSCR (2), CLPNoTagNoSCR (3) CLPtagNoSCR (4),
    NoCLPSCR (5), CLPNo tagSCR (6), CLPtagSCR (7) }
20) Peak Cell Rate (cells/sec) for CLP=0+1                 : 3
21) Peak Cell Rate (cells/sec) for CLP=0                   : 3
```

The PCR will be checked on the aggregate of CLP=0 and CLP=1 (CLP=0+1) traffic and separately on CLP=0 traffic. The default setting for PCR on CLP=0+1 traffic is 3 cells per second. The default setting for PCR on CLP=0 traffic is 3 cells per second.

CLPtagNoSCR Prompts for the Peak Cell Rate (PCR). Options 20 and 21 will display as follows:

- 3) Requested Tx Traffic Descriptor Type { None (1), : CLP_Tag_NoSCR
 NoCLPNoSCR (2), CLPNoTagNoSCR (3) CLPtagNoSCR (4),
 NoCLPSCR (5), CLPNo tagSCR (6), CLPtagSCR (7) }
- 20) Peak Cell Rate (cells/sec) for CLP=0+1 : 3
- 21) Peak Cell Rate (cells/sec) for CLP=0 : 3

The PCR will be checked on the aggregate of CLP=0 and CLP=1 (CLP=0+1) traffic and separately on CLP=0 traffic. The default setting for PCR on CLP=0+1 traffic is 3 cells per second. The default setting for PCR on CLP=0 traffic is 3 cells per second.

NoCLPSCR Prompts for the Peak Cell Rate (PCR), Sustained Cell Rate (SCR), and Maximum Burst Size (MBS). Options 20, 21, and 22 displays as follows:

- 3) Requested Tx Traffic Descriptor Type { None (1), : NoCLP SCR
 NoCLPNoSCR (2), CLPNoTagNoSCR (3) CLPtagNoSCR (4),
 NoCLPSCR (5), CLPNo tagSCR (6), CLPtagSCR (7) }
- 20) Peak Cell Rate (cells/sec) for CLP=0+1 : 3
- 21) Sustaining Cell Rate (cells/sec) for CLP=0+1 : 2
- 22) Maximum Burst Size : 1

The PCR will be checked on the aggregate of CLP=0 and CLP=1 (CLP=0+1) traffic. The default setting for PCR is 3 cells per second. The SCR will be checked on the aggregate of CLP=0 and CLP=1 traffic. Both the minimum value and the default setting for SCR is 2 cells per second. SCR must be less than PCR. The MBS will be checked on the aggregate of CLP=0+1 traffic. The MBS default setting is 1 cell.

CLPNoTagSCR Prompts for the Peak Cell Rate (PCR), Sustained Cell Rate (SCR), and Maximum Burst Size (MBS). Options 20, 21, and 22 will display as follows:

- 3) Requested Tx Traffic Descriptor Type { None (1), : CLP NoTag SCR
 NoCLPNoSCR (2), CLPNoTagNoSCR (3) CLPtagNoSCR (4),
 NoCLPSCR (5), CLPNo tagSCR (6), CLPtagSCR (7) }
- 20) Peak Cell Rate (cells/sec) for CLP=0+1 : 3
- 21) Sustaining Cell Rate (cells/sec) for CLP=0 : 2
- 22) Maximum Burst Size (cells) for CLP=0 : 1

The PCR will be checked on the aggregate of CLP=0 and CLP=1 (CLP=0+1) traffic. The default setting for PCR is 3 cells per second. The SCR will be checked on CLP=0 traffic. The default setting for SCR is 2 cells per second. The MBS will be checked on CLP=0 traffic; the MBS default setting is 1 cell.

CLPtagSCR Prompts for the Peak Cell Rate (PCR), Sustained Cell Rate (SCR), and Maximum Burst Size (MBS).

- 3) Requested Tx Traffic Descriptor Type { None (1), : CLP Tag SCR
NoCLPNoSCR (2), CLPNoTagNoSCR (3) CLPtagNoSCR (4),
NoCLPSCR (5), CLPNo tagSCR (6), CLPtagSCR (7) }
20) Peak Cell Rate (cells/sec) for CLP=0+1 : 3
21) Sustaining Cell Rate (cells/sec) for CLP=0 : 2
22) Maximum Burst Size (cells) for CLP=0 : 1

The PCR will be checked on the aggregate of CLP=0 and CLP=1 (CLP=0+1) traffic. The default setting for PCR is 3 cells per second. The SCR will be checked on CLP=0 traffic. The default setting for SCR is 2 cells per second. The MBS will be checked on CLP=0 traffic. The MBS default setting is 1 cell.

The following sections describe the traffic parameter prompts that display after you select a traffic descriptor bundle.

Peak Cell Rate

The following is a sample prompt display:

20) Peak Cell Rate (cells/sec) for CLP=0+1 : 3

In this field, you specify the Peak Cell Rate (PCR), in cells per second allowed on this VPI or VPI/VCI. The PCR is the fastest cell rate allowed on the connection. The switch will use this parameter as part of the traffic contract for this virtual circuit. A cell rate above the rate you indicate here will denote a violation of the traffic contract and the leaky bucket algorithm will determine which enforcement action take. Note that the PCR will be enforced on CLP=0+1 or CLP=0 cell flows; this prompt will indicate which cell flow is checked.

Sustaining Cell Rate

The following is a sample prompt display:

21) Sustaining Cell Rate (cells/sec) for CLP=0+1 : 2

In this field, you specify the Sustaining Cell Rate (SCR), in cells per second allowed on this VPI or VPI/VCI. The SCR is highest average cell rate allowed on the circuit. The switch will use the parameter as part of the traffic contract for this virtual circuit. An average cell rate above the rate you indicate here will denote a violation of the traffic contract and the leaky bucket algorithm will determine which enforcement action take. Note that the SCR will be enforced on CLP=0+1 or CLP=0 cell flows; this prompt indicates which cell flow is checked.

Maximum Burst Size

The following is a sample prompt display:

22) Maximum Burst Rate (cells) for CLP=0+1 : 1

In this field, you specify the Maximum Burst Size (MBS), in cells allowed on this VPI or VPI/VCI. The MBS is the largest single burst of cells allowed on the connection. The switch will use this parameter as part of the traffic contract for this virtual circuit. A burst size above the value you indicate here will denote a violation of the traffic contract and the leaky bucket algorithm will determine which enforcement action to take. Note that the MBS will be enforced on CLP=0+1 or CLP=0 cell flows; this prompt indicates which cell flow is checked.

4) Requested Rx QoS Class

The Quality of Service (QoS) for cells received from the destination at the source on this VPI or VPI/VCI. The QoS can be Unspecified (0), Class 1 (1), Class 2 (2), Class 3 (3), or Class 4 (4). Each of these five classes is described in Chapter 41, “Managing Cell Switch Modules (CSMs),” and they are listed below. The QoS Class that you select affects the priority of this Virtual Circuit and the Generic Cell Rate Algorithm (GCRA) used to police traffic. See Chapter 41, “Managing Cell Switch Modules (CSMs),” for more information on the interaction of QoS and GCRA.

Unspecified	Best Effort for data traffic (UBR)
Class 1	Circuit Emulation, Constant Bit Rate Traffic (CBR)
Class 2	Variable Bit Rate for Audio and Video Traffic (rt-VBR)
Class 3	VBR for Connection-Oriented Protocols Such as Frame Relay (nrt-VBR)
Class 4	Available Bit Rate for Connectionless Data Protocols Such as IP (ABR)

5) Requested Rx Best Effort

Indicates whether to use the Peak Cell Rate (PCR) setting—specified later in this procedure—to determine the amount of bandwidth allocated or to use all available bandwidth. Setting this field to **True** specifies this circuit to use all available bandwidth. Setting this field to **False** specifies the circuit to use the PCR to determine the amount of bandwidth; if bandwidth is not available to support the PCR then this connection will be disabled.

6) Requested Rx Traffic Descriptor Type

The traffic descriptor bundle to be used with this Class of Service. The traffic descriptor bundle you choose here determines which traffic parameters you will specify. The traffic parameters will include the Peak Cell Rate (PCR) and may also include the Sustained Cell Rate (SCR) and Maximum Burst Size (MBS). Each traffic descriptor bundle available is described in Chapter 41, “Managing Cell Switch Modules (CSMs).” In addition, please refer to *3) Requested Tx Traffic Descriptor Type* on page 42-9 for information on the traffic descriptor options included in this software option.

7) Bi-directional Traffic Params

Indicates whether you want to use the same traffic parameters for the transmit and receive sides of this virtual circuit. If you enter a **Yes** in this field then the Tx traffic parameters (fields 1 to 3) will match the Rx traffic parameters (fields 4 to 6).

Configuring Statistics and Priority Parameters

The **scvc** command contains a sub-option for configuring the Priority level and the statistics that display for this connection. Option 12 on the main **scvc** screen provides the link to this submenu. Enter **12** at the **Enter** prompt at the bottom of the main **scvc** screen and you will see the following screen of sub-options:

```

Slot 5 Port 1 Connection VPI 2 VCI 200 Configuration
Available bandwidth: Tx=353209 Rx=353209
1) User Priority (0-15)                : 4
2) CDV (10us-10000us)                 : 1000

```

Enter (option=value/save/cancel) :

The options in this screen are described below.

User Priority

The priority level assigned to this virtual circuit. This priority is used to decide which virtual circuit's traffic is discarded first in a situation where congestion occurs. The priority level for a virtual circuit can range from 0 to 15, with 0 being the highest priority and 15 being the lowest. A default value is supplied for User Priority based on the type of traffic you specified under the **Traffic Priority** option on the main **scvc** screen (Option 7). The following defaults are supplied for each traffic type:

Traffic Type and Priority

Traffic Type	Default Priority Level
CBR	4
VBR	8
ABR	8
UBR	15

You can fine tune these priorities through this option. For example, some CBR circuits can be given higher priority than other CBR circuits by assigning a User Priority of 1, 2, or 3 rather than CBR default of 4.

CDV

Cell Delay Variation in microseconds. Also referred to as "jitter," this value is the change that occurs in cell spacing from the time cells leave one node and arrive at another node.

Configuring Point-to-Multipoint Soft PVCs

While configuring a soft PVC through the **scvc** command, you can configure multicast circuits to be associated with the primary soft PVC. Multicast circuits are leaves of the root soft PVC and inherit its traffic properties. Cells on the root circuit are copied to all leaf circuits you specify. See Chapter 41, “Managing Cell Switching Modules (CSMs),” for more information on point-to-multipoint connections. Option 8 in the **scvc** command allows you to set up point-to-multipoint soft PVCs. Follow these steps:

1. At the bottom of the main **scvc** screen, you will find the following prompt.

Enter (option=value/save/cancel) :

Enter **8=1** at this prompt to enable multicast support on this soft PVC. The **scvc** screen re-displays with an additional option under the **Point to Multipoint** option, as follows.

Slot 5 Port 1 Connection VPI 1 VCI 300 Configuration

Available bandwidth: Tx=353209 Rx=353209

```

1) Description (30 chars max)      : Connection 300
2) End point Id (1..65535)        : 1
3) Terminating ATM Address       : 000000000000000000000000000000000000
4) Other End VPI (0..4095)        : 1
5) Other End VCI (0..65535)       : 1
6) Channel Type { vc-uni(3), vc-uni(4) } : VC-UNI
7) Transport Priority { CBR(1), CBR_PRS(2), VBR_RT(3), : UBR
   VBR_NRT(4), ABR(5), UBR(6) }
8) Point to Multipoint { disable(0), enable(1) } : enabled
   20) Add/Delete Point to Multipoint{ add(1), delete(2) }
9) Channel Redirect { not allowed(0), allowed(1) } : not allow
10) AAL5 Discard Continue { disable(0), enable(1) } : disable

11) Traffic Parameters
13) Advanced Parameters
14) Target Selector Type {required(1), any(2) } : any
15) Advanced SoftPvc parameters
16) Broadband Bearer Capability Parameters

```

Enter (option=value/save/cancel) :

2. Enter **20=1** at the **Enter** prompt to add a point-to-multipoint soft PVC.
3. The following prompt displays:

Enter Terminating atm Address:

Enter the ATM address for the output port of the ATM switch at the end of this soft PVC. You could also specify the ATM address for the end device on this soft PVC.

4. The following prompt displays:

Enter EndPoint Id (1..65535) :

Enter the endpoint identification. This identification number is used to keep track of the endpoints within the soft PVC. This number is used for identification purposes only and does not affect VPI/VCI numbering.

5. The following prompt displays:

Enter Selector Type {required(1), any(2)} :

This prompt indicates whether or not you want the destination ATM switch to choose the VPI and VPI/VCI values or if you want to specify these values manually. **Required** means that you must specify **Other End VPI** and/or **Other End VCI** values manually. **Any** means the destination switch will select the VPI and VCI values.

6. If you select **Required** after the **Selector Type** field, the following prompt displays:

Enter Other End VPI:

Enter the Virtual Path Identifier (VPI) used for this circuit on the ATM switch at the other end of this soft PVC connection. This prompt will not display if you selected **Any** as the **Selector Type** in Step 5.

7. If you select **Required** after the **Selector Type** field, the following prompt displays:

Enter Other End VCI:

Enter the Virtual Channel Identifier (VCI) used for this circuit on the ATM switch at the other end of this soft PVC connection. This field will not display if you are not setting up a Virtual Channel Connection (VCC) or if you selected **Any** as the **Selector Type** in Step 5.

8. The following prompt displays:

Enter Retry Interval (0..3600) :

Enter the period to wait, in seconds, before attempting to establish another soft PVC connection after the first failed call attempt. A value of zero (0) indicates that no retries will be attempted.

9. The following prompt displays:

Enter Retry Threshold (0..65535) :

Enter the number of call setup attempts that will be made to establish the same soft PVC connection before an alarm is generated. After this threshold is reached an alarm will be generated. A value of zero (0) indicates that an infinite number of retries will be attempted before an alarm is generated.

10. The following prompt displays:

Enter Retry Limit (0..65535) :

Enter the maximum number of consecutive unsuccessful call setup attempts that will be made before stopping any further attempts to set up the connection. A value of zero (0) indicates that an infinite number of attempts will be made to establish the connection.

Timing Requirements

Indicates whether end-to-end timing over the broadband link is necessary. End-to-end timing for traffic types sensitive to transit delay, such as CBR traffic, typically require end-to-end timing. Indicate whether you want to require end-to-end timing in this field.

Susceptibility to Clipping

Indicates whether or not cells on this link can be discarded under congestion conditions. If you want cells to be discarded when congestion occurs, then select the **True** option. If you do not want cells to be discarded under congestion, then select the **False** option.

User Plane Connection Configuration

Select whether this soft PVC is a standard point-to-point connection or whether it is a point-to-multipoint connection. Point-to-multipoint connections are configured through Option 8; the procedure for configuring multipoint connections is described in *Configuring Point-to-Multipoint Soft PVCs* on page 42-15.

Configuring Transport Priority with the Multiple-Peer Group Software

If you are running the multiple-peer group version of the software (i.e., **cell_mpg.img** instead of **cell.img**, **asm_mpg.img** or **asmc_mpg.img** instead of **asm.img** or **asmc.img**), then Option 7 in the **scvc** command, **Transport Priority**, will not be available to you.

To configure the transport priority in the multiple-peer group software, you use a combination of configuring the QoS class parameters (with Option 11, which is described in *Configuring Traffic Parameters* on page 42-8) and the Broadband Bearer Capabilities (with Option 16, which is described in *Configuring Broadband Bearer Capability Parameters* on page 42-18). However, you must observe the following rules:

- If you set the QoS class to UBR (i.e., you set Suboptions 1 and/or 4 to **0** in Option 11), then the transport priority will be UBR regardless of how you set the Broadband Bearer Capabilities in Option 16.
- If you set the QoS class to CBR, rt-VBR, nrt-VBR, or ABR (i.e., you set Suboptions 1 and/or 4 to **1, 2, 3, or 4**, in Option 11, respectively), follow the rules shown in the table below to obtain the desired transport priority.

Setting Transport Priority in Multiple-Peer Group Software

Traffic Type (Set in Suboption 2 of Option 11)	Broadband Bearer Timing Requirements		
	No Indication (Set Suboption 3 in Option 11 Equal to 1)	End-to-End Timing Required (Set Suboption 3 in Option 11 Equal to 2)	End-to-End Timing Not Required (Set Suboption 3 in Option 11 Equal to 3)
No Indication (1)	Transport Priority = nrt-VBR	Transport Priority = rt-VBR	Transport Priority = nrt-VBR
CBR (2)	Transport Priority = CBR	Transport Priority = CBR	Transport Priority = CBR
VBR (3)	Transport Priority = nrt-VBR	Transport Priority = rt-VBR	Transport Priority = nrt-VBR

For example, to set the transport priority of an SPVC to rt-VBR (real time, Variable Bit Rate) using multiple-peer group software, you would:

- Set the QoS class to rt-VBR (i.e., set Suboption 1 and/or 4 in Option 11 to **2**);
- Set the traffic type to VBR (i.e., set Suboption 2 in Option 16 to **3**); and
- Set the Broadband Bearer Timing Requirements to end-to-end required (i.e., set Suboption 3 in Option 16 to **2**).

Broadband Bearer Capability Parameters									
Slot	Port	VPI	VCI	Class	Traffic Type	Timing Requirement	Suscept To Clip	User Plane Config	
5	5	1	1	C	noIndication	noIndication	True	pt2pt	

Slot	Port	VPI	VCI	User Up Time	Down Time	Pri.	Statistics Mode
5	5	1	1	MON FEB 03 13:30:08	MON FEB 03 13:30:08	15	CntGcra, PsCell

Tx Traffic Information									
Slot	Port	VPI	VCI	Tx Traffic Descrip Type	Peak Cell Rate	Sustain Cell Rate	Maximum Burst Sz	Tx QoS	Best Effort
5	5	1	1	NoCLP NoSCR	1			Uns	True

Rx Traffic Information									
Slot	Port	VPI	VCI	Rx Traffic Descrip Type	Peak Cell Rate	Sustain Cell Rate	Maximum Burst Sz	Rx QoS	Best Effort
5	5	1	1	NoCLP NoSCR	1			Uns	True

Multicast									
Slot	Port	VPI	VCI	gcra a enf mode	gcra b enf mode	grp id	enable	ingrs/egrss	
5	5	1	1	no cong dx clp1	no cong dx clp1	0	disable	ingress	

The legend at the top of the display indicates the symbols used to differentiate the virtual circuit types. A symbol is placed after the **Transport Priority** column to indicate the circuit type. The **svvc** command displays only soft PVCs, shown by the @ symbol.

Incoming Port, Outgoing Port, Connection Description, Chan Type, and Transport Priority. These variables are described earlier in *Creating a Soft PVC* on page 42-3.

EndPt Id, Terminating Atm Address, Other End Vpi/Vci. These variables are described in *Creating a Soft PVC* on page 42-3.

Release Cause. Indicates an internal code that gives information on why this connection was released.

Oper Status. Indicates the current operational status of this soft PVC.

Release Diagnostic. Indicates an internal diagnostic code used for releasing this connection.

Retry Intvl, Retry T'hold, Retry Limit. These variables are described earlier in *Configuring Soft PVC Retry Parameters* on page 42-18.

Retry Timer. The current value, in seconds, for the retry timer on this soft PVC connection.

Retry Failures. The total number of retry failures experienced on this connection.

Traffic Type, Timing Requirement, Suscept To Clip, User Plane Config. These variables are described earlier in *Configuring Broadband Bearer Capability Parameters* on page 42-18.

User Pri., Statistics Mode. These variables are described in *Configuring Statistics and Priority Parameters* on page 42-14.

Tx Traffic Information, Rx Traffic Information. These variables are described in *Configuring Traffic Parameters* on page 42-8.

gcra a mode, gcra b mode. The type of algorithm used for the Generic Cell Rate Algorithm (GCRA), or “leaky bucket,” with this virtual circuit. By default, this column will read **no cong dx clp1**, meaning that only CLP=1 cells will be discarded.

Multicast grp id. The group identification number for this multicast virtual circuit. This number is not user-configurable and is used internally by the switch.

Multicast enable. Indicates whether multicast leaf virtual circuits are associated with this root virtual circuit.

Multicast ingres/egress. Indicates whether this is the ingress or egress point for this multicast virtual circuit.

Virtual UNI/NNI Using Virtual Path (VP) Tunneling

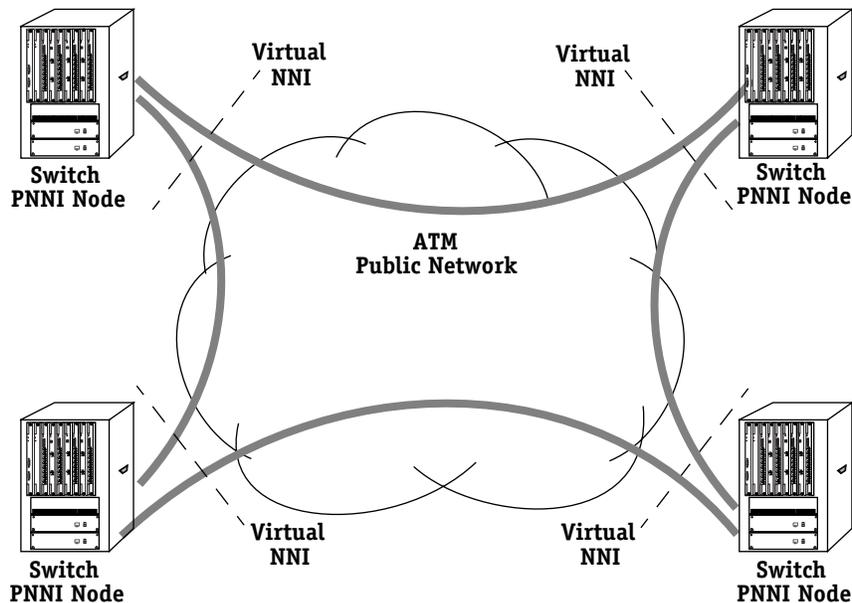
You can create multiple UNI or NNI instances on a CSM physical port through the use of virtual path (VP) tunneling. A single switch connected to a PVC-based ATM network, such as a public carrier network, can support up to 255 UNI or NNI instances. You create these instances through the **cvpt** command, which allows you to configure signaling parameters on a per UNI or NNI basis. You can configure each instance to be a UNI (public or private), PNNI, or IISP connection.

The virtual UNI/NNI feature can be used in multiple applications. The following sections provide three examples in which this feature could be deployed.

Extending PNNI Over Public Networks

The most common VP Tunneling application interconnects campus networks via public ATM bearer services. This application extends the PNNI network over the public network. PNNI nodes on each side of the public network are interconnected by Permanent Virtual Paths (PVPs). Although the nodes use the public network to communicate with each other, the nodes function as if they are part of the same small private network.

The Virtual Path that connects the OmniSwitch nodes in the following diagram is managed and policed by the ATM carrier service provider. PNNI nodes manage and police the virtual tunnels within the Virtual Path, but not the Virtual Path itself.

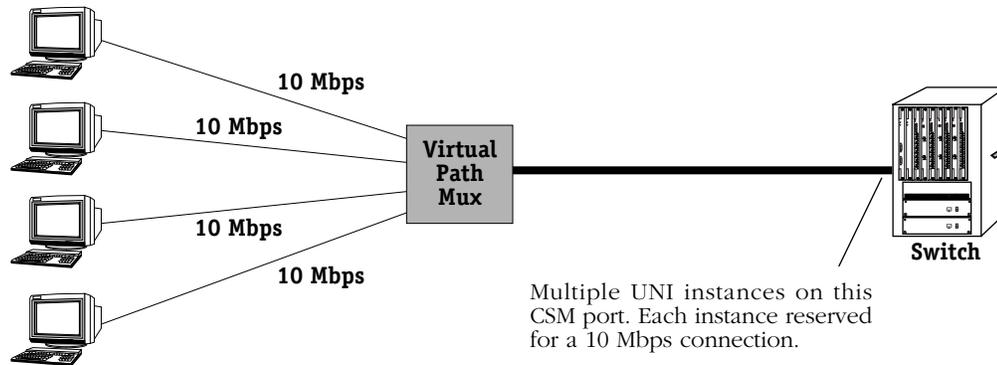


Virtual NNI Instances Extend PNNI Over Public Network

The Virtual Path Identifier (VPI) for all virtual paths piped across the public network will be the same in this example. When configuring virtual paths, it is important that the VPI used matches the VPI supplied by the service carrier. For example, if the service carrier assigns the network a VPI of 80, then all configured virtual paths must use 80 as their VPI.

Virtual Path Mux

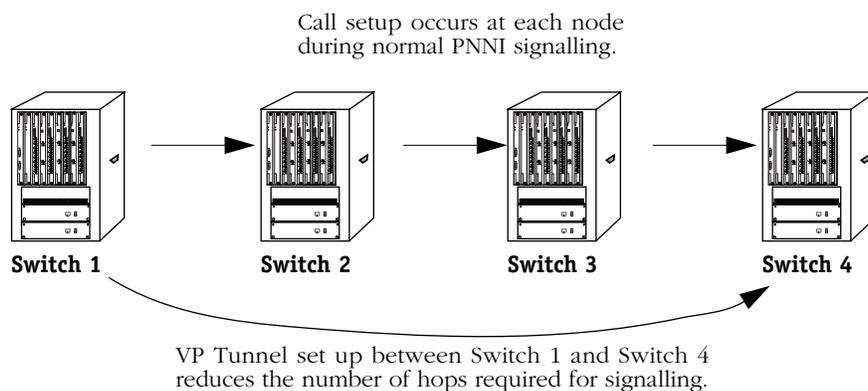
As a second application, you could assign a virtual UNI to each of several low-speed links that combine into a high-speed ATM link. The diagram below shows several 10 Mbps devices connecting into a VP mux, or cross-connect. Each 10 Mbps device could use a LAN Emulation (LANE) switched virtual circuit (SVC) to connect to the ATM network. Signaling messages on the user side would take VCI 5 within each virtual path and ILMI messages would take VCI 16. The user devices are muxed through the cross-connect and sent on an ATM link, such as an OC-3 link, to the OmniSwitch. On the OmniSwitch port connected to the VP mux you would assign unique UNI instances to distinguish the various 10 Mbps connections.



Switch Distinguishes User Devices Through Virtual UNIs

Signaling Hop Reduction

A virtual path tunnel can also be used to reduce the number of signaling hops in a PNNI network. In a daisy-chain of ATM switches, call setups and other signaling messages are normally processed at each hop. Using a virtual NNI, a virtual path tunnel could be created between the first and last switches of the daisy-chain, reducing the amount of signaling that must take place to establish a call.



VP Tunnel Reduces Signalling Overhead

Creating a VP Tunnel

You can use the **cvpt** command to configure Virtual Path (VP) Tunnels on a CSM port. To use this command, enter **cvpt** followed by the slot and port number of the CSM port on which you want to set up the VP tunnel. For example, to configure a virtual path for port 1 on the CSM module in slot 8, you would enter:

```
cvpt 8/1
```

A screen similar to the following displays:

Slot 5 Port 3 VP Tunnel Configuration

- 1) Description (30 chars max) :
- 2) Tunnel VPI : 1
- 3) I/F Type {Pub UNI(1), Pri UNI(2),
PNNI (3), IISP(4)} : PNNI
- 4) SIG Enable {False(1), True(2)} : Enable
- 5) Signaling Ver {3.0(1), 3.1(2)
4.0(3)} : 3.1
- 6) ILMI Enable {False(1), True(2)} : Disable
- 7) Admin Status { disable (1)
enable (2)} : Enable
- 8) Shaping Status { disable (1)
enable (2)} : Disable

Enter (option=value/save/cancel) :

These fields are discussed on the following page.

◆ Important Note ◆

Option 8) **Shaping Status** and any sub-options are displayed only if the slot you've specified uses a CSM-ABT-155F daughtercard.

You change a value in the field by entering the line number for the value, an equal sign (=), and then the new value for the variable. For example, to change the **Description** field variable to read “VP Tunnel 1,” you would enter a 1 (the line number for **Description**), an equal sign, and then the new description as follows:

1=VP Tunnel 1

Description

A textual description of this VP Tunnel. The description may be up to 30 characters long. This identifier will be used in displays for other software commands.

Tunnel VPI

The Virtual Path Identifier (VPI) for the VP tunnel you are creating. If this VPI will be used over a public network, then it should match the VPI assigned by your carrier. You can configure traffic parameters for this VPI through the **cvc** command.

Note that the valid VPI range for this VP tunnel is determined by the **Max VPI Bits** value you specified through the **map** command. For example, if the value indicated for **Max VPI Bits** allows the CSM port to support VPIs in the range of 1 to 15, then make sure the VP tunnel VPI you specify here falls within that range.

◆ Caution ◆

When configuring a VP tunnel, you need to consider the range of VPIs supported by the CSM ports on each side of the tunnel connection. For example, if one CSM port supports VPIs 0 to 3 and the other CSM port supports VPIs 0 to 7, then you need to make sure that the VP tunnel between the two ports uses a VPI in the range of 0 to 3. Otherwise, if a VP tunnel were to use a VPI greater than 3, then the VPI on one CSM port would be truncated and data would appear to come in on the wrong VPI.

I/F Type

Specifies the type of ATM interface that this VP tunnel supports. The options include:

- Pub UNI** Public UNI. This virtual path will be used for connections to public ATM service carrier switches, such as those used by Telcos.
- Priv UNI** Private UNI. The virtual path is used for private UNI uplinks. Such a VP would connect either directly to an ATM workstation, LAN switch, or ATM attached router.
- PNNI 1.0** Private Network-to-Network Interface (PNNI). The virtual path will support PNNI version 1.0 ATM routing, which includes support for a single peer group mapping.

◆ Important Note ◆

If your software version is prior to 4.1, then you *must* reboot the switch when you change the **I/F Type** from **PNNI 1.0** to **Pub UNI**.

- IISP** Interim Interswitch Signaling Protocol. Typically an IISP virtual path would be part of an intermediate ATM node that did not support the PNNI routing protocol. It is used primarily for establishing static routes using the IISP protocol. See Chapter 47, “Managing IISP and PNNI Routes” for further information.

SIG Enable

Indicate whether you want to enable the Service-Specific Connection Oriented Protocol (SSCOP). SSCOP operates on the ATM control plane and is a peer-to-peer protocol that helps set up connections, detect errors in connections, and correct connection errors.

Signaling Ver

The version of the User-to-Network Interface (UNI) used on this virtual path. The switch is compliant with ATM Forum UNI specifications versions 3.0, 3.1, and 4.0. You select which version your ATM network supports.

◆ Important Note ◆

If you change the **Signaling Ver**, then you *must* reboot the switch.

ILMI Enable

Indicates whether or not you want to enable ILMI. Normally you will want to enable ILMI to allow the switch to discover attached ATM End Systems (ESs). If you disable ILMI, then you must configure a static route between this virtual path and all attached ESs.

Admin Status

Indicates the administrative status for this VP tunnel. When first configuring your network, you may want to create a VP tunnel and disable it until it is ready for live operation. The VP tunnel will not be available for traffic flow until the **Admin Status** is set to **Enable**.

Shaping Status

This field is displayed only if the slot you've specified uses a CSM-ABT-155F daughtercard. **Shaping Status** indicates the status of tunnel shaping for this VP tunnel (default = **Disable**). When enabled, this feature can be used to limit the amount of bandwidth used in the tunnel. When Tunnel Shaping is created, all VC channels created with a VPI are checked and recreated with a valid tunnel identifier in order to associate them with the tunnel. After Tunnel Shaping has been created, whenever a VC channel with the same VPI is created or modified, the tunnel identifier is added so that the VC channel can be associated with the tunnel. To activate tunnel shaping, the **Shaping Status** field must be set to **Enable**. To enable Shaping Status, enter **8=2**.

◆ Important Note ◆

Only one instance of Tunnel Shaping can be created per VPI, because the tunnel is created based on the VPI value.

When **Shaping Status** is set to **Enable**, the following options will appear:

A screen similar to the following displays:

```

Slot 5 Port 3 VP Tunnel Configuration

1) Description (30 chars max)      :
2) Tunnel VPI                      : 1
3) I/F Type {Pub UNI(1), Pri UNI(2),
   PNNI (3), IISP(4)}              : PNNI
4) SIG Enable {False(1), True(2)}  : Enable
5) Signaling Ver {3.0(1), 3.1(2),
   4.0(3)}                          : 3.1
6) ILMI Enable {False(1), True(2)} : Disable
7) Admin Status { disable (1)
   enable (2) }                    : Enable
8) Shaping Status { disable (1)
   enable (2) }                    : Enable

81) Priority
   {CBR=1 rtVBR=2 nrtVBR=3 UBR=4}
   : 0
82) Bandwidth limitation           : 0

```

Enter (option=value/save/cancel) :

Priority

Tunnel Shaping designates transport priority values from 1 to 4 (default=0) based on the following service categories:

- **CBR=1** - All VC connections into the tunnel will have the same priority as **CBR** cross connections.
- **rtVBR=2** - All VC connections into the tunnel will have the same priority as **rtVBR** cross connections.
- **nrtVBR=3** - All VC connections into the tunnel will have the same priority as **nrtVBR** cross connections.
- **UBR=4** - All VC connections into the tunnel will have the same priority as **UBR** cross connections.

To specify a priority equivalent to **CBR=1**, for example, enter **81=1**.

Bandwidth Limitation

When Tunnel Shaping has been enabled on the CSM-ABT-155 daughtercard, bandwidth restrictions can be applied to all VC channels linked to the tunnel. Data throughput is restricted based on the specified transport priority, ranging from 0 (default) to 353208 cells per second (maximum rate for a CSM-ABT-155 OC3 daughtercard).

To specify a bandwidth limitation factor of 1000, for example, enter **82=1000**.

To save your configuration settings, enter **s**.

Displaying VP Tunnel Information

The **lvpt** command allows you to display information on all configured VP tunnels in the switch. If you enter **lvpt** at any prompt a screen similar to the following displays:

```

CSM VP Tunnel(s)
=====
Index Slot Port Inst VP Tunnel Descriptor VP Tun Number VPI Type
=====
1 6 1 1 ATM Tunnel #2 on VP 1. 2 1 PNNI
2 7 1 1 ATM Tunnel #1 on VP 1. 1 1 PNNI
3 7 2 1 ATM Tunnel #3 on VP 1. 3 1 PNNI

Index Slot Port Inst Abs Port Enable ILMI Enable SSCOP Admin Status
=====
1 6 1 1 702 Disabl Enable Enable
2 7 1 1 701 Disabl Enable Enable
3 7 2 1 703 Disabl Enable Enable

Status
=====
Sit Prt Inst Sscop Up Sscop Down Up Dn Status
=====
6 1 1 TUE FEB 23 15:34:41 2001 WED FEB 24 11:42:47 2001 4 5 Down
7 1 1 TUE FEB 23 10:09:57 2001 ----- 1 0 Up
7 2 1 TUE FEB 23 14:57:11 2001 TUE FEB 23 14:56:18 2001 10 10 Up

Sit Prt Inst Ilmi Up Ilmi Down Up Dn Status
=====
6 1 1 TUE FEB 23 15:34:29 2001 WED FEB 24 11:42:47 2001 5 1 Down
7 1 1 TUE FEB 23 10:09:57 2001 ----- 1 0 Up
7 2 1 TUE FEB 23 14:57:11 2001 TUE FEB 23 11:04:26 2001 8 1 Up

Sit Prt Inst Phy Up Phy Down Up Dn Status
=====
6 1 1 TUE FEB 24 11:45:21 2001 WED FEB 24 11:42:47 2001 2 2 En
7 1 1 TUE FEB 23 14:06:49 2001 ----- 2 0 En
7 2 1 TUE FEB 23 14:06:49 2001 TUE FEB 23 11:04:26 2001 3 1 Dis

```

Index. This value is a running total, or counter, of all VP tunnels set up in the switch. It is not related to the VPI value. You can use this value to help interpret displays. Since the **lvpt** display requires two sets of columns, the **Index** value can help you keep track of values between the top and bottom sets of columns.

Slot. The slot within the switch where this VP tunnel is set up.

Port. The port on the CSM module where this VP tunnel is set up.

Inst. The instance of this VP tunnel on this particular CSM module port. This value is not the same as the VPI. It is a counter of the number of VP tunnels set up on this CSM port, and can be used with the **mvpt** and **dvpt** commands. The physical CSM port has an instance of zero (0).

VP Tunnel Descriptor. The textual description of this VP tunnel entered through the **cvpt** command

VP Tun Number. This value is a number assigned by switch software to keep track of VP tunnels. It is not the same as the VPI and is used internally; it can also be used with the **mvpt** and **dvpt** commands.

VPI. The Virtual Path Identifier (VPI) assigned to this VP tunnel through the **cvpt** command. The VPI identifies a discrete path through the ATM network. Multiple virtual paths can be set up on the same CSM port; the VPI is used to identify each path on a CSM port.

Type. Specifies the type of ATM interface that this VP tunnel supports. Possible types are **PNNI**, **PrUNI** (Private UNI), **PuUNI** (Public UNI), and **IISP** (Interim Interswitch Signalling Protocol). Definitions for each of these types are provided in the section, *Creating a VP Tunnel* on page 42-26.

Abs Port. An internal port assignment used by PNNI software to identify specific VP tunnels. You might use this number for the sake of comparison when viewing displays for PNNI-specific commands, which are found in the PNNI sub-menu. Some PNNI commands use these port assignments to describe connections. The same number in this **lvpt** display will correspond to a port assignment in a PNNI display screen.

ILMI Enable. Indicates whether the Integrated Local Management Interface (ILMI) has been enabled on this virtual path through the **cvpt** command.

Enable SSCOP. Indicates whether the Service-Specific Connection Oriented Protocol (SSCOP) has been administratively enabled through the **cvpt** command.

Admin Status. Indicates whether this VP tunnel was administratively enabled or disabled through the **cvpt** command. The VP tunnel can not become operational until the **Admin Status** has been set to **Enable**.

The following column headings fall under the table heading labeled **Status**.

SSCOP. The current operational state of the Service-Specific Connection Oriented Protocol (SSCOP). SSCOP operates on the ATM control plane and is a peer-to-peer protocol that helps set up connections, detect errors in connections, and correct connection errors. The **Sscop Up** and **Sscop Down** columns will indicate the last time SSCOP last came up and went down, respectively. The **Up** and **Down** columns will indicate the number of times SSCOP came up and went down, respectively. The SSCOP **Status** column will indicate Up or Down.

ILMI. The current operational state of the Integrated Local Management Interface (ILMI), which is a standard ATM management protocol based on SNMP. By default, ILMI uses VPI 0 and VCI 16 for management signalling. The **Ilmi Up** and **Ilmi Down** columns will indicate the last time ILMI last came up and went down, respectively. The **Up** and **Down** columns will indicate the number of times ILMI came up and went down, respectively. The ILMI **Status** column will indicate Up or Down.

PHY. The Operational Status of this virtual path. This column indicates if the virtual path is **Enabled** or **Disabled**. The **Phy Up** and **Phy Down** columns will indicate the last time PHY last came up and went down, respectively. The **Up** and **Down** columns will indicate the number of times PHY came up and went down, respectively. The PHY **Status** column will indicate whether the port is **Enabled** or **Disabled**. The virtual path is enabled if the connection is good on this end and the far end. If there is a disconnection at either end, the operational status will be **Disabled**.

Viewing SSCOP, ILMI, and PHY

You can view general and detailed SSCOP, ILMI, and PHY information on all configured VP tunnels in a switch, a single CSM board, and individual ports. The **lvpt** command is used to provide this information.

Viewing SSCOP, ILMI, and PHY Information on All Ports

To view SSCOP, ILMI, and PHY information on all configured VP tunnels in a switch, you enter the **lvpt** command along with the following parameters:

lvpt sip

where **s** indicates SSCOP, **i** indicates ILMI, and **p** indicates PHY. This command displays a screen similar to the following:

```

CSM VP Tunnel(s)
Status
=====
Slt Prt Inst      Sscop Up          Sscop Down        Up  Dn  Status
=====
6   1   1   TUE FEB 23 15:34:41 2001  WED FEB 24 11:42:47 2001  4   5   Down
7   1   1   TUE FEB 23 10:09:57 2001  -----              1   0   Up
7   2   1   TUE FEB 23 14:57:11 2001  TUE FEB 23 14:56:18 2001 10  10  Up

Slt Prt Inst      Ilmi Up           Ilmi Down          Up  Dn  Status
=====
6   1   1   TUE FEB 23 15:34:29 2001  WED FEB 24 11:42:47 2001  5   1   Down
7   1   1   TUE FEB 23 10:09:57 2001  -----              1   0   Up
7   2   1   TUE FEB 23 14:57:11 2001  TUE FEB 23 11:04:26 2001  8   1   Up

Slt Prt Inst      Phy Up           Phy Down           Up  Dn  Status
=====
6   1   1   TUE FEB 24 11:45:21 2001  WED FEB 24 11:42:47 2001  2   2   En
7   1   1   TUE FEB 23 14:06:49 2001  -----              2   0   En
7   2   1   TUE FEB 23 14:06:49 2001  TUE FEB 23 11:04:26 2001  3   1   Dis
    
```

Additionally, you may enter the parameters for SSCOP, ILMI, and PHY in any order and combination. For example, if you wanted to view only the ILMI and PHY, you would enter the **lvpt** command along with the respective parameters as follows:

lvpt ip

or

lvpt pi

This command displays a screen similar to the following:

```

Slt Prt Inst      Ilmi Up          Ilmi Down          Up  Dn  Status
=====
6   1   1   TUE FEB 23 15:34:29 2001  WED FEB 24 11:42:47 2001  5   1   Down
7   1   1   TUE FEB 23 10:09:57 2001  -----              1   0   Up
7   2   1   TUE FEB 23 14:57:11 2001  TUE FEB 23 11:04:26 2001  8   1   Up

Slt Prt Inst      Phy Up           Phy Down           Up  Dn  Status
=====
6   1   1   TUE FEB 24 11:45:21 2001  WED FEB 24 11:42:47 2001  2   2   En
7   1   1   TUE FEB 23 14:06:49 2001  -----              2   0   En
7   2   1   TUE FEB 23 14:06:49 2001  TUE FEB 23 11:04:26 2001  3   1   Dis
    
```

Descriptions of the columns included in the two displays above are described earlier in *Displaying VP Tunnel Information* on page 42-30.

Viewing SSCOP, ILMI, and PHY Information on One CSM Board

To view SSCOP, ILMI, and PHY information on a single CSM board, you enter the **lvpt** command along with the slot number for the CSM board and the following parameters:

lvpt <slot> sip

where **<slot>** is the slot number where the CSM board is installed, **s** indicates SSCOP, **i** indicates ILMI, and **p** indicates PHY. For example, if you wanted to view SSCOP, ILMI, and PHY information for the board in slot 7, you would enter:

lvpt 7 sip

This command displays a screen similar to the following:

```

                                CSM VP Tunnel(s)
=====
Index Slot Port Inst VP Tunnel Descriptor VP Tun Number VPI Type
=====
2      7   1   1   ATM Tunnel #1 on VP 1.      1     1   PNNI
3      7   2   1   ATM Tunnel #3 on VP 1.      3     1   PNNI
=====

Index Slot Port Inst Abs Port Enable ILMI Enable SSCOP Admin Status
=====
2      7   1   1   701 Disabl Enable Enable
3      7   2   1   703 Disabl Enable Enable
=====

                                Status
                                =====

Slt Prt Inst Sscop Up Sscop Down Up Dn Status
=====
7  1  1  TUE FEB 23 10:09:57 2001 ----- 1  0  Up
7  2  1  TUE FEB 23 14:57:11 2001 TUE FEB 23 14:56:18 2001 10 10  Up

Slt Prt Inst Ilmi Up Ilmi Down Up Dn Status
=====
7  1  1  TUE FEB 23 10:09:57 2001 ----- 1  0  Up
7  2  1  TUE FEB 23 14:57:11 2001 TUE FEB 23 11:04:26 2001 8  1  Up

Slt Prt Inst Phy Up Phy Down Up Dn Status
=====
7  1  1  TUE FEB 23 14:06:49 2001 ----- 2  0  En
7  2  1  TUE FEB 23 14:06:49 2001 TUE FEB 23 11:04:26 2001 3  1  Dis

```

Additionally, you may enter the parameters for SSCOP, ILMI, and PHY in any order and combination. For example, if you wanted to view the statistics for only SSCOP and ILMI for a single board, you would enter the **lvpt** command along with the slot number and the respective parameters as follows:

lvpt <slot> si

or

vap <slot> is

Descriptions of the columns included in the display above are described earlier in *Displaying VP Tunnel Information* on page 42-30.

Viewing SSCOP, ILMI, and PHY Information on One Port

To view SSCOP, ILMI, and PHY information on a single CSM port, you enter the **lvpt** command along with the slot number for the CSM board, the port number for which you want to receive information, and the following parameters:

```
lvpt <slot>/<port> sip
```

where **<slot>** is the slot number where the CSM board is installed, **<port>** is the port number on the CSM board, **s** indicates SSCOP, **i** indicates ILMI, and **p** indicates PHY. For example, if you wanted to view SSCOP, ILMI, and PHY information for port 2 on the CSM module in slot 7, you would enter:

```
lvpt 7/2 sip
```

This command displays a screen similar to the following:

```

                                CSM VP Tunnel(s)
=====
Index  Slot  Port  Inst  VP Tunnel Descriptor  VP Tun  VPI  Type
=====
  3     7     2     1     ATM Tunnel #3 on VP 1.  3       1   PNNI

Index  Slot  Port  Inst  Abs  Enable  Enable  Admin
=====  =====  =====  =====  =====  =====  =====  =====
  3     7     2     1     703  Disabl  Enable  Enable

                                Status
                                =====

Slt  Prt  Inst  Sscop Up  Sscop Down  Up  Dn  Status
=====  =====  =====  =====  =====  =====  =====  =====
  7     2     1     TUE FEB 23 14:57:11 2001  TUE FEB 23 14:56:18 2001  10  10  Up

Slt  Prt  Inst  Ilmi Up  Ilmi Down  Up  Dn  Status
=====  =====  =====  =====  =====  =====  =====  =====
  7     2     1     TUE FEB 23 14:57:11 2001  TUE FEB 23 11:04:26 2001  8   1   Up

Slt  Prt  Inst  Phy Up  Phy Down  Up  Dn  Status
=====  =====  =====  =====  =====  =====  =====  =====
  7     2     1     TUE FEB 23 14:06:49 2001  TUE FEB 23 11:04:26 2001  3   1   Dis

```

Additionally, you may enter the parameters for SSCOP, ILMI, and PHY in any order and combination. For example, if you wanted to view the statistics for only SSCOP and PHY for a single CSM port, you would enter the **lvpt** command along with the slot number, the port number for which you want to receive information, and the respective parameters as follows:

```
lvpt <slot>/<port> sp
```

or

```
lvpt <slot>/<port> ps
```

Descriptions of the columns included in the display above are described earlier in *Displaying VP Tunnel Information* on page 42-30.

Modifying a VP Tunnel

The **mvpt** command enables you to modify a VP tunnel. It uses the same screens and allows you to change the same parameters as the **cvpt** command. To begin modifying a VP tunnel, enter **mvpt** followed by the slot number, a slash (/), and the port number where the VP tunnel currently exists. Enter a space and then the instance number for the VP tunnel. You can find the instance number through the **lvpt** display. For example, to modify a VP tunnel with an instance number of 3 on Port 1 of the CSM module in slot 4, you would enter:

```
mvpt 4/1 3
```

Alternatively, you can enter **mvpt** followed simply by the VP tunnel number. Each VP tunnel on the switch has a unique VP tunnel number, which you can find through an **lvpt** command display. Using this method, you could delete a VP tunnel with a number of 7 by entering:

```
mvpt 7
```

For more information on the **mvpt** screens and parameters, see *Virtual UNI/NNI Using Virtual Path (VP) Tunneling* on page 42-24.

Deleting a VP Tunnel

You can use the **dvpt** command to delete VP tunnels previously created through **cvpt**. To delete a VP tunnel, enter **dvpt** followed by the slot number, a slash (/), and the port number where the VP tunnel currently exists. Enter a space and then the instance number for the VP tunnel. Find the instance number through an **lvpt** display. For example, to delete a VP tunnel with an instance number of 3 on Port 1 of the CSM module in slot 4, you would enter:

```
dvpt 4/1 3
```

Alternatively, you can enter **dvpt** followed simply by the VP tunnel number. Each VP tunnel on the switch has a unique VP tunnel number, which you can find through an **lvpt** command display. Using this method, you could delete a VP tunnel with a number of 7 by entering:

```
dvpt 7
```

A prompt displays to confirm the deletion. After you answer that prompt a message displays to indicate whether the VP tunnel was deleted.

Configuring a LECS ATM Address

The **masrt** command configures LANE Configuration Server (LECS) ATM addresses on an ATM cell switch. This command modifies the service registry table in the Integrated Local Management Interface (ILMI) database. ILMI is responsible for the LECS ATM address as this address is configured on the network side of a user-to-network (UNI) connection.

LANE clients find a LECS address by going directly to the ILMI service registry table or by using the ATM Well-Known Address (WKA) for a LECS. The LANE client will typically use the well-known address to locate the LECS. This well-known ATM address for a LECS is as follows:

47007900000000000000000000000000A03E00000100

However if you want to configure multiple LECSs (e.g., redundant configurations) or if your LANE client bypasses the LECS well-known address and goes straight to the ILMI service registry table for the LECS address, then you will have to use **masrt**.

Multiple LECS can be helpful. LANE clients (LECs) use the LECS to locate LANE servers. If the LECS is unavailable and you have not configured another LECS in ILMI, then no new clients will be able to locate the LANE server. You can configure up to 16 LECS addresses in the service registry table of an ATM switch.

Instructions for using **masrt** are provided as follows:

1. Enter **masrt** and press **<Enter>**. A screen similar to the following displays:

ATM Service Registry Table configuration:

ATM Service Registration Table is empty!

(add/save/quit/cancel/help)

:

2. Enter **add** at the colon prompt (:) and press **<Enter>**. The following prompt displays:

Enter 20 byte ATM address:

3. Enter the ATM address that you want to configure and press **<Enter>**. The following prompt displays:

Type of Service ([L]ecs/[A]ns): (L)

4. Indicate whether the ATM address is for a LECS or an ATM Name Server (ANS). The ANS is also part of the ILMI database. By default this prompt will select LECS. If this address is for an ANS, then you must specifically select **A**. Press **<Enter>** after making your selection.

- If the ATM address you set up is for a LECS, then the following prompt displays:

Map WKA to this LECS address:

Indicate whether you want the LECS Well-known Address (WKA) to be mapped to this new address. Enter a **Y** for Yes or an **N** for No. In most cases, you will want to indicate Yes at this prompt. If you enter **Y** here, then a LANE client that cannot reach the LECS by well-known address may query (if configured to perform such queries) the service registry table for the address. If you indicate **N**, then the LANE client will not be able to see this address when searching for the LECS by well-known address.

The standard **masrt** prompt re-displays:

```
(add/save/quit/cancel/help)
:
```

- Enter **save** to save the settings you just configured. You can now enter **quit** to exit the command.

Mapping Service Registry Table Addresses to the Well-Known Address

When you map a new LECS address to the well-known address through **masrt** (Step 5 in the above instructions) LANE clients will be able to access the address in the event the well-known address is not available. If the well-known address is not accessible, LANE clients may query (when they are configured to make such queries) the LECS addresses in the service registry table until they find one that is available.

◆ **Note** ◆

Mapping an ATM address to the well-known address does *not* change the well-known address. It just makes the additional LECS address accessible to LANE clients.

You can find out if a LECS address has been mapped to the well-known address by entering the **masrt** command. If any addresses have been configured, they will display. For example, the following **masrt** display shows two configured LECS addresses.

ATM Service Registry Table configuration:

```
1) LECS address - 3902689001bc900001017e2b200020da00004000 WKA
2) LECS address - 3902691001bc900001017e2b200020da00004000 WKA

(add/save/quit/cancel/help)
:
```

Note the **WKA** after the LECS addresses. The WKA (Well-Known Address) indicates that both addresses are accessible to LANE clients. The order of the addresses is important. Once a LANE client starts to query the service registry table, it will start with the first address and then work its way through the addresses in order until it finds an address that is reachable.

Modifying Existing Addresses in the Service Registry Table

Once you add ATM addresses to the service registry table, you can modify or delete them. The following **masrt** display shows two configured LECS addresses:

ATM Service Registry Table configuration:

- 1) LECS address - 3902689001bc900001017e2b200020da00004000 WKA
- 2) LECS address - 3902691001bc900001017e2b200020da00004000 WKA

(add/save/quit/cancel/help)

:

To modify an address, type the index number of the address (1 or 2 in the above example), an equal sign, then the new ATM address. For example, to change the second ATM address to **3902841001bc900001017e2b200020da00004000**, you would enter the following at the colon prompt:

2=3902841001bc900001017e2b200020da00004000

To delete an address, type the index number of the address, an equal sign, then a period (.). For example, to delete the second ATM address in the sample shown above, you would enter:

2=.

Viewing ATM Layer Statistics

The **vls** command displays the ATM layer statistics table. This table provides a summary of transmit and receive activity on all ports of a given CSM or ATM access module. The following screen is a sample of the output from the **vls** command:

ATM Layer Statistics							
Slot	Port	Rx SDUs	Tx SDUs	Rx Cells	Tx Cells	Rx Octets	Tx Octets
3	1	0	302458	0	978672	0	46976256
3	2	0	236	0	236	0	11328

CSM ATM Layer Statistics				
Slot	Port	Received Cells	Received CLP=0 Cells	Received CLP=1 Cells
3	1	978672	978672	0
3	2	236	236	0
5	1	0	0	0
5	2	0	0	0
5	3	0	0	0
5	4	432	432	0
5	5	0	0	0
5	6	0	0	0
5	7	0	0	0
5	8	0	0	0

CSM ATM Layer Statistics				
Slot	Port	Transmitted Cells	Mark EFCI Cells	Marked GCRA Cells
3	1	0	0	0
3	2	92	0	0
5	1	0	0	0
5	2	0	0	0
5	3	0	0	0
5	4	236	0	0
5	5	0	0	0
5	6	0	0	0
5	7	0	0	0
5	8	0	0	0

The first part of the display, which is labelled **ATM Layer Statistics**, provides information on the ATM access ports (if applicable). In the sample above, information is provided only on the two FCSM internal ports. Descriptions of the columns in this table are provided in Chapter 33, "Managing ATM Access Modules."

Descriptions of the second part of the display, which is labelled **CSM ATM Layer Statistics**, are provided below.

Slot/Port. Indicates the CSM module and the port number for which statistical information is provided. Each row in the table gives information for a single CSM port.

Received Cells. The total number of ATM cells received on this port since that last initialization of the OmniSwitch. This count includes all cells (data, management, and discarded), regardless of their CLP bit setting.

Received CLP=0 Cells. The number of cells received on this port with the CLP bit set to 0. CLP=0 cells have a higher priority than cells with their CLP bit set to 1.

Received CLP=1 Cells. The number of ATM cells received on this port with the CLP bit set to 1. CLP=1 cells have a lower priority than cells with their CLP bit set to 0. Under the OmniSwitch policing algorithms, there is a higher probability of CLP=1 cells being discarded than CLP=0 cells being discarded.

Transmitted Cells. The total number of cells transmitted from this CSM port. This count includes all cells (data, management, and discarded), regardless of their CLP bit setting.

Mark EFCI Cells. The number of ATM cells for which this OmniSwitch set the Explicit Forward Congestion Indication (EFCI) bit. The switch sets the EFCI bit to 1 on cells that experience congestion. See Chapter 41, “Managing Cell Switching Modules (CSMs),” for further information.

Marked GCRA Cells. The number of ATM cells this OmniSwitch tagged (i.e., set the CLP bit to 1) during the enforcement of traffic contract parameters. Depending on the Class of Service and traffic descriptors chosen for a virtual connection, an ATM cell may be tagged when it violates one of the traffic contract parameters (i.e., PCR, SCR, or MBS). See Chapter 41, “Managing Cell Switching Modules (CSMs),” for further information on enforcement methods employed by the OmniSwitch.

Viewing ATM Layer Receive Error Statistics

The `vlrs` command displays the ATM Layer receive error statistics table. This table provides a summary of receive activity on all ports of a given CSM or ATM access module. The following screen is a sample of the output from the `vlrs` command:

ATM Layer Rx SDU Error Statistics							
Slot	Port	Discards	Errors	Invalid Sz	No Buffers	Trash	CRC Errors
3	1	0	0	0	0	0	0
3	2	0	0	0	0	0	0
7	1	0	0	0	0	0	0
7	2	0	0	0	0	0	0

ATM Layer Rx Cell Error Statistics						
Slot	Port	Discards	Errors	No Buffers	Trash	CRC Errors
3	1	0	0	0	0	0
3	2	0	0	0	0	0
7	1	0	0	0	0	0
3	2	0	0	0	0	0

CSM ATM Layer Rx Error Statistics					
Slot	Port	Total Discard Cells	Dx Congestion/CLP=0	Dx Congestion/CLP=1	
4	1	0	0	0	
4	2	0	0	0	
4	3	0	0	0	
4	4	0	0	0	
4	5	0	0	0	
4	6	0	0	0	
4	7	0	0	0	
4	8	0	0	0	
5	1	0	0	0	
5	2	0	0	0	
5	3	10	0	0	
5	4	3	0	0	
5	5	0	0	0	
5	6	0	0	0	
5	7	0	0	0	
5	8	0	0	0	
6	1	0	0	0	
6	2	0	0	0	
7	1	3	0	0	
7	2	9	0	0	

— Output continues on next page —

Viewing ATM Layer Receive Error Statistics

CSM ATM Layer Rx Error Statistics

Slot	Port	Dx Cells GRCAA CLP=0	Dx Cells GCRAA CLP=1	Dx Cells GCRAB CLP=0
4	1	0	0	0
4	2	0	0	0
4	3	0	0	0
4	4	0	0	0
4	5	0	0	0
4	6	0	0	0
4	7	0	0	0
4	8	0	0	0
5	1	0	0	0
5	2	0	0	0
5	3	0	0	0
5	4	0	0	0
5	5	0	0	0
5	6	0	0	0
5	7	0	0	0
5	8	0	0	0
6	1	0	0	0
6	2	0	0	0
7	1	0	0	0
7	2	0	0	0

CSM ATM Layer Rx Error Statistics

Slot	Port	Dx Cells GRCAA CLP=1	Unknown VP/VC Cells	Unknown VPI	Unknown VCI
4	1	0	0	0	0
4	2	0	0	0	0
4	3	0	0	0	0
4	4	0	0	0	0
4	5	0	0	0	0
4	6	0	0	0	0
4	7	0	0	0	0
4	8	0	0	0	0
5	1	0	8	0	0
5	2	0	0	0	0
5	3	0	10	0	0
5	4	0	3	0	0
5	5	0	0	0	0
5	6	0	0	0	0
5	7	0	0	0	0
5	8	0	0	0	0
6	1	0	0	0	0
6	2	0	0	0	0
7	1	0	3	0	0
7	2	0	9	0	0

The first part of the display, which is labelled **ATM Layer Rx SDU Error Statistics**, provides information on the ATM access ports (if applicable). In the sample above, information is provided only on the two FCSM internal ports. Descriptions of the columns in this table are provided in Chapter 33, "Managing ATM Access Modules."

Descriptions of the second part of the display, which is labelled **CSM ATM Layer Rx Error Statistics**, are provided on the next page.

Slot/Port. Indicates the CSM module and the port number for which statistical information is provided. Each row in the table gives information for a single CSM port.

Total Discard Cells. The total number of cells that were discarded by this OmniSwitch due to congestion and/or traffic contract violations.

Dx Congestion/CLP=0. The total number of CLP=0 (high priority) cells that were discarded during a congestive state.

Dx Congestion/CLP=1. The total number of CLP=1 (low priority) cells that were discarded during a congestive state.

Dx Cells GCRAA CLP=0. The total number of CLP=0 (high priority) cells that were discarded because they violated traffic parameters policed by the first Generic Cell Rate Algorithm (GCRA), or “leaky bucket.” For more information on GCRA, see Chapter 41, “Managing Cell Switching Modules (CSMs).”

Dx Cells GCRAA CLP=1. The total number of CLP=1 (low priority) cells that were discarded because they violated traffic parameters policed by the first Generic Cell Rate Algorithm (GCRA), or “leaky bucket.” For more information on GCRA, see Chapter 41, “Managing Cell Switching Modules (CSMs).”

Dx Cells GCRAB CLP=0. The total number of CLP=0 (high priority) cells that were discarded because they violated traffic parameters policed by the *second* Generic Cell Rate Algorithm (GCRA), or “leaky bucket.” For more information on GCRA, see Chapter 41, “Managing Cell Switching Modules (CSMs).”

Dx Cells GCRAB CLP=1. The total number of CLP=1 (low priority) cells that were discarded because they violated traffic parameters policed by the *second* Generic Cell Rate Algorithm (GCRA), or “leaky bucket.” For more information on GCRA, see Chapter 41, “Managing Cell Switching Modules (CSMs).”

Unknown VP/VC Cells. The number of cells received on this port that contained Virtual Path (VPI) and/or Virtual Channel (VCI) identifiers that this OmniSwitch did not recognize. When the OmniSwitch does not recognize the identifiers for a cell, it discards the cell.

Information on the Ports for One CSM Board

To view the ATM Layer receive error statistics table on a single CSM board, you enter the **vlrs** command along with the slot number for the CSM board as follows:

vlrs <slot>

where **<slot>** is the slot number where the CSM board is installed. For example, if you wanted to obtain status information for the board in slot 5, you would enter:

vlrs 5

This command displays a screen similar to the following:

CSM ATM Layer Rx Error Statistics

Slot	Port	Total Discard Cells	Dx Congestion/CLP=0	Dx Congestion/CLP=1
5	1	0	0	0
5	2	0	0	0
5	3	10	0	0
5	4	3	0	0
5	5	0	0	0
5	6	0	0	0
5	7	0	0	0
5	8	0	0	0

CSM ATM Layer Rx Error Statistics

Slot	Port	Dx Cells GRCAA CLP=0	Dx Cells GCRAA CLP=1	Dx Cells GCRAB CLP=0
5	1	0	0	0
5	2	0	0	0
5	3	0	0	0
5	4	0	0	0
5	5	0	0	0
5	6	0	0	0
5	7	0	0	0
5	8	0	0	0

CSM ATM Layer Rx Error Statistics

Slot	Port	Dx Cells GRCAA CLP=1	Unknown VP/VC Cells	Unknown VPI	Unknown VCI
5	1	0	8	0	0
5	2	0	0	0	0
5	3	0	10	0	0
5	4	0	3	0	0
5	5	0	0	0	0
5	6	0	0	0	0
5	7	0	0	0	0
5	8	0	0	0	0

Descriptions of the columns included in this display are described earlier in *Viewing ATM Layer Receive Error Statistics* on page 42-41.

Information on One Port

To view ATM Layer receive error statistics on a single CSM port, you enter the **vlrs** command along with the slot number for the CSM board and the port number for which you want to receive information, as follow:

```
vlrs <slot>/<port>
```

where **<slot>** is the slot number where the CSM board is installed and **<port>** is the port number on the CSM board. For example, if you wanted to view status information for Port 4 on the CSM module in slot 5, you would enter:

```
vlrs 5/4
```

This command displays a screen similar to the following:

```

CSM ATM Layer Rx Error Statistics
-----
Slot Port Total Discard Cells Dx Congestion/CLP=0 Dx Congestion/CLP=1
-----
5    4    3                    0                    0

CSM ATM Layer Rx Error Statistics
-----
Slot Port Dx Cells GRCAA CLP=0 Dx Cells GRCAA CLP=1 Dx Cells GCRAB CLP=0
-----
5    4    0                    0                    0

CSM ATM Layer Rx Error Statistics
-----
Slot Port Dx Cells GRCAA CLP=1 Unknown VP/VC Cells Unknown VPI Unknown VCI
-----
5    4    0                    3                    0        0

```

Descriptions of the columns included in this display are described earlier in *Viewing ATM Layer Receive Error Statistics* on page 42-41.

Viewing ATM Connection Statistics Table

You can view ATM connection statistical information on all ATM boards in the switch, a single CSM board, individual ports, and individual virtual circuits. The **vcs** command, which displays the ATM connection statistics table, is used to provide this information. For CSM ports, this table provides a summary of the Cell Loss Priority (CLP) bit settings for all received and transmitted cells. In addition, the statistics are broken down by VPI and VCI.

Information on All ATM Boards in a Switch

To view status information on all ATM boards in a switch, you enter the **vcs** command without any parameters as follows:

```
vcs
```

The command displays a screen similar to the following:

ATM Connection Statistics								
Slot	Port	VCI	Rx SDUs	Tx SDUs	Rx Cells	Tx Cells	Rx Octets	Tx Octets
3	1	100	0	9647	0	28465	0	1366320

CSM Connection Statistics						
Slot	Port	VPI	VCI	Received Cells/ Received CLP=0 Cells	Transmitted Cells/ Received CLP=1 Cells	
3	1	0	5	0	0	
3	1	0	16	0	0	
3	1	0	18	0	0	
3	2	0	32	0	0	
3	2	0	105	444	444	
3	2	0	296	0	0	
3	2	0	369	180	180	
3	2	1	560	0	0	
3	2	1	633	0	0	
5	4	0	5	0	0	
5	4	0	16	182	182	
5	4	0	18	182	0	
				0	0	

The first part of the display, which is labelled **ATM Connection Statistics**, provides information on the ATM access ports (if applicable). In the sample above, information is provided only on the two FCSM internal ports. Descriptions of the columns in this table are provided in Chapter 33, "Managing ATM Access Modules."

Descriptions of the second part of the display, which is labelled **CSM Connection Statistics**, are provided as follows.

Slot/Port/VPI/VCI. These columns identify the virtual circuit for which statistics are displayed. The Slot and Port indicate the physical interface, or CSM port, where this Virtual Circuit is configured. The VPI is the Virtual Path Identifier for the circuit and the VCI is the Virtual Channel Identifier for the circuit.

Received Cells/Received CLP=0 Cells. Statistics in this column are displayed as two values for each VPI/VCI row. The top value for each VPI/VCI row is the total number of cells received by this switch on this virtual circuit. The bottom value is the total number of cells with the CLP bit set to 0 received by this switch on this virtual circuit.

Transmitted Cells/Received CLP=1 Cells. Statistics in this column are displayed as two values for each VPI/VCI row. The top value for each VPI/VCI row is the total number of cells forwarded by this switch on this virtual circuit. The bottom value is the total number of cells with the CLP bit set to 1 received by this switch on this virtual circuit.

◆ **Note** ◆

If you add the number of received CLP=0 cells and CLP=1 cells (the bottom two values for each VPI/VCI row), the sum will equal the total received cells (the top value in the **Received Cells** column for each VPI/VCI row).

Information on the Ports for one CSM Board

To obtain status information on a single CSM board, you enter the **vcs** command along with the slot number for the CSM board, as follows:

vcs <slot>

where the **<slot>** is the slot number where the CSM board is installed. For example, if you wanted to view status information for the CSM board in slot 3, you would enter:

vcs 3

This command displays a screen similar to the following:

ATM Connection Statistics								
Slot	Port	VCI	Rx SDUs	Tx SDUs	Rx Cells	Tx Cells	Rx Octets	Tx Octets
3	1	100	0	9647	0	28465	0	1366320

CSM Connection Statistics						
Slot	Port	VPI	VCI	Received Cells/ Received CLP=0 Cells	Transmitted Cells/ Received CLP=1 Cells	
3	1	0	5	0	0	0
3	1	0	16	0	0	0
3	1	0	18	0	0	0
3	2	0	32	0	0	0
3	2	0	105	444	444	0
3	2	0	296	0	0	0
3	2	0	369	180	180	0
3	2	1	560	0	0	0
3	2	1	633	0	0	0

The first part of the display, which is labelled **ATM Connection Statistics**, provides information on the ATM access ports (if applicable). In the sample above, information is provided only on the two FCSM internal ports. Descriptions of the columns in this table are provided in Chapter 33, "Managing ATM Access Modules."

The second part of the display, which is labelled **CSM Connection Statistics**, provides information on the CSM module ports. Descriptions of the columns in this table are described earlier in *Viewing ATM Connection Statistics Table* on page 42-46.

Information on One Port

To obtain status information on a single CSM port, you enter the **vcs** command along with the slot number for the CSM board and the port number for which you want to receive information, as follows:

vcs <slot>/<port>

where **<slot>** is the slot number where the CSM board is installed and **<port>** is the port number on the CSM board. For example, if you want to view status information for port 2 on the CSM module in slot 3, you would enter:

vcs 3/2

This command displays a screen similar to the following:

CSM Connection Statistics					
Slot	Port	VPI	VCI	Received Cells/ Received CLP=0 Cells	Transmitted Cells/ Received CLP=1 Cells
3	2	0	32	0	0
3	2	0	105	444	444
3	2	0	296	0	0
3	2	0	369	180	180
3	2	1	560	0	0
3	2	1	633	0	0

Descriptions of the columns included in this display are described earlier in *Viewing ATM Connection Statistics Table* on page 42-46.

Information on One Virtual Path

To obtain status information on a single virtual path, you enter the **vcs** command along with the slot number for the CSM board, the port number, and the VPI number for the virtual path on which you want information, as follows:

```
vcs <slot>/<port> <vpi>
```

where **<slot>** is the slot number where the CSM board is installed, **<port>** is the port number on the CSM board, and **<vpi>** is the virtual path identifier. For example, if you wanted to obtain status information for the board in slot 3, port 2, and VPI 1, you would enter:

```
vcs 3/2 1
```

This command displays a screen similar to the following:

CSM Connection Statistics					
Slot	Port	VPI	VCI	Received Cells/ Received CLP=0 Cells	Transmitted Cells/ Received CLP=1 Cells
3	2	1	560	0	0
3	2	1	633	0	0

Descriptions of the columns included in this display are described earlier in *Viewing ATM Connection Statistics Table* on page 42-46.

Information on One Virtual Channel

To obtain status information on a single virtual channel, you enter the **vcs** command along with the slot number for the CSM board, the port number, the VPI number, and the VCI number for the virtual channel on which you want information, as follows:

```
vcs <slot>/<port> <vpi>/<vci>
```

where **slot** is the **<slot>** number where the CSM board is installed, **<port>** is the port number on the CSM board, and **<vpi>** is the virtual path identifier, and **<vci>** is the virtual channel identifier. For example, if you wanted to obtain status information for the board in slot 3, port 2, VPI 1, and VCI 369, you would enter:

```
vcs 3/2 1/633
```

This command displays a screen similar to the following:

CSM Connection Statistics					
Slot	Port	VPI	VCI	Received Cells/ Received CLP=0 Cells	Transmitted Cells/ Received CLP=1 Cells
3	2	1	633	0	0

Descriptions of the columns included in this display are described earlier in *Viewing ATM Connection Statistics Table* on page 42-46.

Viewing CSM Port and Connection Statistics

The **vcst** command can be used to display port and connection statistics for CSMs, such as the number of cells that are sent and received on a port, or for one connection on a specific port. The syntax for this command is as follows:

```
vcst <slot>/<port> [<vpi>/<vci>]
```

You use the **<slot>/<port>** parameters to specify the specific slot/port for which statistics are required. You can use the **<vpi>/<vci>** option to specify the connection for which statistics are required.

Displaying Port Statistics

As an example, to display the port statistics for Port 1 in Slot 3, you would enter:

```
vcst 3/1
```

at the system prompt. A screen similar to the following display will be shown.

Statistics for Slot/Port 3/1

Port Speed (cells/sec)	: 353208
Port Utilization - last minute	: Tx : 0.00 %, Rx : 0.00 %
Port Utilization - last 5 minutes	: Tx : 0.00 %, Rx : 0.00 %
Port Utilization - last hour	: Tx : 0.00 %, Rx : 0.00 %
Port Utilization - last 24 hrs	: Tx : 0.00 %, Rx : 0.00 %
Total Received Cells	: 2899800
Total Received CLP0 Cells	: 2899800
Total Received CLP1 Cells	: 0
EFCI Marked Cells	: 0
Total Transmitted Cells	: 390400
Total Discarded Cells	: 10
Unknown VPI/VCI Cells	: 10

The Port Statistics fields displayed by the **vcst** command appear under a heading that lists the slot number and port number of the CSM port (e.g., **Statistics for Slot/Port 3/1**), and include:

Port Speed. The speed in cells per second.

Port Utilization - last minute. The percentage of maximum cells per second transmitted and received within the last minute.

Port Utilization - last 5 minutes. The percentage of maximum cells per second transmitted and received within the last 5 minutes.

Port Utilization - last hour. The percentage of maximum cells per second transmitted and received within the last hour.

Port Utilization - last 24 hours. The percentage of maximum cells per second transmitted and received within the last 24 hours.

Total Received Cells. The total number of received cells on this port.

Total Received CLP0 Cells. The total number of received cells on this port with a cell loss priority designation 0.

Total Received CLP1 Cells. The total number of received cells on this port with a cell loss priority designation 1.

Viewing CSM Port and Connection Statistics

EFCI Marked Cells. The number of received cells marked with Explicit Forward Congestion Indication.

Total Transmitted Cells. The total number of transmitted cells on this port.

Total Discarded Cells. The total number of discarded cells on this port.

Unknown VPI/VCI Cells. The number of cells with unknown virtual path or virtual channel identifiers.

Displaying Connection Statistics

To display the connection statistics for Slot/Port 3/1 VPI/VCI 0/100, you would enter:

```
vcst 3/1 0/100
```

at the system prompt. A screen similar to the following display will be shown.

Statistics for Connection Slot/Port 3/1 0/100

Received Cells	: 2900551
Received CLP0 Cells	: 2900551
Received CLP1 Cells	: 0
Transmitted Cells	: 37438
Total CLP1 Discards	: 0
Total CLP0 Discards	: 0
Outgoing Connection	: 2/1 0/100
Received Cells	: 37438
Received CLP0 Cells	: 37438
Received CLP1 Cells	: 0
Transmitted Cells	: 2900551
Total CLP1 Discards	: 0
Total CLP0 Discards	: 0

The Connection Statistics fields displayed by the **vcst** command appear under a heading that lists the slot number, port number and VPI/VCI identifiers of the connection on the CSM port (e.g., **Statistics for Connection Slot/Port 3/1 0/100**), and include:

Received Cells. The total number of received cells.

Received CLP0 Cells. The total number of received cells with a cell loss priority designation 0.

Received CLP1 Cells. The total number of received cells with a cell loss priority designation 1.

Transmitted Cells. The total number of transmitted cells on this port.

Total CLP1 Discards. The total number of discarded cells with a cell loss priority designation 1.

Total CLP0 Discards. The total number of discarded cells with a cell loss priority designation 0.

Outgoing Connection. The outgoing slot/port/virtual path identifier/virtual channel identifier of the virtual channel.

Received Cells. The total number of received cells.

Received CLP0 Cells. The total number of received cells with a cell loss priority designation 0.

Received CLP1 Cells. The total number of received cells with a cell loss priority designation 1.

Transmitted Cells. The total number of transmitted cells on this port.

Total CLP1 Discards. The total number of discarded cells with a cell loss priority designation 1.

Total CLP0 Discards. The total number of discarded cells with a cell loss priority designation 0.

Viewing Connection Receive Error Statistics

The **vcrs** command displays the ATM receive error statistics table. This table provides a summary of receive activity on a virtual channel basis. The following screen is a sample of the output from the **vcrs** command:

ATM Connection Rx SDU Error Statistics

Slot	Port	VCI	Discards	Errors	Invalid Sz	No Buffers	Trash	CRC Errors
3	1	100	0	0	0	0	0	0

ATM Connection Rx Cell Error Statistics

Slot	Port	VCI	Discards	Errors	No Buffers	Trash	CRC Errors
3	1	100	0	0	0	0	0

CSM Connection Rx Error Statistics

Slot	Port	VPI	VCI	Dx Congestion CLP=0/ Dx GCRA A for CLP=0/ Dx GCRA B for CLP=0	Dx Congestion CLP=1/ Dx GCRA A for CLP=1/ Dx GCRA B for CLP=1
3	1	0	5	0	0
				0	0
				0	0
3	1	0	16	0	0
				0	0
				0	0
3	1	0	18	0	0
				0	0
				0	0
3	2	0	32	0	0
				0	0
				0	0
3	2	0	105	0	0
				0	0
				0	0
3	2	0	296	0	0
				0	0
				0	0
3	2	0	369	0	0
				0	0
				0	0
3	2	0	560	0	0
				0	0
				0	0
3	2	0	633	0	0
				0	0
				0	0
5	4	0	5	0	0
				0	0
				0	0
5	4	0	16	0	0
				0	0
				0	0
5	4	0	18	0	0
				0	0
				0	0

The first part of the display, which is labelled **ATM Connection Rx SDU Error Statistics**, provides information on the ATM access module ports (if applicable). In the sample above, information is provided only on the two FCSM internal ports. Descriptions of the columns in this table are provided in Chapter 33, “Managing ATM Access Modules.”

Descriptions of the second part of the display, which is labelled **CSM Connection Rx Error Statistics**, are provided as follows.

Slot/Port/VPI/VCI. These columns identify the virtual circuit for which statistics are displayed. The Slot and Port indicate the physical interface where this virtual circuit is configured. The VPI is the Virtual Path Identifier for the circuit and the VCI is the Virtual Channel Identifier for the circuit.

The next two columns provide information on the number of cells discarded under several conditions. The first column provides information on cells with the CLP bit set to 0; the second column describes cells with the CLP bit set to 1.

Dx Congestion CLP=0. This value displays as the top value in the first column for each virtual circuit. It is the number of CLP=0 cells that were discarded during a congestive state. It does *not* include cells discarded due to traffic contract violations. The cells counted here were discarded due to the priority level of their virtual channel (i.e., the QoS and/or User Priority levels were lower than other connections on this CSM port). Some virtual channels have higher priority than others. For example, a virtual channel with a QoS for CBR traffic has a higher priority than a channel with a QoS for ABR traffic. This statistic lists the cells discarded for these priority-based reasons.

Dx GCRA A for CLP=0. This value displays as the middle value in the first column for each virtual circuit. It is the number of CLP=0 cells that were discarded because they violated the traffic policing algorithm for the *first* leaky bucket. The policing algorithm describes what happens to traffic when it exceeds traffic contract parameters, such as PCR, SCR, and MBS. Depending on the Class of Service on the circuit and CLP bit setting of the cell, cells that violate the traffic contract will either be tagged or discarded. See Chapter 41, “Managing Cell Switching Modules (CSMs),” for more information on traffic policing and Class of Service.

Note

This statistic does not count CLP=0 cells that were discarded during a congestive state; it counts only CLP=0 cells that were discarded during a time of no congestion.

Dx GCRA B for CLP=0. This value displays as the bottom value in the first column for each virtual circuit. It is the number of CLP=0 cells that were discarded because they violated the policing algorithm for the *second* leaky bucket. It is technically the same as the **Dx GCRA A for CLP=0** statistic, except it counts only traffic in the second leaky bucket. See the above **Dx GCRA A for CLP=0** description for further information.

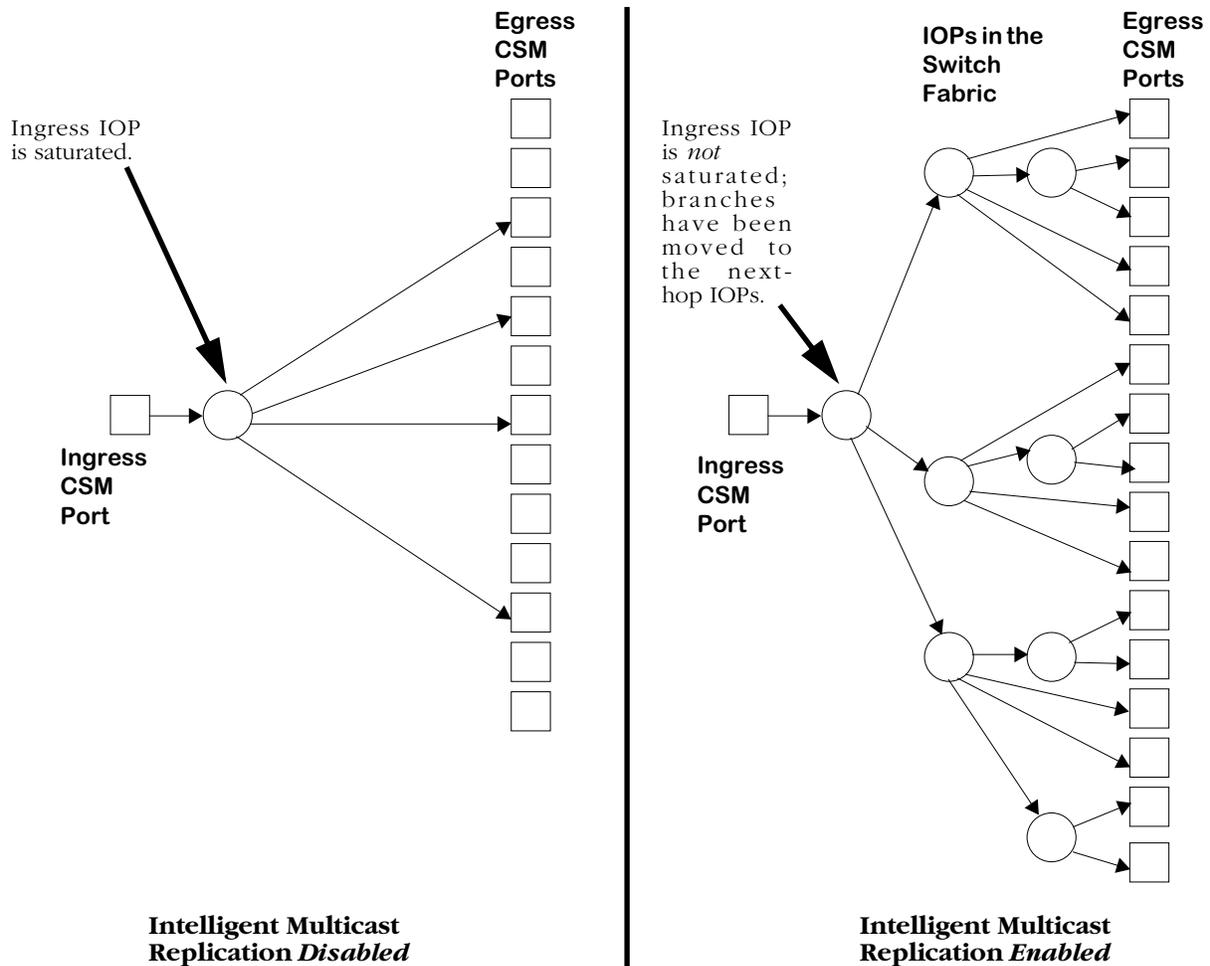
Dx Congestion for CLP=1. This value displays as the top value in the second column for each virtual circuit. It is the number of CLP=1 cells that were discarded during a congestive state. It does *not* include cells discarded due to traffic contract violations. The cells counted here were discarded due to the priority level of their virtual channel (i.e., the QoS and/or User Priority levels were lower than other connections on this CSM port). Some virtual channels have higher priority than others. For example, a virtual channel with a QoS for CBR traffic has a higher priority than a channel with a QoS for ABR traffic. This statistic lists the cells discarded for these priority-based reasons.

Intelligent Multicast Replication

In point-to multipoint (PTOMP) connections, virtual channels are mapped from an ingress CSM port to two or more egress CSM ports. In this configuration, cells branch from an Alcatel-proprietary cell fabric ASIC, known as an Input-Output Processor (IOP), connected to the ingress port (i.e., an “ingress IOP”) to egress CSM port(s). The number of branches at the ingress IOP effectively limits the cell input rate.

Intelligent multicast replication is a software algorithm that increases the input cell rate in PTOMP connections by reducing the number of branches at the ingress IOP. This algorithm uses existing branches from the ingress IOP instead of “blindly” branching from an ingress IOP. Instead, this algorithm creates branches at the loopback port of the next-hop IOP. In addition, idle IOPs in the switch are also used in the same manner. (See *Multicast Replication Trees* on page 42-58 for more information on replication trees.)

The figure below provides a side-by-side comparison between the cell fabric of a switch where intelligent multicast replication has not been enabled and a switch where it has been enabled. In the switch without intelligent multicast replication, the ingress IOP has been saturated — the cell input rate *cannot* increase. The switch with intelligent multicast replication enabled, on the other hand, has more egress ports and at the same time can still increase its effective cell input rate.



Intelligent Multicast Replication Performance Gain

Intelligent multicast replication is supported on all OC-3 CSM modules (CSM-155-8, CSM-155-8S, CSM-155C-8, FCSM I). It is *not* supported on OC-12 (CSM-622, FCSM II), CSM-A25, or CSM-U modules. However, these modules can join as a “leaf” (i.e., their CSM ports can be used as egress ports) in the intelligent multicast replication tree. In addition, the input cell rate will *not* improve for non OC-3 modules if you enable intelligent multicast replication.

◆ **Note** ◆

Intelligent multicast replication is *not* supported on OC-3 ATM access modules (i.e., ASM, ASM2, and ASX modules).

The following User Interface (UI) commands in the ATM menu are used to support intelligent multicast replication:

imce. This command enables intelligent multicast replication. It is described in *Enabling Intelligent Multicast Replication* on page 42-59.

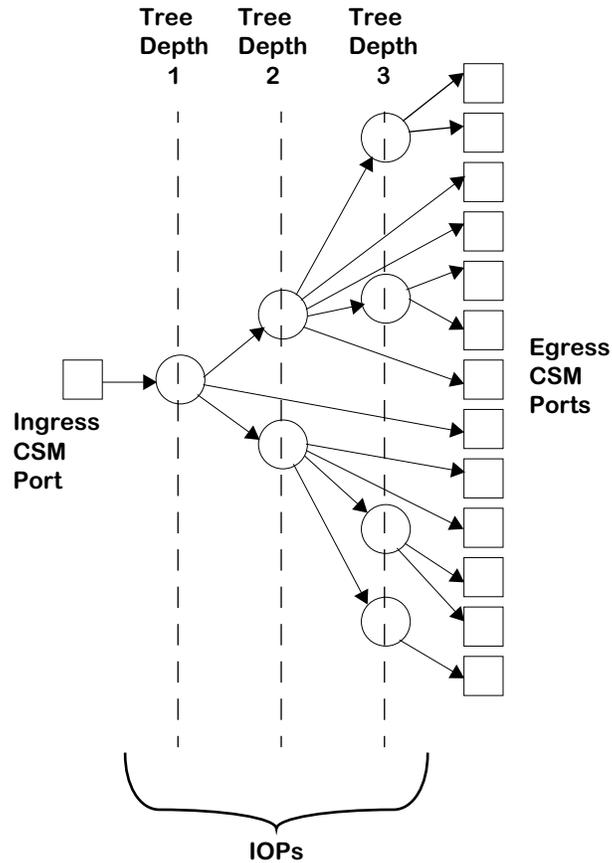
imcr. This command disables intelligent multicast replication. It is described in *Disabling Intelligent Multicast Replication* on page 42-59.

imci. This command displays the gain in performance from intelligent multicast replication. It is described in *Displaying Intelligent Multicast Replication Performance Gain* on page 42-60.

imcd. This command displays the intelligent multicast replication tree. It is described in *Displaying Intelligent Multicast Replication Trees* on page 42-61.

Multicast Replication Trees

The figure below shows a diagram of the paths of cells in a point-to-multipoint connection. Cells entering the ingress CSM are processed by an IOP, which replicates them so they can be sent to other egress CSM ports and/or IOPs within the switch. These IOPs will, depending on the number of egress connections, also replicate cells. This process of replicating cells by IOPs is also known as a *replication tree*.



Point-to-Multipoint Replication Tree

In the figure above the ingress CSM port is at tree depth 1; subsequently, tree depth increases. There is a tree depth of three (3) since three levels of IOPs are involved between the ingress CSM port and the egress CSM ports. You can use the **imcd** command, which is described in *Displaying Intelligent Multicast Replication Trees* on page 42-61, to display the parameters for intelligent multicast replication trees.

Enabling Intelligent Multicast Replication

To enable intelligent multicast replication on all OC-3 modules in your switch, you use the **imce** command. To use this command, enter

imce

at the system prompt. The following prompt will be displayed.

Do you want to enable Intelligent multicast Feature? (y) :

Enter **y** (the default) to enable intelligent multicast replication or **n** to exit the command. If you entered **y**, the following message will be displayed.

Intelligent multicast Feature will be enabled upon reboot.

You *must* reboot your switch for intelligent multicast replication to take effect.

Disabling Intelligent Multicast Replication

To disable intelligent multicast replication on all OC-3 modules in your switch, you use the **imcr** command. To use this command, enter

imcr

at the system prompt. The following prompt will be displayed.

Do you want to disable Intelligent multicast Feature? (y) :

Enter **y** (the default) to disable intelligent multicast replication immediately or **n** to exit the command. If you entered **y**, the following message will be displayed.

Intelligent multicast Feature disabled.

Since this takes effect immediately you do not need to reboot your switch.

Displaying Intelligent Multicast Replication Performance Gain

To display the gain in performance from intelligent multicast replication, you use the **imci** command. The syntax for this command is as follows.

```
imci <slot>/<port> [<vpi>/<vci>]
```

You can use the **<vpi>/<vci>** option to specify a specific virtual channel. If you do not use this option, then the performance gain for all virtual channels on the port you selected will be displayed.

For example, to display the intelligent multicast replication gain for all virtual channels on Port 1 in Slot 3, enter

```
imci 3/1
```

at the system prompt. A screen similar to the following will be displayed.

CSM Intelligent Multicast Tree

Incoming				No. of	Max. BW	Worst case	Max. BW	Gain
-----				Branches	in Mbps	Branches	in Mbps	in
Slot	Port	VPI	VCI	with	with	with	with	times
====	====	====	====	IMC	IMC	IMC	IMC	=====
Disabled	Disabled	Enabled	Enabled					
3	1	0	453	20	16.5	3	110.0	6.66
3	1	0	455	2	115.0	2	115.0	1.0
3	1	0	458	20	16.5	3	110.0	6.66
3	1	0	461	2	115.0	2	115.0	1.0

The fields displayed by the **imci** command are described below.

Incoming Slot. The incoming slot number of the virtual channel.

Incoming Port. The incoming port number of the virtual channel.

Incoming VPI. The incoming virtual path identifier of the virtual channel.

Incoming VCI. The incoming virtual channel identifier of the virtual channel.

No. of Branches with IMC Disabled. The maximum number of branches at any node of the replication tree if intelligent multicast replication has *not* been enabled.

Max. BW in Mbps with IMC Disabled. The maximum bandwidth (in Megabits per second) for cells this virtual channel in PTOMP connections if intelligent multicast replication has *not* been enabled.

Worst case Branches with IMC Enabled. The maximum number of branches at any node of the replication tree if intelligent multicast replication *has* been enabled.

Max. BW in Mbps with IMC Enabled. The maximum bandwidth (in Megabits per second) for cells this virtual channel if intelligent multicast replication *has* been enabled.

Gain in time. The ratio between enabling and disabling intelligent multicast replication for this virtual channel. The higher the value in this field the greater the gain in maximum bandwidth will be for this virtual channel.

Displaying Intelligent Multicast Replication Trees

To display all intelligent multicast replication trees on an ingress CSM port in point-to-multi-point (PTOMP) connections, you use the **imcd** command. The syntax for this command is as follows:

```
imcd <slot>/<port> [<vpi>/<vci>]
```

You can use the **<vpi>/<vci>** option to specify a specific virtual channel. If you do not use this option, then the intelligent multicast replication trees for all virtual channels on the port you selected will be displayed.

For example, to display the intelligent multicast replication trees for all virtual channels for Port 1 in Slot 3, enter

```
imcd 3/1
```

at the system prompt. The following prompt will be displayed.

```
Do you want to verify conn records? (y) :
```

Enter **y** to verify connection records or **n** to ignore this option. The following is a sample display of one (1) intelligent multicast replication tree on a port. A complete display produced by the **imcd** command consists of all intelligent multicast replication trees on an ingress CSM port in PTOMP connections.

```
L ==> Loopback port of the IOP serving slot/port  
P ==> Physical port
```

CSM Intelligent Multicast Tree											
Tree Depth	Incoming					Outgoing					Port Type
	Slot	Port	VPI	VCI	IOP	Slot	Port	VPI	VCI	IOP	
1	3	1	0	453	4	4	L	0	8192	9	L
						4	L	0	8192	8	L
						4	1	0	82	8	P
2	4	L	0	8192	9	4	3	0	86	9	P
						5	L	0	8192	14	L
						7	1	0	107	21	P
	4	L	0	8192	8	6	L	0	8192	16	L
						3	1	0	454	4	P
3	5	L	0	8192	14	5	L	0	8192	13	L
						6	L	0	8192	19	L
						5	6	0	93	14	P
	6	L	0	8192	16	4	L	0	8192	10	L
						6	2	0	84	16	P

— Output continues on next page —

Intelligent Multicast Replication

```

4      5  L  0  8192 13  5  4  0  83  13  P
      6  L  0  8192 19  5  L  0  8192 12  L
      6  8  0  92  19  P
      4  L  0  8192 10  7  2  0  700 22  P
      4  5  0  82  10  P
5      5  L  0  8192 12  9  L  0  8192 31  L
      5  2  0  423 12  P
6      9  L  0  8192 31  5  L  0  8192 15  L
      9  7  0  122 31  P
7      5  L  0  8192 15  6  L  0  8192 18  L
      5  8  0  124 15  P
8      6  L  0  8192 18  4  L  0  8192 11  L
      6  6  0  129 18  P
9      4  L  0  8192 11  9  L  0  8192 30  L
      4  7  0  125 11  P
10     9  L  0  8192 30  6  L  0  8192 17  L
      9  5  0  78  30  P
11     6  L  0  8192 17  9  L  0  8192 28  L
      6  4  0  86  17  P
12     9  L  0  8192 28  9  L  0  8192 29  L
      9  1  0  74  28  P
13     9  L  0  8192 29  8  2  0  80  26  P
      9  3  0  80  29  P

```

Multicast tree displayed above is successfully validated with the information stored in IOP SRAM.

The legend at the top of the display provides a definition of non numeric values in the **Incoming Port**, **Outgoing Port**, and **Port Type** fields. A **P** in these fields indicates that port is a physical port in the switch whereas an **L** indicates that the port is a loopback port on an IOP.

If you selected the option to verify the connection records (as shown on the previous page), then a message will be printed after each display for a replication tree that will state if the multicast replication tree has been verified against the data stored in the Static RAM (SRAM) of the CSMs.

The fields displayed by the **imcd** command are described below.

Tree Depth. The tree depth indicates one (1) plus the number of hops between the incoming IOP (displayed in the **Incoming IOP** field described below) and the ingress IOP.

Incoming Slot. The incoming slot number of the virtual channel.

Incoming Port. The incoming port number of the virtual channel.

Incoming VPI. The incoming virtual path identifier of the virtual channel.

Incoming VCI. The incoming virtual channel identifier of the virtual channel.

Incoming IOP. The IOP number (which is assigned by the switch) for the incoming IOP for this tree depth.

Outgoing Slot. The outgoing slot number of the virtual channel.

Outgoing Port. The outgoing port number of the virtual channel.

Outgoing VPI. The outgoing slot virtual path identifier of the virtual channel.

Outgoing VCI. The outgoing slot virtual channel identifier of the virtual channel.

Outgoing IOP. The IOP number (which is assigned by the switch) for the outgoing IOP for this tree depth.

Port Type. This field will display an **L** if the next hop from the outgoing IOP is a loopback port on another IOP, or a **P** if the next hop is a physical port on a CSM.

CSM-ABT Traffic Shaping

Different network links typically cannot support the same traffic contracts. Some links can easily handle the kinds of peak traffic rates that can congest other links, resulting in varying levels of network traffic congestion. To reduce the risk of ATM backbone congestion, CSM-ABT Traffic Shaping flow contracts can be applied to outgoing traffic flows across ATM links. Depending on the traffic type, this feature can help ensure that outgoing traffic flows won't oversubscribe assigned bandwidth rates, promoting maximum traffic throughput.

Depending on the CSM port configuration parameters that you have specified (*see below*), CSM-ABT Traffic Shaping uses the following algorithms to shape outgoing traffic:

- TSS (Traffic Scheduling System) - this algorithm shapes outgoing traffic based on the Transport Priority you specified.
- WRR (Weight Round Robin) - this algorithm sends traffic based on the User Priority you specified (*from 0-15, with 0 indicating highest priority*). To use WRR (i.e., when the TSS has nothing to send), you must specify:
 - **Transport Priority: UBR**
 - **Requested RX Traffic Descriptor Type: None**
 - **User Priority: 0-15**

These algorithms require the following transport priorities and traffic descriptors:

Algorithm	Transport Priority	Traffic Descriptor
TSS	CBR	PCR, CDVT
TSS	ABR	PCR, CDVT
TSS	Shaped UBR	PCR, CDVT
TSS	rt-VBR	PCR, SCR, MBS, CDVT
TSS	nrt-VBR	PCR, SCR, MBS, CDVT
WRR	Unshaped UBR	User Priority

To utilize CSM-ABT Traffic Shaping, you must first specify parameters for CSM port configuration commands. There are two ways to do this:

- The **csm pvc** CLI (Command Line Interface) commands can be used to create and/or modify a PVC connection. See the chapter titled, “CSM Commands” in the *Text-Based Configuration CLI Reference Guide* for information about CSM Connection Commands.
- The **cvc** and **mvc** UI (User Interface) commands can be used to create and/or modify a PVC connection. See Chapter 41, “Managing Cell Switching Modules (CSMs)” for details.

◆ **Note** ◆

CSM-ABT Traffic Shaping is factory enabled (default), and is automatically re-enabled whenever the switch reboots. This feature is supported in CLI (Command Line Interface) Mode on CSM-ABT-155F submodules, but is not supported in UI (User Interface) Mode.

Using the CLI to Configure CSM Traffic Shaping

The CLI is a form of text-based configuration in which you connect to an active switch, then manually enter single-line, CLI configuration commands. You can enter these commands using one of two methods:

- (a) **On-Line Configuration**, entering commands at the CLI prompt.
- (b) **Off-Line Configuration**, entering commands in a standalone text editor, such as Microsoft Word, WordPad, or NotePad.

When Off-Line Configuration is used, the resulting configuration file is placed in the switch's **/flash** or **/simm** directory, and changes are applied to the switch by issuing a **configuration** command.

Off-Line Configuration is useful in that a configuration file can be viewed or edited offline at any time, then uploaded and applied to additional switches in the network. This makes it easy for users to clone switch configurations. Also, the ability to store comprehensive network information in a single file facilitates troubleshooting, testing, and overall understanding of the network configuration.

For information on using the CLI, along with a list of the CSM traffic shaping commands, see the chapter titled, "CSM Commands" in the *Text-Based Configuration CLI Reference Guide*.

Software Requirements

Before you can use the CLI to configure CSM traffic shaping, you must have the following software installed:

1. The switch must be running Software Release 4.4 or later.
2. The **text_cfg.img** file must be loaded into your switch's flash file system.
3. The **cell_mpg.img** file must be loaded into your switch's flash file system.
4. The **sonet.img** file must be loaded into your switch's flash file system.
5. The **pm_ctm.exe** file must be loaded into your switch's flash file system.

Items (1) and (2) are requirements for using the Text-Based Configuration feature. Items (3), (4) and (5) are requirements of the CSM Traffic Shaping function.

For information on how to use FTP or ZMODEM to load files onto the switch, refer to Chapter 9, "Installing Switch Software."

CLI Conventions

The CSM Traffic Shaping commands are documented using the following CLI syntax conventions:

CLI Conventions

boldface	Indicates a CLI command. Example: view csm shaping slot/port
<i>italicized text</i>	Indicates variable information entered by the user. Example: IP addresses, port numbers, etc. See example for “curly braces.”
[] (Straight Brackets)	Indicate <i>optional</i> command parameters. Commands themselves may have bracketed portions, indicating that the command can be entered in an abbreviated form and still be recognized by the system. See example for “curly braces.”
{ } (Curly Braces)	Indicate that the user must choose between one or more parameters. Example: csm shaping slot/port [no] traffic { cbr rtvbr nrtvbr abr ubr all }
(Vertical Line)	Used to separate parameter choices within a command string. See example for “curly braces.”

Global Definitions

The CLI Traffic Shaping commands also use certain global definitions.

Global Definitions

slot/port	A port identifier is defined by slot and port number, separated from each other by a slash (/). Example: 5/3
-----------	---

Traffic Shaping Configuration Examples

This section offers examples on how to activate, enable or disable CSM Traffic Shaping using the CLI. These commands are valid for atm connections. Each example begins with a statement of the full CLI command, along with all optional parameters. However, only certain optional parameters are illustrated. For a detailed explanation of each of the parameters, refer to the chapter titled, “CSM Commands” in the *Text-Based Configuration CLI Reference Guide*.

Activating CSM Traffic Shaping

```
csm pvc slot/port vpi [ vci ] shap
```

This CLI command can be used to activate traffic shaping on a CSM-ABT-155F daughterboard module and create a connection for a CSM-ABT physical port. This command should be used to activate CSM-ABT Traffic Shaping after a connection has been created and all necessary parameters have been specified or modified.

Enabling/Disabling CSM Traffic Shaping

```
csm shaping slot/port [ no ] traffic { cbr | rtvbr | nrtvbr | abr | ubr | all }
```

You can use this CLI command to enable or disable CSM traffic shaping for specific service categories and types of traffic between a CSM-ABT Port and another switch’s ATM Port. When enabled, traffic is shaped based on the traffic contracts (service requirements) previously specified (e.g., pcr, scr). When disabled, traffic is shaped at the line rate (maximum speed of the port).

- **cbr** - Constant Bit Rate (Voice or Video Traffic); intended for traffic with stable data transmission rate requirements. Examples include AAL-1 traffic, such as Circuit Emulation and fixed rate video.
- **rtvbr** - Real-Time Variable Bit Rate (Video Traffic); intended for traffic with varying data transmission rate requirements, where CDV (cell delay variation) is specified. Examples include AAL-5 traffic, such as interactive compressed video.
- **nrtvbr** - Non-Real-Time Variable Bit Rate (Frame Relay); intended for traffic with varying data transmission rate requirements, where CDV (cell delay variation) *is not* specified. Examples include AAL-5 traffic, such as Multimedia or E-mail.
- **abr** - Available Bit Rate (Data Traffic); utilizes remaining available bandwidth (based on flow control) after **cbr** and **vbr** services have been accounted for. Quality of Service (QoS) guarantees are not supported. Typically used for AAL-5 traffic.
- **ubr** - Unspecified Bit Rate (Data Traffic); offers “best-effort” delivery, but doesn’t support Connection Admission Control (CAC) refusal due to bandwidth unavailability, Quality of Service (QoS) guarantees or flow control. Typically used for AAL-5 traffic.
- **all** - Supports multiple traffic types, where the required Bit Rates, traffic types and service categories may vary, including **cbr**, **rtvbr**, **nrtvbr**, **abr**, and **ubr**.

Traffic Shaping Configuration Examples

As an example, if you wanted to enable CSM Traffic Shaping on Slot 4, Port 1 for all traffic types, you would enter the following command at the CLI prompt:

```
csm shaping 4/1 traffic all
```

If the command is accepted, you should see a display similar to the following:

```
Set done
```

If the command is not accepted, an error message will be displayed (such as a Slot, Port or Command Syntax Error).

◆ Note ◆

CSM Traffic Shaping is factory enabled (default), and will automatically be re-enabled whenever the switch reboots. This feature is supported in CLI (Command Line Interface) Mode on CSM-ABT-155F submodules, but is not supported in UI (User Interface) mode.

Viewing CSM Traffic Shaping

```
view csm shaping slot/port
```

To view the status of CSM traffic shaping, enter the following command:

```
-> view csm shaping slot/port
```

A screen similar to one of the following examples will be displayed:

Slot	Line	(m/p)	cbr	rtvbr	nrtvbr	abr	ubr
====	====	====	===	====	====	===	===
4	1	0/0	1	1	0	1	0

Slot	Line	(m/p)	cbr	rtvbr	nrtvbr	abr	ubr
====	====	====	===	====	====	===	===
4	1	0/0	1	1	0	1	0
4	2	0/1	1	1	1	1	1

The display screens shown above include **Slot**, **Line** (*port*), and **module/port** (module location) indicators, and provide traffic shaping status (**1 = Enabled**, **0 = Disabled**) for **cbr**, **rtvbr**, **nrtvbr**, **abr**, and **ubr** traffic types.

Disabling CSM Traffic Shaping

```
csn shaping slot/port no traffic [ cbr | rtvbr | nrtvbr | abr | ubr | all ]
```

To disable CSM traffic shaping, enter one of the following commands, depending on the traffic type (service category) that was previously specified (**cbr**, **rtvbr**, etc.):

- > **csn shaping slot/port no traffic**
- > **csn shaping slot/port no traffic all**
- > **csn shaping slot/port no traffic cbr**

You should see a display similar to the following:

```
Set done
```

Switching from CLI Mode to UI Mode

To switch from CLI mode to UI mode, type **ui** at the CLI prompt (->), as shown below:

```
-> ui
```

A prompt similar to the following will be displayed:

```
/=>
```

To switch back to CLI mode from UI mode, type **cli** at the UI prompt (/=>), as shown below:

```
/=> cli
```

A display similar to the following will appear:

```
Entering command line interface.
```

```
->
```

◆ Important Note ◆

See the chapter titled, “CSM Commands” in the *Text-Based Configuration CLI Reference Guide* for additional information on using CLI commands.

43 Inverse Multiplexing Over ATM (IMA)

Inverse Multiplexing over ATM (IMA) increases the bandwidth of ATM traffic by combining several physical links into a single virtual link. On the transmitting (or *near-end*) side of the physical links, IMA combines (multiplexes) an individual ATM cell stream in a cyclical fashion across physical links of an IMA *group*. Cells in the IMA group are transmitted to the receiving (or *far-end*) side of the links. The far-end side of the links disassembles (demultiplexes) the IMA group back into an individual IMA cell stream.

Alcatel's implementation is fully compliant with the *ATM Forum Inverse Multiplexing for ATM (IMA) Specification*, Version 1.0, dated July 1997 (document No. af-phy-0086.000), and the *ATM Forum Inverse Multiplexing for ATM (IMA) Specification*, Version 1.1, dated March 1999 (document No. af-phy-0086.001).

◆ Note ◆

IMA operates between the physical interface and the ATM layer of the ATM reference model. All of the features that Alcatel Internetworking Division supports on ATM interfaces are supported in Alcatel's IMA hardware and software.

The following are some of the benefits of using IMA in a wide-area network (WAN):

Scalability. As the demand for bandwidth increases, additional links can be added. For example, you could configure an IMA group initially with two T1 or E1 lines and later add additional T1 or E1 lines as the needs for bandwidth increase.

IMA provides a solution for organizations with bandwidth needs greater than those provided by T1 (1.544 Mbps) or E1 (2.048 Mbps) lines, but less than T3 (44.736 Mbps) or E3 (34.368 Mbps) lines. Therefore, network administrators can avoid the higher costs of T3 and E3 lines.

Reliability. If a link for an IMA group fails, ATM cells will continue to be transmitted (although at a lower bandwidth).

Load balancing. By consolidating ATM traffic over multiple links of an single IMA group, T1 or E1 circuits can be used much more efficiently.

IMA Hardware

Currently, you can implement IMA groups with the CSM-AB-IMA-DS1/E1-8W adapter board for the CSM-U and CSM-U+ switching modules. You can have up to four (4) IMA groups over eight (8) ports (links). For example, you can combine four physical T1 links transmitting at 1.544 Mbps into a single virtual link transmitting at approximately 6 Mbps. See Chapter 40, “Cell Switching Modules (CSMs),” for a detailed description of this submodule.

◆ Important Note ◆

IMA is *not* supported on other T1/E1 modules, such as the CSM-AB-T1/E1-4W and CSM-AB-CE-T1/E1 adapter boards.

IMA Software

You can create, modify, and display an IMA group and its links through Network Management Software (NMS), User Interface (UI) commands, and Command Line Interface (CLI) commands. This chapter documents UI commands, which are part of the IMA submenu (described in *The IMA Submenu* on page 43-13). See the online documentation for descriptions of NMS IMA software. See the *WAN Text-Based Configuration Reference Manual* for CLI commands.

IMA Configuration Overview

Follow the steps below to create an IMA group. All of these steps use User Interface (UI) commands that are part of the IMA submenu, which is described in *The IMA Submenu* on page 43-13. These steps present a very broad outline; all of these steps are described in greater detail later in this chapter. Instructions for configuring a sample IMA network are shown in *IMA Application Example* on page 43-8.

◆ Note ◆

You *must* install the **ima.img** image file in your switch before you can use IMA hardware or software.

Step 1. Create IMA Group on Both Sides of the Link

You create IMA groups with the **igpa** command, which is described in greater detail in *Creating IMA Groups* on page 43-15.

Step 2. Assign Links to the IMA Group

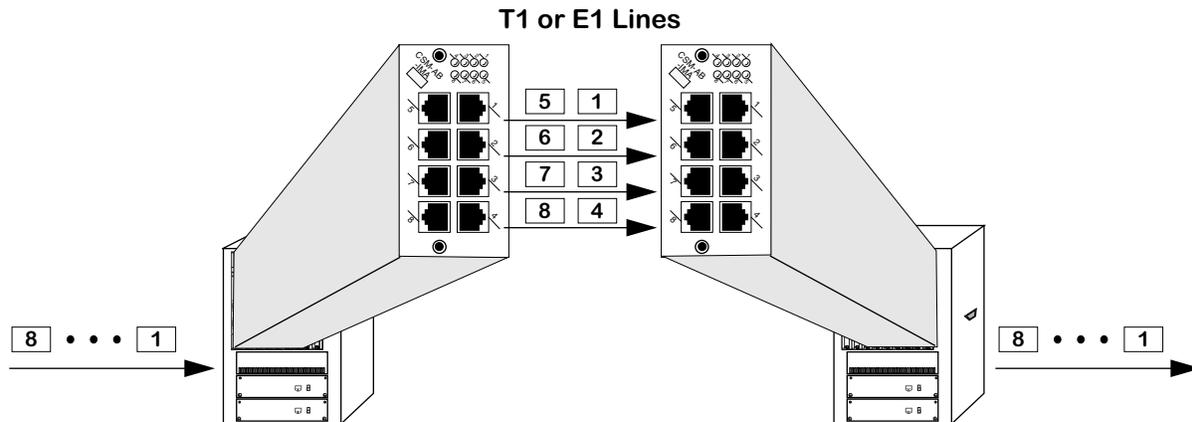
The **igpa** command only creates logical groups; it does not assign them to any ports (links). To assign logical IMA groups to physical links, use the **igpmem** command, which is described in greater detail in *Adding and Modifying IMA Group Membership* on page 43-18.

Step 3. Set Global IMA Parameters (Optional)

IMA submenu commands are available that allow you to assign logical IMA group parameters and physical IMA link parameters globally. For example, if you had an IMA group with four links over T1 lines and you wanted to set Extended SuperFrame (ESF) frame format, you could use the **igpm** command (described in *Modifying IMA Groups* on page 43-21) to set ESF frame format on all the ports in the IMA group in one step.

IMA Process Overview

Multiplexing of ATM cells is done on a cell by cell basis. As shown in the figure below, ATM cells are transmitted in a cyclical (i.e., “round robin”) fashion among links. The links are grouped to form higher bandwidth logical links. These logical links, known as an IMA group, have a transmit rate that is approximately the sum of the physical links.



❶ ATM cell stream enters near end side of the IMA group and is multiplexed into IMA frames over multiple IMA links.

❷ IMA frames are transmitted from the near end of the link to the far end of the link in a round robin fashion. (See *Typical IMA Frame Format* on page 43-5 for more information on IMA frames.)

❸ IMA frames are demultiplexed into the original ATM cell stream, which exits the far end of the IMA group.

IMA Multiplexing and Demultiplexing Process

The IMA implementation creates IMA Control Protocol (ICP) cells that contain information (e.g., IMA configuration, synchronization, status, and defect information) which permits reconstruction of the ATM cell stream at the receiving end. In addition, the IMA implementation will create filler cells in the IMA group to maintain a constant rate of transmission.

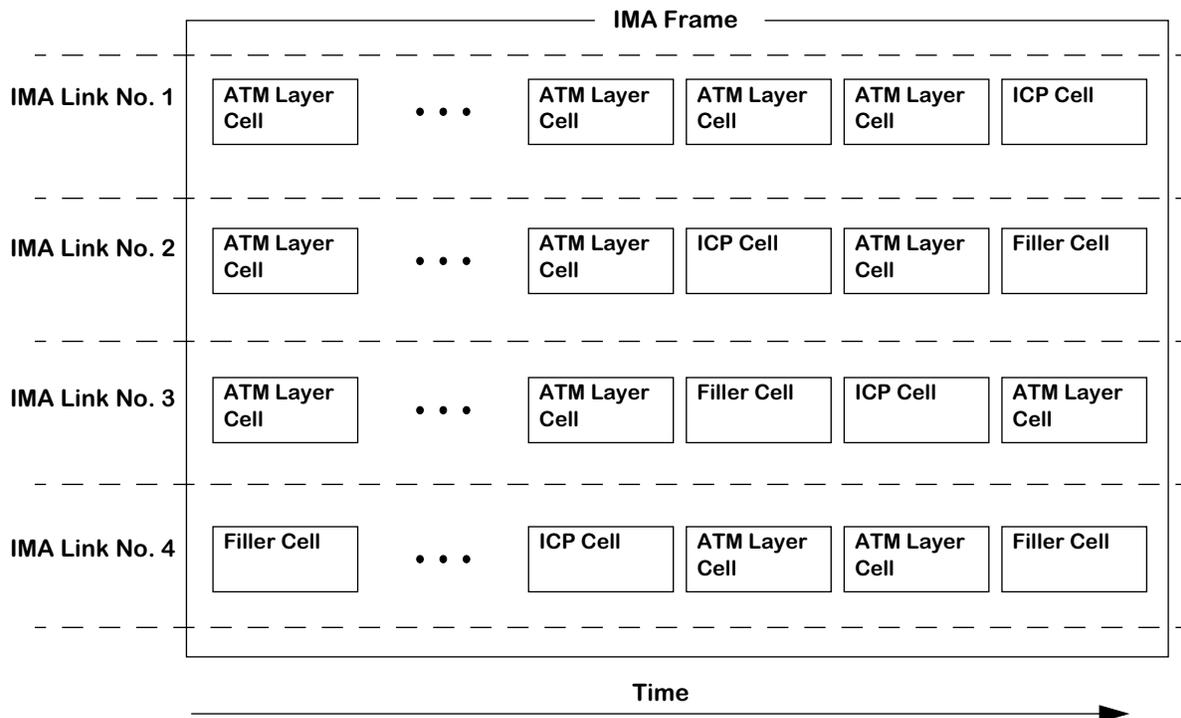
Stuff cells (i.e., repetition of ICP cells over one IMA link to compensate for timing differences with other links within the IMA group) are sent to adjust link speed variation. All of these cells are assembled into IMA frames 128 bytes long (see figure on the following page).

Demultiplexing of IMA groups is done at the far end of the IMA link. The ATM cell stream is reconstructed from information in ICP cells. The ATM cell stream is passed to the ATM layer while filler and ICP cells are discarded.

Adding and Deleting Links in an IMA Group

If a link fails, the IMA implementation will automatically use the remaining good links only. Bandwidth will be reduced and loss of cells is possible when the link initially fails. If a link is disabled intentionally, the IMA implementation will notify the far-end of the link and gracefully remove the link from the group. The bandwidth will be reduced but no cells will be lost.

You can also add links without taking the IMA group off-line. Bandwidth will be increased and no cells will be lost.



Typical IMA Frame Format

Cell Switching Module (CSM) Ports and IMA Groups (CSM-AB-IMA-DS1/E1-8W Submodule)

You can assign Cell Switching Module (CSM) port numbers to IMA groups on the CSM-AB-IMA-DS1/E1-8W submodule. The switch treats IMA groups just like individual ports on other CSM modules (e.g., the CSM-155F).

For example, you can create Permanent Virtual Circuits (PVCs) with the **cvc** command and soft PVCs with the **scvc** command on IMA groups. (See Chapter 41, “Managing Cell Switching Modules (CSMs),” for more information on CSM ports, VCs, ATM traffic parameters, and the **cvc** and **scvc** commands.)

Virtual paths, point-to-point virtual circuits (VCs), and point-to-multipoint (multicast) VCs can be created on IMA groups. Quality of Service (QoS) and other ATM traffic parameters are also supported. In addition, switched virtual circuits (SVCs) are also supported.

Sample IMA Network

The figure on the following page shows how IMA can be used to send ATM traffic from a corporate headquarters to two branch offices across low-cost public T1 or E1 lines. The OmniSwitches in all three offices are configured with both cell switching and frame switching modules.

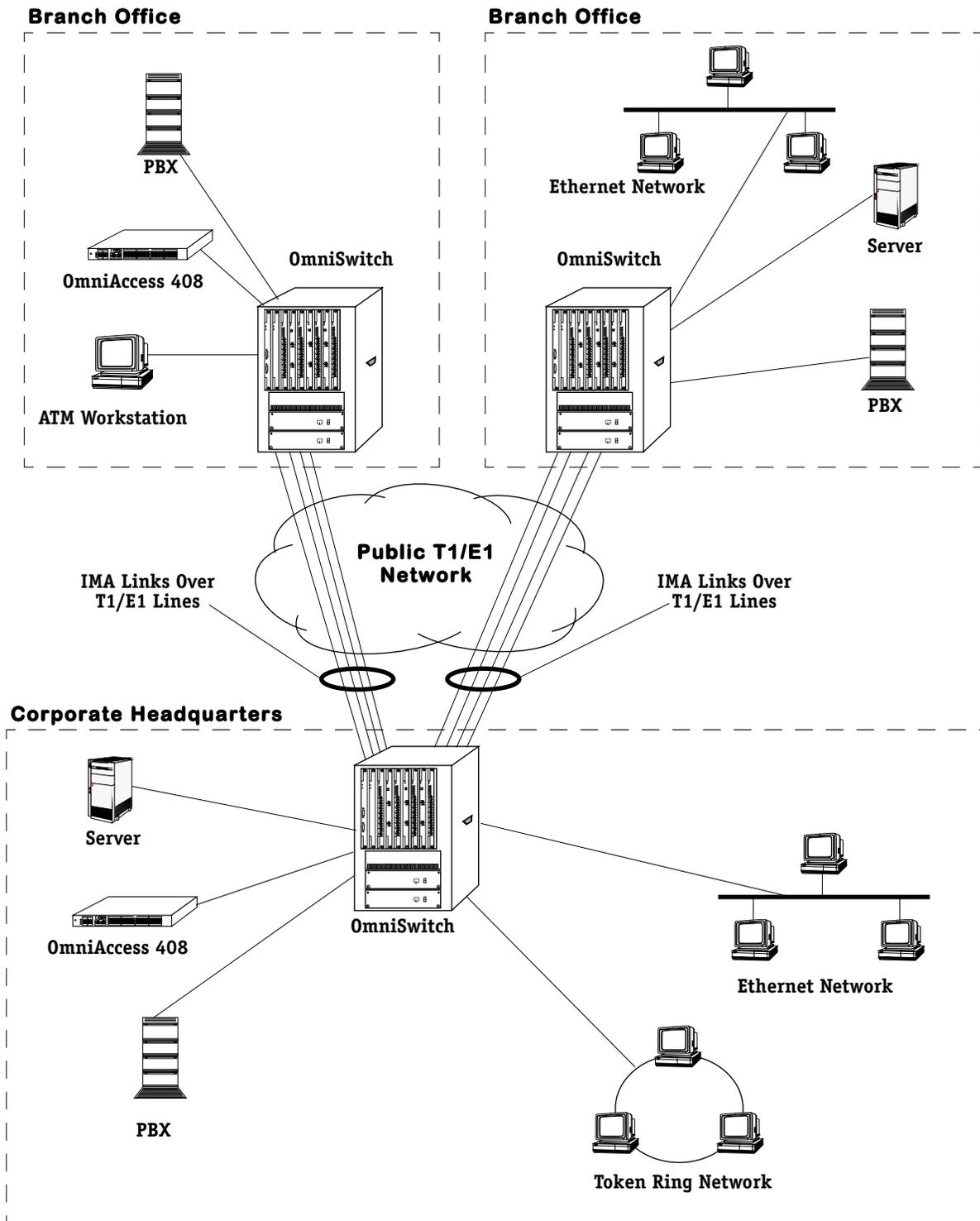
In the corporate headquarters, the OmniSwitch has an MPM 1G; a Frame to Cell Switching Module (FCSM), a CSM-U with a CSM-AB-IMA-DS1/E1-8W adapter board, a CSM-AB-CE-T1/E1 adapter board, and a CSM-AB-155F OC-3 adapter board; a TSM-CD-16W token ring switching module; and an ESM-C-32W Ethernet switching module. This OmniSwitch configuration is known as a hybrid LAN/ATM switch. (See Chapter 40, “Cell Switching Modules (CSMs),” for more information on hybrid LAN/ATM switches.)

The OC-3 CSM-AB-155F adapter board links the OmniSwitch in the corporate headquarters to the server and the OmniAccess 408 with its OC-3 uplink module. The CSM-AB-CE-T1/E1 adapter board connects the OmniSwitch to the PBX. And the CSM-AB-IMA-DS1/E1-8W adapter board links the devices in the corporate headquarters to devices in the two branch offices.

The OmniSwitches in the two branch offices are also configured as hybrid LAN/ATM switches with FCSMs and CSM-U's with CSM-AB-IMA-DS1/E1-8W adapter boards. With IMA, the networks in all three locations gain the advantages of ATM's QoS and its ability to send voice, video, and data while using low-cost T1 or E1 lines.

◆ **Note** ◆

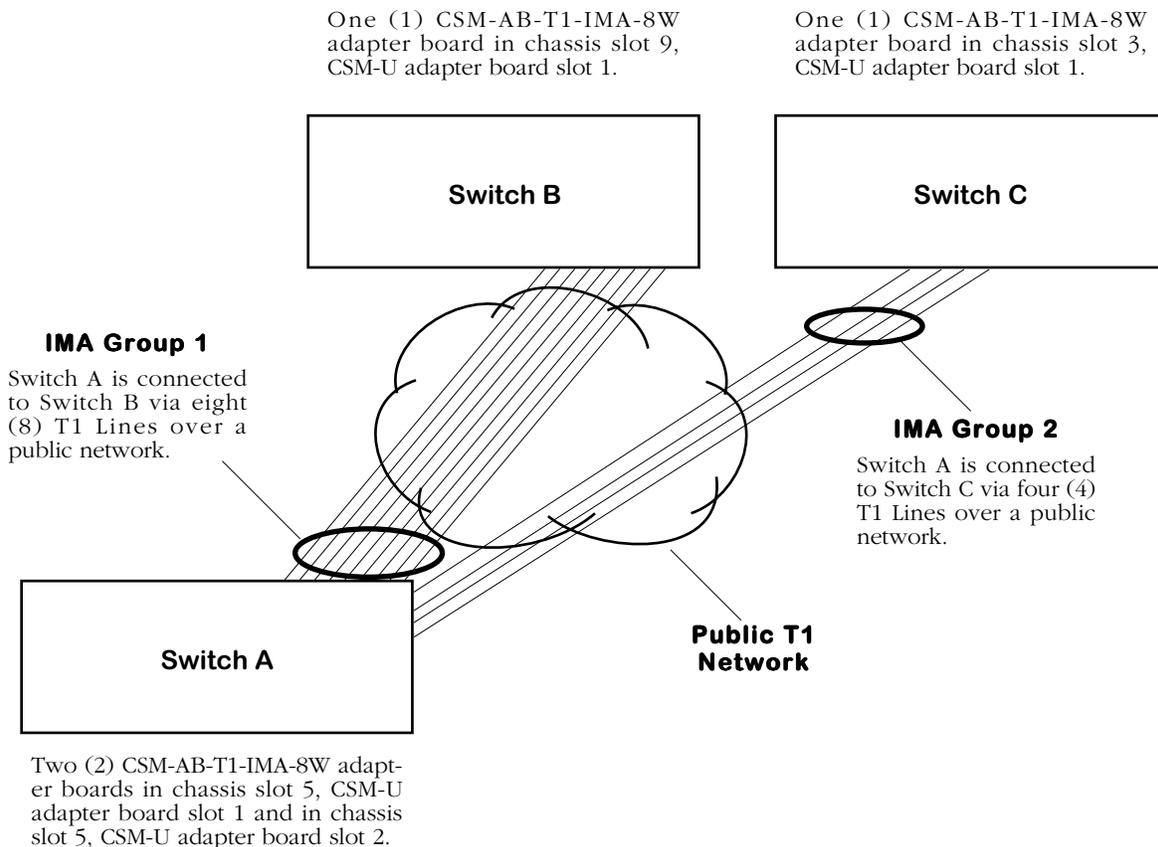
See *IMA Application Example* on page 43-8 on how to configure a similar network.



Example IMA Network

IMA Application Example

The illustration below shows a sample IMA configuration. Switch A is connected to Switch B with eight (8) T1 lines over a public network. IMA Group 1 was created to produce a virtual link transmitting ATM cells at approximately 12.35 Mbps. In addition, Switch A is connected to Switch C with four (4) T1 lines over a public network. IMA Group 2 was created to produce a virtual link transmitting ATM cells at approximately 6 Mbps.



IMA Application Example Network Diagram

In addition, there is a requirement for data to be transmitted as extended superframes (ESFs), and the ports need to be set for loop timing.

How to Set Up this Network

You can configure the application example on the previous page through the following steps. You create the logical IMA groups, assign ports to the IMA groups, and optionally set any T1 or E1 parameters.

Step 1. Configure the IMA Groups

1. On Switch A, perform the following steps to create IMA Group 1 and Group 2 with the **igpa** command, which is described in greater detail in *Creating IMA Groups* on page 43-15.
 - a. Enter **igpa 1** at the system prompt to create IMA Group 1.
 - b. Enter **save** at the **igpa** command prompt to accept the defaults.
 - c. Enter **igpa 2** at the system prompt to create IMA Group 2.
 - d. Enter **save** at the **igpa** command prompt to accept the defaults.
2. On Switch B, perform the following steps to create IMA Group 1.
 - a. Enter **igpa 1** at the system prompt to create IMA Group 1.
 - b. Enter **save** at the **igpa** command prompt to accept the defaults.
3. On Switch C, perform the following steps to create IMA Group 2.
 - a. Enter **igpa 2** at the system prompt to create IMA Group 2.
 - b. Enter **save** at the **igpa** command prompt to accept the defaults.

Step 2. Assign Links to the IMA Groups

1. On Switch A, perform the following steps to assign links to IMA Group 1 and Group 2 with the **igpmem** command, which is described in greater detail in *Adding and Modifying IMA Group Membership* on page 43-18.
 - a. At the system prompt, enter **igpmem 1** to add physical links to IMA Group 1.
 - b. Enter **2=1** at the **igpmem** command prompt to configure the CSM-AB-IMA-DS1-8W adapter board in CSM-U slot 1, which has ports (links) 1 through 8.
 - c. Enter **3=+all** at the **igpmem** command prompt to add ports (links) 1 through 8 to IMA Group 1.
 - d. Enter **save** at the **igpmem** command prompt to save your settings.
 - e. At the system prompt, enter **igpmem 2** to add physical links to IMA Group 2.
 - f. Enter **2=2** at the **igpmem** command prompt to configure the CSM-AB-IMA-DS1-8W adapter board in CSM-U slot 2, which has ports (links) 9 through 16.
 - g. Enter **3=+9+10+11+12** at the **igpmem** command prompt to add ports (links) 9 through 12 to IMA Group 2.
 - h. Enter **save** at the **igpmem** command prompt to save your settings.

2. On Switch B, perform the following steps to assign links to IMA Group 1.
 - a. Enter **igpmem 1** at the system prompt to add physical links to IMA Group 1.
 - b. Enter **2=1** at the **igpmem** command prompt to configure the CSM-AB-IMA-DS1-8W adapter board in CSM-U slot 1, which has ports (links) 1 through 8.
 - c. Enter **3=+all** at the **igpmem** command prompt to add ports (links) 1 through 8 to IMA Group 1.
 - d. Enter **save** at the **igpmem** command prompt to save your settings.
3. On Switch C, perform the following steps to assign links to IMA Group 2.
 - a. Enter **igpmem 2** to add physical links to IMA Group 2.
 - b. Enter **2=1** at the **igpmem** command prompt to configure the CSM-AB-IMA-DS1-8W adapter board in CSM-U slot 1, which has ports (links) 1 through 8.
 - c. Enter **3=+1+2+3+4** at the prompt to add ports (links) 1 through 4 to IMA Group 2.
 - d. Enter **save** at the prompt to save your settings.

Step 3. Configure Global T1 Parameters

1. You modify global parameters of IMA groups with the **igpm** command, which is described in greater detail in *Modifying IMA Groups* on page 43-21. On either Switch A or Switch B, perform the following steps to globally set Extended Superframe (ESF) and loop timing to all the ports in IMA Group 1. It does not matter which switch you configure since only symmetrical configurations are supported.
 - a. At the system prompt, enter **igpm 1** to configure IMA Group 1.
 - b. Enter **100=2** at the **igpm** command prompt to set all the links in IMA Group 1 to Extended Superframe (ESF).
 - c. Enter **102=1** at the **igpm** command prompt to set all the links in IMA Group 1 to loop timing.
 - d. Enter **save** at the **igpm** command prompt to save your settings.
2. On Switch A or Switch C, perform the following steps to globally set Extended Superframe (ESF) and loop timing to all the ports in IMA Group 2. It does not matter which switch you configure since only symmetrical configurations are supported.
 - a. At the system prompt, enter **igpm 2** to configure IMA Group 2.
 - b. Enter **100=2** at the **igpm** command prompt to set all the links in IMA Group 2 to Extended Superframe (ESF).
 - c. Enter **102=1** to set all the links in IMA Group 2 to loop timing.
 - d. Enter **save** at the **igpm** command prompt to save your settings.

IMA Theory of Operation

The following sections describe two important concepts, the IMA Link State Machine (LSM) and the IMA synchronization process, used to maintain IMA links. The IMA LSM is described below and the IMA synchronization process is described in *IMA Synchronization Process* on page 43-12.

IMA Link State Machine (LSM)

The IMA Link State Machine (LSM) is the transmit and receive direction of each IMA link. The LSM can be in one of the following four states:

Not In Group. The link is currently not configured to any IMA group.

Unusable. The link is configured, but is not in the usable state due to a fault, inhibition, etc.

Usable. The link is ready to operate (e.g., free of alarms and faults, etc.), but is waiting for the other end to be usable or active.

Active. The link is transmitting ATM layer cells and is part of the data round robin from or to the ATM layer.

The usable state is an “extra” state between the unusable and active state that allows coordination of the near-end and far-end sides when bringing up the link. The usable state also provides a clear synchronization point before activating links that are ready to be set to the active state.

The IMA LSM begins in the not-in-group state and remains there until the link is configured by the unit management entity. Once configured, the LSM moves to the unusable state. From the unusable state, the LSM moves between the unusable, usable, and active states.

The unusable state provides a synchronization point for application-dependent or group-level control of link usability. Link error conditions (either physical errors or IMA errors) and application-dependent conditions can delay the transition of the LSM into the usable state or can bring the IMA LSM back to the unusable state from the usable or active states. The unusable state also allows the IMA to voluntarily delay restoration of the link for reasons other than detected problems; this is referred to as inhibition of the link.

IMA Synchronization Process

Before ATM cells can be transmitted, the IMA implementation uses a cell delineation mechanism to synchronize the near end and the far end of the link. This mechanism proceeds as follows:

1. A cell-by-cell IMA HUNT state is entered at startup.
2. The frame-by-frame IMA PRESYNC state is entered when one (1) valid IMA Control Protocol (ICP) cell is received.
3. The frame-by-frame IMA SYNC state is entered when a user-defined number of ICP cells, which is known as the Gamma (γ) value, has been received.

The IMA implementation can leave the IMA SYNC state and return to the IMA HUNT state for the following reasons:

- If the IMA implementation detects a user-defined number of invalid ICP cells, which is known as the Alpha (α) value.
- If the IMA implementation detects a user-defined number of errored ICP cells, which is known as the Beta (β) value.

The IMA Submenu

The IMA submenu is part of the Physical Interface menu, as shown below.

Command	Physical Interface Menu
slipc	Configure SLIP (Serial Line IP) on a TTY Port
atm	Enter the ATM Management sub-menu
eth100	Enter the 100BaseT sub-menu
10/100	Enter the 10/100BaseT sub-menu
te	Enter T1/E1 Port Management sub-menu
ima	Enter IMA Port Management sub-menu

The IMA submenu contains User Interface (UI) commands to display and configure IMA ports and links. To enter the IMA submenu, enter

ima

at any system prompt. Enter a question mark (?) to display the commands in the IMA submenu, as shown below.

Command	IMA Management Menu
igpa	Add an IMA group
igpd	Delete an IMA group
igpm	Modify an IMA group
igps	View status of IMA groups
igpsts	View statistics of an IMA group
igpcls	Clear statistics of an IMA group
igplts	Display 24-hour period statistics of a local group
igpcls	Display current 15-minute statistics of a local group
igplis	Display 15-minute interval statistics of a local group
igpmem	Configure IMA group membership
igrprt	Restart an IMA group
igptestb	Initiate a test procedure on an IMA group
igpteste	Terminate a test procedure on an IMA group
ilkm	Configure link parameters
ilks	View status of IMA links
ilksts	View statistics of an IMA link
ilkcls	Clear statistics of a link
ilkltts	Display 24-hour period statistics of a local port
ilkcls	Display current 15-minute statistics of a local port
ilkltis	Display 15-minute interval statistics of a local port
iupgfpga	Upgrade FPGA of an IMA module

◆ Note ◆

The **ima** submenu will not display and the **ima** commands will not be available unless your IMA hardware is properly installed and the IMA software (**ima.img**) has loaded properly.

The commands in the IMA submenu are described in the sections that follow.

User Interface Command Syntax

Some commands in the User Interface (UI) have parameters that must be entered for the command to function properly. This chapter lists these parameters by surrounding them with a “less-than” sign (<) and a “greater-than” (>) sign. A vertical line (|) between two parameters indicates that only one of the parameters can be used, but not both of them.

For example, the syntax for the **igpm** command is as follows:

igpm <IMA group id> | <CSM slot/port>

You *must* enter **<IMA group ID>** or **<CSM slot/port>**, but not both.

For example, if you want to modify IMA Group 5, which is assigned to CSM slot/port 5/1, you can enter **igpm 5** or **igpm 5/1**.

Some commands in the IMA submenu have optional parameters. These parameters are indicated by square brackets (e.g., [**<slot>/<port>**]). For example, the syntax for the **igps** command is as follows:

igps [<IMA group id> | <CSM slot/port>] [all]

You can enter **<IMA group ID>** or **<CSM slot/port>**, but not both. In addition, you can enter the **all** option whether or not you entered the other option.

Creating IMA Groups

You create new IMA groups with the **igpa** command. The syntax for this command is as follows:

```
igpa [<IMA group id>]
```

If you do not enter the <IMA group id> option, it will create an IMA group with the next available number. For example, if there is an existing IMA Group 0, the **igpa** command will create IMA Group 1. The group number must be between 0 and 255.

◆ Note ◆

IMA group IDs only have local significance and you could enter any valid ID number. However, you should use the same ID numbers on both sides of the links to aid tracking and debugging.

To create an IMA group with the next available group number, enter

```
igpa
```

at the system prompt. A screen similar to the following will be displayed.

Add new IMA Group 0

1)	Description {30 Characters}	: IMA Group 0
2)	Admin Status { up(1), down(2) }	: up
3)	IMA Version { 1.0(1), 1.1(2) }	: 1.1
4)	Minimum Transmit Links { 1..8 }	: 1
5)	Minimum Receive Links { 1..8 }	: 1
6)	Maximum Differential Delay in milliseconds { 1 . . 50 }	: 25
7)	Invalid ICP before HUNT { 1..2 }	: 2
8)	Consecutive Errored ICP before HUNT { 1..5 }	: 2
9)	Consecutive Valid ICP before SYNC state { 1..5 }	: 1
10)	Unique Physical Parameters { Yes(1), No(2) }	: Yes

```
Enter (option=value/save/cancel) :
```

The **igpa** command also sets all the group's parameters for you. If you want to change any of these parameters, enter the line number of the parameter, followed by an equal sign, and then the new value. For example, to change the minimum number of receive links from 1 to 2, enter:

```
5=2
```

To create the new IMA group, enter **save**. If you do not want to save the changes enter **quit** or **cancel**, or press **Ctrl-D**. If you entered **save**, the following message should be displayed.

```
Group configured successfully.
```

◆ Important Note ◆

The **igpa** command creates a logical IMA group but does *not* assign it to any physical connections. You must execute the **igpmem** command (described in *Adding and Modifying IMA Group Membership* on page 43-18) to assign physical ports to the IMA group.

The configurable fields (parameters) displayed by the **igpa** command are described below.

1) Description {30 Characters}

Enter a unique description of the group, using up to 30 ASCII characters. The default is **IMA Group** followed by the group number.

2) Admin Status { up(1), down(2) }

Enter **1** to enable the group (the default) or **2** to disable it. (If you disable this group then it will be unable to transmit or receive ATM cells.)

3) IMA Version{ 1.0(1), 1.1(2) }

Enter **1** to use IMA version 1.0 or **2** (the default) to use IMA version 1.1.

◆ Note ◆

In order to interoperate with devices running IMA version 1.0, you *must* configure the port for IMA version 1.0 instead of the default of IMA version 1.1.

4) Minimum Transmit Links { 1..8 }

Enter a number from **1** (the default) to **8** to set the minimum number of active transmit links required for the IMA group to be in an Up (i.e., operational) state. You can use this field to specify the minimum required bandwidth for the IMA link. A lower number will help ensure connectivity if a link goes down. In addition, changing this field will update **Minimum Receive Links** field since only symmetric mode is currently supported.

5) Minimum Receive Links { 1..8 }

Enter a number from **1** (the default) to **8** to set the minimum number of active receive links required for the IMA group to be in an Up (i.e., operational) state. You can use this field to specify the minimum required bandwidth for the IMA link. A lower number will help ensure connectivity if a link goes down. In addition, changing this field will update **Minimum Transmit Links** field since only symmetric mode is currently supported.

◆ Important Note ◆

Fields 6 (**Maximum Differential Delay**) through 9 (**Consecutive Valid ICP before SYNC state**) are set by default to ATM Forum IMA standards. Modifying these fields can cause interoperability problems. These fields should only be modified by experienced ATM network administrators.

6) Maximum Differential Delay { 1 . . 50 }

The maximum (in milliseconds) differential delay among the links that will be tolerated on this interface. An IMA link will be removed from service if it exceeds this limit.

Enter a value from 1 to 50 milliseconds. The default is **25** milliseconds.

7) Invalid ICP before HUNT { 1..2 }

The number of invalid IMA Control Protocol (ICP) cells allowed before moving from a synchronized mode to an ICP hunt mode. This parameter is also known as the Alpha (α) value used in the IMA synchronization process, which is described in *IMA Synchronization Process* on page 43-12.

Enter either **1** or **2**. The default value is **2**.

8) Consecutive Errored ICP before HUNT { 1..5 }

The number of consecutive invalid IMA Control Protocol (ICP) cells allowed before moving from a synchronized mode to an ICP hunt mode. This parameter is also known as the Beta (β) value used in the IMA synchronization process, which is described in *IMA Synchronization Process* on page 43-12.

Enter a value from 1 to 5. The default value is **2**.

9) Consecutive Valid ICP before SYNC state { 1..5 }

The number of consecutive valid IMA Control Protocol (ICP) cells detected before moving from a pre-synchronized state to a synchronized state. This parameter is also known as the Gamma (γ) value used in the IMA synchronization process, which is described in *IMA Synchronization Process* on page 43-12.

Enter a value from 1 to 5. The default value is **5**.

10) Unique Physical Parameters { Yes(1), No(2) }

This parameter determines if the configurations of all T1/E1 ports that belong to this group should be identical or not. If you enter **1** (Yes), which is the default, then T1/E1 physical parameters will only be configurable by the **igpm** command, not the **temod** command. In addition, changing any physical port parameters with the **igpm** command will change all physical port parameters for all ports that belong to this group. See *Modifying IMA Groups* on page 43-21 for more information on the **igpm** command.

Adding and Modifying IMA Group Membership

To add or modify IMA group membership, use the **igpmem** command. This command links the logical IMA group created with the **igpa** command (see *Creating IMA Groups* on page 43-15) to physical connections. To modify existing group membership, see *Modifying IMA Group Membership* on page 43-20. To add group membership on new IMA groups, see the subsection below.

Adding IMA Group Membership

The syntax for this command is as follows:

```
igpmem <IMA group id> | <CSM slot/port>
```

Enter **igpmem** followed by the IMA group number. For example, to configure group membership for IMA Group 0, enter

```
igpmem 0
```

at the system prompt. A screen similar to the following will be displayed:

```
          Add Memberships to Group 0

Available Links: 1, 2, 3, 4, 5, 6, 7, 8

1) Physical Slot { 1..5 }           : 5
2) Physical Module { 1..3 }        : 1
3) Physical Port                   : None
   (Usage: '+/-<port|all>' add/remove a link port.
   Example: '3=+2+4-3' to add link port 2 & 4 and
   remove link port 3.
   '3=+all' add all available link ports.
   '3=-all' remove all link ports assigned.)
4) CSM Port { 2,3,4 }              : 1
```

```
Enter (option=value/save/cancel) :
```

◆ Note ◆

The **igpmem** command will display the first slot and module that still has available links and CSM ports.

Select the number of the item you want to change. To change any of the values listed above except for the **Physical Port** field, enter the line number, followed by an equal sign, and then the new value. For example, to configure a CSM-AB-IMA-DS1/E1-8W submodule installed in the middle of a CSM-U, enter:

```
2=2
```

To change the values for **Physical Port** field, see *3) Physical Port* on page 43-19.

To update the values you have changed, enter **save**. If you do not want to save the changes, enter **quit** or **cancel**, or press **Ctrl-D**.

The fields displayed by the **igpmem** command are described below. Configurable fields are preceded by a number.

Available Links

This field displays the physical ports that are available. For example, you can have up to eight (8) links on a CSM-AB-IMA-DS1/E1-8W submodule.

1) Physical Slot

Enter the slot number of the module you want to configure. (The last number displayed in the brackets will match the number of slots in your chassis.)

2) Physical Module

Enter the number of the CSM-U or CSM-U+ submodule you want to configure. CSM-U and CSM-U+ submodules are numbered (1-3) from left to right on an Omni-3wx or Omni-5wx and from top to bottom on an Omni-9wx.

3) Physical Port

Enter the physical port number on the module that you want to add or delete. If you want to add a port to the IMA group, enter **3=+** followed by the port number. For example, if you want to add Port 2, enter

3=+2

at the prompt. If you want to delete a port from the IMA group, enter **3=-** followed by the port number. For example, if you want to delete Port 2, enter

3=-2

at the prompt. In addition, you can add and delete ports at the same prompt. For example, to add Ports 1, 3, and 8 and delete Ports 2 and 4, enter

3=+1-2+3-4+8

at the prompt. To add or delete all the ports from the IMA group use the **all** option. To add all available ports, enter

3=+all

at the prompt. To delete all the ports, enter

3=-all

at the prompt.

4) CSM Port

You can enter an optional Cell Switching Module (CSM) port number for the IMA group. For example, if you set this field to **2** and the physical slot of the CSM is **5**, then the CSM port number will be **5/2**. The CSM port number along with the CSM slot number can be used in place of the IMA group ID in the **igpm**, **igps**, **igpsts**, **igpcls**, **igplts**, **igplcs**, **igplis**, **igprst**, **igpd**, **igptestb**, **igpteste**, **ilk**, **ilks**, **ilksts**, **ilkcls**, **ilkcls**, **ilkcls**, and **ilkcls** commands.

In addition, after you have assigned a CSM port number, you can use the CSM slot and port numbers instead of the IMA group number in this (**igpmem**) command. See *Cell Switching Module (CSM) Ports and IMA Groups (CSM-AB-IMA-DS1/E1-8W Submodule)* on page 43-5 for more information on CSM ports.

Modifying IMA Group Membership

The syntax for this command is as follows:

```
igpmem <IMA group id> | <CSM slot/port>
```

◆ **Note** ◆

You *cannot* use the **<CSM slot/port>** parameter until you have assigned a CSM port number to the IMA group with the **igpmem** command. See *Adding IMA Group Membership* on page 43-18 for more information on assigning CSM ports.

Enter **igpmem** followed by the IMA group number CSM slot/port number. For example, to configure group membership for the IMA group assigned to CSM slot/port 5/2, enter

```
igpmem 5/2
```

at the system prompt. A screen similar to the following will be displayed:

Add Memberships to Group 0

Available Links:

- | | |
|---|-------------------|
| 1) Physical Slot { 1..5 } | : 5 |
| 2) Physical Module { 1..3 } | : 1 |
| 3) Physical Port | : 1,2,3,4,5,6,7,8 |
| (Usage: '+/-<port all>' add/remove a link port.
Example: '3=+2+4-3' to add link port 2 & 4 and
remove link port 3.
'3=+all' add all available link ports.
'3=-all' remove all link ports assigned.) | |
| 4) CSM Port { 1,3,4 } | : 2 |

Enter (option=value/save/cancel) :

Select the number of the item you want to change. To change any of the values listed above except for the **Physical Port** field, enter the line number, followed by an equal sign, and then the new value. For example, to configure a CSM-AB-IMA-DS1/E1-8W submodule installed in the middle of a CSM-U, enter:

```
2=2
```

To change the values for **Physical Port** field, see *3) Physical Port* on page 43-19.

To update the values you have changed, enter **save**. If you do not want to save the changes enter **quit** or **cancel**, or press **Ctrl-D**.

The fields displayed by the **igpmem** command are described in *Adding IMA Group Membership* on page 43-18. Configurable fields are preceded by a number.

Modifying IMA Groups

To modify an IMA group, use the **igpm** command. The configurable parameters vary depending on whether you have T1 or E1 ports. If you have E1 ports, see *Modifying IMA Groups with E1 Ports* on page 43-25. If you have T1 ports and you are using long-haul line, see *Modifying IMA Groups with T1 Ports (Long-Haul Line)* on page 43-24. And if you have T1 ports and you are using short-haul line, see the subsection below.

Modifying IMA Groups with T1 Ports (Short-Haul Line)

The syntax for this command is as follows:

```
igpm <IMA group id> | <CSM slot/port>
```

Enter **igpm** followed by the IMA group number or the CSM slot/port number you assigned with the **igpmem** command (see *Adding and Modifying IMA Group Membership* on page 43-18). To modify IMA Group 0, for example, enter

```
igpm 0
```

at the system prompt. A screen similar to that shown below will be displayed:

```

      Modify IMA Group 0

1)  Description {30 Characters}                : IMA Group 0
2)  Admin Status { up(1), down(2) }           : up
3)  IMA Version { 1.0(1), 1.1(2) }            : 1.1
4)  Minimum Transmit Links { 1..8 }           : 1
5)  Minimum Receive Links { 1..8 }            : 1
6)  Maximum Differential Delay in milliseconds { 1 . . 25 } : 25
7)  Invalid ICP before HUNT { 1..2 }          : 2
8)  Consecutive Errored ICP before HUNT { 1..5 } : 2
9)  Consecutive Valid ICP before SYNC state { 1..5 } : 1
10) Unique Physical Parameters { Yes(1), No(2) } : Yes
    100) Framing Format { ESF(2), SF(3) }       : ESF
    101) Line Build Out { short(1), long(2) }   : short
        110) Line Length in meters { 0..200 }   : 30
    102) Transmit Clock Source
        { loopTiming(1), localTiming(2) }      : localTiming
103) Group Loopback
        { none(1), payload(2), line(3), inward(5) } : none

```

```
Enter (option=value/save/cancel) :
```

Select the number of the item you want to change. To change any of the values listed above, enter the line number, followed by an equal sign, and then the new value. For example, to change the minimum number of receive links from 1 to 2, enter:

```
4=2
```

To update the values you have changed, enter **save**. If you do not want to save the changes enter **quit** or **cancel**, or press **Ctrl-D**. If you entered **save**, the following message should be displayed.

```
Group configured successfully.
```

◆ Note ◆

Option 10 (**Unique Physical Parameters**) and its suboptions will not be displayed until at least one link has been created.

See *Creating IMA Groups* on page 43-15 for fields 1 (**Description**) through 9 (**Consecutive Valid ICP before SYNC state**). The remaining configurable fields displayed by the **igpm** command are described below.

10) Unique Physical Parameters { Yes(1), No(2) }

This parameter determines if the configurations of all T1/E1 ports that belong to this group should be identical or not. If you enter **1** (Yes), which is the default, then T1/E1 physical parameters will only be configurable by the this command, not the **temod** command. In addition, changing any physical port parameters with the this command will change all physical port parameters for all ports that belong to this group.

100) Framing Format { ESF(2), SF(3) }

A T1 frame consists of twenty-four (24) 8-bit time slots and a 1-bit synchronization and control bit. Twelve (12) T1 frames can be grouped into a SuperFrame (SF), and twenty-four (24) T1 frames can be grouped into an Extended SuperFrame (ESF).

Only option **2** (ESF) is supported since only the ESF format is compliant with the ATM Forum *DS1 Physical Layer Specification* (af-phy-0016.00). In addition, to support FDL and remote loopback activation/deactivation on the ATM UNI you must use the ESF format.

◆ Note ◆

Changing the framing format here will also change the framing format on all links assigned to this group

101) Line Build Out { short(1), long(2) }

Long haul support is necessary if this T1 port is directly connected to a Central Office (CO) and the cable length is greater than 200 meters. If this T1 port connects locally (i.e., it is not connected to an external CSV) using less than 200 meters of cable, short haul is adequate.

Enter **1** for a cable length of 200 or less meters or **2** for a cable length greater than 200 meters. (Changing the line length here will also change the framing format on all links assigned to this group.) If you entered **1** (short), the following sub-option will be displayed:

110) Line Length in meters { 0..200 }

Enter the cable length in meters. This value must be less than or equal to 200 meters.

102) Transmit Clock Source { loopTiming(1), localTiming(2) }

The source of the transmit clock. Loop timing means the receive clock (recovered from receive data) is used as the transmit clock. Local timing indicates the local clock source (generated from PLLs) is used as the transmit clock. For more information, see Chapter 45, "Clocking ATM Networks."

Enter **1** for loop timing or **2** for local timing (the default). (Changing the transmit clock source here will also change the framing format on all links assigned to this group.)

◆ Note ◆

You *cannot* have different clock settings on the same CSM-AB-IMA-DS1/E1-8W submodule.

103) Group Loopback { none(1), payload(2), line(3), inward(5) }

The loopback configuration for this port. Loopback configurations are used to test the framing functionality within the T1 port. Framing functionality assembles T1 frames into SuperFrames and Extended SuperFrames, depending on how the port is configured. Possible values are as follows:

◆ Note ◆

Loopback states should be used for debugging purposes only.

none. The port is not in a loopback state. This is the typical live network state for a T1 port.

payload. The received signal for this IMA group is looped out of the port after passing through the port's framing functionality.

line. The received signal at this T1 port does not go through the port's framing functionality, and is looped straight back out the port.

inward. The transmitted signal from the inward side of this port is looped back internally. The signal passes through the T1 framing functionality before looping back.

Enter **1** for no group loopback, **2** for payload, **3** for line, or **5** for inward group loopback (the default).

Modifying IMA Groups with T1 Ports (Long-Haul Line)

The syntax for this command is as follows:

```
igpm <IMA group id> | <CSM slot/port>
```

Enter **igpm** followed by the IMA group number or the CSM slot/port number you assigned with the **igpmem** command (see *Adding and Modifying IMA Group Membership* on page 43-18). To modify IMA Group 0, for example, enter

```
igpm 0
```

at the system prompt. A screen similar to that shown below will be displayed:

```

Modify IMA Group 0

1) Description {30 Characters}           : IMA Group 0
2) Admin Status { up(1), down(2) }      : up
3) IMA Version { 1.0(1), 1.1(2) }       : 1.1
4) Minimum Transmit Links { 1..8 }      : 1
5) Minimum Receive Links { 1..8 }       : 1
6) Maximum Differential Delay in milliseconds { 1 . . 25 } : 25
7) Invalid ICP before HUNT { 1..2 }     : 2
8) Consecutive Errored ICP before HUNT { 1..5 } : 2
9) Consecutive Valid ICP before SYNC state { 1..5 } : 1
10) Unique Physical Parameters { Yes(1), No(2) } : Yes
    100) Framing Format { ESF(2), SF(3) } : ESF
    101) Line Build Out { short(1), long(2) } : long
        110) Attenuation
            { 0 dB(1), -7.5dB(2), -15.0dB(3), -22.5dB(4) } : 0 dB
    102) Transmit Clock Source
            { loopTiming(1), localTiming(2) } : localTiming
    103) Group Loopback
            { none(1), payload(2), line(3), inward(5) } : none

```

```
Enter (option=value/save/cancel) :
```

Select the number of the item you want to change. To change any of the values listed above, enter the line number, followed by an equal sign, and then the new value. For example, to change the minimum number of receive links from 1 to 2, enter:

```
4=2
```

To update the values you have changed, enter **save**. If you do not want to save the changes enter **quit** or **cancel**, or press **Ctrl-D**. If you entered **save**, the following message should be displayed.

```
Group configured successfully.
```

◆ Note ◆

Option 10 (**Unique Physical Parameters**) and its suboptions will not be displayed until at least one link has been created.

See *Creating IMA Groups* on page 43-15 for fields 1 (**Description**) through 9 (**Consecutive Valid ICP before SYNC state**) and see *Modifying IMA Groups with T1 Ports (Short-Haul Line)* on page 43-21 for all other fields except for **110) Attenuation**, which is described below. The remaining configurable field displayed by the **igpm** command is described below.

```
110)Attenuation { 0dB(1), -7.5dB(2), -15.0dB(3), -22.5dB(4) }
```

Enter **1** for 0 decibels (dB), **2** for -7.5 dB, **3** for - 15.0 dB, or **4** for -22.5 dB.

Modifying IMA Groups with E1 Ports

The syntax for this command is as follows:

```
igpm <IMA group id> | <CSM slot/port>
```

Enter **igpm** followed by the IMA group number or the CSM slot/port number you assigned with the **igpmem** command (see *Adding and Modifying IMA Group Membership* on page 43-18). To modify IMA Group 0, for example, enter

```
igpm 0
```

at the system prompt. A screen similar to that shown below will be displayed:

```

Modify IMA Group 0

1) Description {30 Characters} : IMA Group 0
2) Admin Status { enabled(1), disabled(2) } : enabled
3) IMA Version { 1.0(1), 1.1(2) } : 1.1
4) Minimum Transmit Links { 1..8 } : 1
5) Minimum Receive Links { 1..8 } : 1
6) Maximum Differential Delay in milliseconds { 1 . . 25 } : 25
7) Invalid ICP before HUNT { 1..2 } : 2
8) Consecutive Errored ICP before HUNT { 1..5 } : 2
9) Consecutive Valid ICP before SYNC state { 1..5 } : 1
10) Unique Physical Parameters { Yes(1), No(2) } : Yes
    100) Framing Format { E1(4), E1-CRC(5) } : E1-CRC
    101) Line Build Out { short(1), long(2) } : short
        110) Cable Type { 75 Ohms(1), 120 Ohms(2) } : 75 Ohms
    102) Transmit Clock Source
        { loopTiming(1), localTiming(2) } : localTiming
    103) Group Loopback
        { none(1), payload(2), line(3), inward(5) } : n

```

```
Enter (option=value/save/cancel) :
```

Select the number of the item you want to change. To change any of the values listed above, enter the line number, followed by an equal sign, and then the new value. For example, to change the minimum number of receive links from 1 to 2, enter:

```
5=2
```

To update the values you have changed, enter **save**. If you do not want to save the changes enter **quit** or **cancel**, or press **Ctrl-D**. If you entered **save**, the following message should be displayed.

```
Group configured successfully.
```

◆ Note ◆

Option 10 (**Unique Physical Parameters**) and its suboptions will not be displayed until at least one link has been created.

See *Creating IMA Groups* on page 43-15 for fields 1 (**Description**) through 9 (**Consecutive Valid ICP before SYNC state**). The remaining configurable fields displayed by the **igpm** command are described below.

100) Framing Format { E1(4), E1-CRC(5) }

Enter **4** for E1 (standard E1 frame format using the framing bits in time slot 0 for framing) or **5** for E1-CRC (E1 frame using framing bits in both time slot 0 and CRC-4 multiframe for framing).

101) Line Build Out { short (1), long (2) }

Long haul support is necessary if this E1 port is directly connected to a Central Office (i.e., not connected via an external CSU) and the cable length is greater than 200 meters. If this E1 port connects locally using less than 200 meters of cable, then short haul is adequate.

Enter **1** for a cable length of 200 or less meters or **2** for a cable length greater than 200 meters.

110) Cable Type { 75 Ohm(1), 120 Ohm(2) }

Enter **1** to set the Line Interface Unit (LIU) to 75 Ohm or **2** to set it to 120 Ohm.

◆ Important Note ◆

The impedance value set here must match the impedance value set by hardware jumpers. See Chapter 40, "Cell Switching Modules (CSMs)," for more information on setting these impedance jumpers.

102) Transmit Clock Source { loopTiming(1), localTiming(2) }

The source of the transmit clock. Loop timing means the receive clock (recovered from receive data) is used as the transmit clock. Local timing indicates the local clock source (generated from PLLs) is used as the transmit clock. For more information, see Chapter 45, "Clocking ATM Networks."

Enter **1** for loop timing or **2** for local timing (the default).

◆ Note ◆

You *cannot* have different clock settings on the same CSM-AB-IMA-DS1/E1-8W submodule.

103) Group Loopback { none(1), payload(2), line(3), inward(5) }

The loopback configuration for this port. Loopback configurations are used to test the framing functionality of the E1 port. Framing functionality assembles E1 frames into multi-frames. Possible values are as follows:

◆ Note ◆

These loopback states should be used for debugging purposes only.

none. The port is not in a loopback state. This is the typical live network state for an E1 port.

payload. The received signal at this E1 port is looped out of the port after passing through the port's framing functionality.

line. The received signal at this E1 port does not go through the port's framing functionality, and is looped straight back out the port.

inward. The transmitted signal from the inward side of this port is looped back internally. The signal passes through the E1 framing functionality before looping back.

Enter **1** for no group loopback, **2** for payload, **3** for line, or **5** for inward group loopback (the default).

Configuring IMA Link Parameters

You configure IMA links (physicals ports in an IMA group) with the **ilkm** command. The syntax for this command is as follows:

```
ilkm <slot/port>
```

Enter **ilkm** followed by the slot and port numbers of the port you want to configure. For example, to configure the link parameters on Port 1 in Slot 5, enter

```
ilkm 5/1
```

at the system prompt. A screen similar to the following will be displayed:

```
Modify Link 5/1
```

```
1) Description { 30 characters } : IMA Link  
2) Administrative Status { up(1), down(2) } : up
```

```
Enter (option=value/save/cancel) :
```

Select the number of the item you want to change. To change any of the values listed above, enter the line number, followed by an equal sign, and then the new value. For example, to disable the IMA link (i.e., change the administrative state from **enabled** to **disabled**), enter:

```
2=2
```

To update the values you have changed, enter **save**. If you do not want to save the changes enter **quit** or **cancel**, or press **Ctrl-D**.

The fields displayed by the **ilkm** command are described below.

1) Description { 30 characters }

Enter a description up to 30 characters long. The default is **IMA Link**.

2) Administrative Status { up(1), down(2) }

Enter **1** to enable the link (the default) or **2** to disable the link.

◆ Note ◆

If you did not set the **Unique Physical Parameters** option to **Yes** with the **igpa** or **igpm** command, then you can use the **temod** command to modify individual physical links. See Chapter 53, “Managing T1 and E1 Ports,” for more information on the **temod** command.

Conducting an IMA Test

To verify the connectivity of a link within an IMA group, you can conduct an IMA test. A test pattern, which is a single byte with a value of 0 to 255, is sent from the near-end side of the IMA group in octet 17 of the IMA Control Protocol (ICP) cell and looped back over all the other links in the far-end of the IMA group.

◆ Note ◆

The **igptestb** command will not affect performance and will not disrupt user traffic since the test pattern is embedded within the ICP cell of an IMA frame.

You can initiate an IMA test procedure with the **igptestb** command, which is described in the subsection below. The test procedure will be active until you terminate it. To conclude the test procedure, use the **igpteste** command, which is described in *Ending an IMA Test* on page 43-31.

Starting an IMA Test

You initiate an IMA test with the **igptestb** command. The syntax for this command is as follows:

```
igptestb <IMA group id> | <CSM slot/port> [<slot>/<port>]
```

To initiate transmission the test pattern on the first link in the group to the far-end of the IMA link, enter **igptestb** followed by the IMA group number or the CSM slot/port number. (See *Adding and Modifying IMA Group Membership* on page 43-18 for more information on assigning a CSM port number to an IMA group.) The far-end of the link will then send the test pattern on all of its links in sequence back to the near-end side of the IMA link.

Next, the near-end of the IMA link will send the test pattern across the last link in the group. The far-end of the IMA link will again send the test pattern in sequence back on all of its links to the near-end of the IMA link.

This test will continue until you terminate it with the **igpteste** command, which is described in *Ending an IMA Test* on page 43-31. However, only the first two passes will be displayed. If you want to monitor a test procedure while it is running, use the **igps** command, which is described in *Displaying the Summary Status of IMA Groups* on page 43-35.

For example, to initiate the IMA test procedure on IMA Group 0 on its first link, enter

```
igptestb 0
```

at the system prompt. A screen similar to the following will be displayed.

```
Trying to transmit pattern #1 (2) on link 5/1... successful  
Verifying Rx pattern #1 on all links from remote  
Link 5/1 ... OK  
Link 5/2 ... OK  
Link 5/3 ... OK  
Link 5/4 ... OK  
Link 5/5 ... OK  
Link 5/6 ... OK  
Link 5/7 ... OK  
Link 5/8 ... OK  
Trying to transmit pattern #2 (253) on link 5/8... successful  
Verifying Rx pattern #2 on all links from remote  
Link 5/1 ... OK  
Link 5/2 ... OK  
Link 5/3 ... OK  
Link 5/4 ... OK  
Link 5/5 ... OK  
Link 5/6 ... OK  
Link 5/7 ... OK  
Link 5/8 ... OK
```

If you want to initiate the test procedure on a particular link, enter **igptestb**, followed by the IMA group number or the CSM slot/port number, and followed by the slot and port number of the selected link.

For example, to initiate the test procedure on Port 2 of Slot 5 in IMA Group 0, enter

```
igptestb 0 5/2
```

at the system prompt. A screen similar to the following will be displayed.

```
Trying to transmit pattern #1 (7) on link 5/2... successful  
Verifying Rx pattern #1 on all links from remote  
Link 5/1 ... OK  
Link 5/2 ... OK  
Link 5/3 ... OK  
Link 5/4 ... OK  
Link 5/5 ... OK  
Link 5/6 ... OK  
Link 5/7 ... OK  
Link 5/8 ... OK  
Trying to transmit pattern #2 (248) on link 5/8... successful  
Verifying Rx pattern #2 on all links from remote  
Link 5/1 ... OK  
Link 5/2 ... OK  
Link 5/3 ... OK  
Link 5/4 ... OK  
Link 5/5 ... OK  
Link 5/6 ... OK  
Link 5/7 ... OK  
Link 5/8 ... OK
```

The IMA test will continue to run until it is stopped by the **igpteste** command, which is described in *Ending an IMA Test* on page 43-31. After the initial messages are printed, you can use the **igps** command (which is described in *Displaying the Summary Status of IMA Groups* on page 43-35) or the **ilks** command (which is described in *Displaying the Summary Status of IMA Links* on page 43-44) to check the status of the IMA test.

Ending an IMA Test

You use the **igpteste** command to end an IMA test procedure. The syntax for this command is as follows:

```
igpteste <IMA group id> | <CSM slot/port>
```

To use this command, enter **igpteste** followed by the IMA group number (or the CSM slot/port number) of the test procedure that you activated with the **igptestb** command (see *Starting an IMA Test* on page 43-29). For example, to terminate the test on IMA Group 0, enter

```
igpteste 0
```

at the system prompt. If the test procedure terminated successfully, the following will be displayed.

```
Trying to disable test procedure on group 0 ... successful
```

Restarting an IMA Group

You use the **igprst** command to restart IMA groups. This command is equivalent to bringing an IMA group down and then bringing back up again. It is normally used when the near end of a group cannot sync up with the far end of the group. When you restart an IMA group, configuration settings and statistics are unaffected.

The syntax for this command is as follows:

```
igprst <IMA group id> | <CSM slot/port>
```

To use this command, enter **igprst** followed by the IMA group number or the CSM slot/port number. (See *Adding and Modifying IMA Group Membership* on page 43-18 for more information on assigning a CSM port number to an IMA group.) To restart IMA Group 0, for example, enter

```
igprst 0
```

at the system prompt. The following message will be displayed

```
Group 0 will be restarted
```

```
Do you want to continue (y/n)? (n) :
```

Enter **y** to restart the group or press **<Return>** to cancel (the default). If the group was successfully restarted, you should see the following message:

```
Group 0 successfully restarted
```

Deleting IMA Groups

Use the **igpd** command to delete IMA groups. The syntax for this command is as follows:

```
igpd <IMA group id> | <CSM slot/port>
```

To use this command, enter **igpd** followed by the IMA group number or the CSM slot/port number. (See *Adding and Modifying IMA Group Membership* on page 43-18 for more information on assigning a CSM port number to an IMA group.) For example, to delete IMA group 0, enter

```
igpd 0
```

at the system prompt. The following message will be displayed.

```
Group 0 will be deleted.
```

```
Do you want to continue? (y/n) ? (n) :
```

Enter **y** to delete the IMA group or press **<Return>** to cancel (the default). If you successfully deleted the group, the following will be displayed.

```
Group 0 successfully deleted
```

Upgrading Flash Memory on CSM-AB-IMA-DS1/E1-8W Submodules

You use the **iupgfpga** to upgrade the flash content of CSM-AB-IMA-DS1/E1-8W submodules with a Field Programmable Gate Array (FPGA) file. This command reads the contents of the FPGA file and compares it to the contents of the flash memory on the submodule. If a difference is found, then the **iupgfpga** command will replace the contents of the submodule's flash memory with the contents of the FPGA file.

◆ Important Note ◆

The **iupgfpga** command is used for hardware upgrades only. Do not use this command unless you have been directed by Alcatel to do so.

The syntax for this command is as follows:

```
iupgfpga <slot> <file_name> | <slot/module> <file_name> | all <file_name>
```

To upgrade all the CSM-AB-IMA-DS1/E1 submodules in a single CSM-U or CSM-U+, enter **iupgfpga** followed by the CSM-U or CSM-U+ slot number and the FPGA file name. To upgrade a specific CSM-AB-IMA-DS1/E1-8W submodule, enter **iupgfpga**, followed by the CSM-U or CSM-U+ slot number, followed by the CSM-AB-IMA-DS1/E1-8W submodule number, and followed by the FPGA file name. And to upgrade all CSM-AB-IMA-DS1/E1-8W submodules in a switch, enter **iupgfpga**, followed by **all**, and followed by the FPGA file name.

For example, to upgrade all the CSM-AB-IMA-DS1/E-8W submodules in a switch with the FPGA file **fpga319.bin**, enter

```
iupgfpga all fpga319.bin
```

at the system prompt. The following message will be displayed

```
Upgrading FPGA on all IMA modules in the switch with file fpga319.bin
```

```
Do you want to continue (y/n)? (n) :
```

Upgrading Flash Memory on CSM-AB-IMA-DS1/E1-8W Submodules

Enter **y** to upgrade all the CSM-AB-IMA-DS1/E1-8W submodules with the **fpga319.bin** FPGA file or press **<Return>** to cancel (the default). If you entered **y**, messages similar to the following will be displayed.

***** Attempting to upgrade FPGA on 5/1 *****

Device Am29F040 (512 Kbytes) is detected

Erasing flash successful

Programming flash successful

Upgrading FPGA completed successfully!

***** Attempting to upgrade FPGA on 5/2 *****

Device Am29F040 (512 Kbytes) is detected

Erasing flash successful

Programming flash successful

Upgrading FPGA completed successfully!

Displaying the Summary Status of IMA Groups

To view the summary status of IMA groups, use the **igps** command. The syntax for this command is as follows:

```
igps [<IMA group id> | <CSM slot/port>] [all]
```

The **<IMA group id>** or **<CSM slot/port>** option will give you a detailed list for a single IMA group (see *Displaying the Summary Status of a Single IMA Group* on page 43-38). The **<IMA group id>** or **<CSM slot/port>** option used together with the **all** option will give you a detailed list for a single IMA group with the status of all of the links on that group (see *Displaying the Detailed Status of a Single IMA Group with Link Status* on page 43-41). If you do not use either of these options, then you will see a brief list of all the IMA groups (see the subsection below).

(See *Adding and Modifying IMA Group Membership* on page 43-18 for more information on assigning a CSM port number to an IMA group.)

Displaying the Summary Status of All IMA Groups

To view the summary status of all IMA groups, enter

```
igps
```

at the system prompt. A screen similar to the following will be displayed.

IMA Group Status						
Grp	Near-end State	Far-end State	Failure Status	Num of Failures		
				Near-end	Far-end	
0	operational	operational	noFailure	0	0	
1	notConfigured	notConfigured	noFailure	0	0	
30	startUp	startUp	startUpNe	0	0	

The fields displayed by the **igps** for all IMA groups are described below.

Grp. The IMA group number.

Near-end State. The current operational state of the near-end side of the IMA group. The following are possible values.

operational. Indicates that group is the state where it can accept or pass cells from or to the ATM layer.

notConfigured. Indicates no links have been assigned to this group yet.

startUp. Indicates that group is in the first stage of negotiating with far-end side of the IMA group. It will not move out of this state until it receives acceptable parameters (such as IMA frame length, transmit clock configuration, symmetry, etc.) from the far-end side.

startUpAck. Indicates that group has received acceptable group parameters from far-end side of the IMA group.

cfgAbrtUnsuppM. Indicates that the IMA group has received a far-end negotiable IMA frame length parameter that is not supported by the near-end side of the IMA group, such as a mismatched configuration.

cfgAbrtUnsuppV. Indicates that the IMA group has received a far-end negotiable IMA version that is not supported by the near-end side of the IMA group, such as a mismatched configuration.

cfgAbrtIncompSym. Indicates that the IMA group has received a far-end negotiable IMA group symmetry parameter that is not supported by near-end side of the IMA group.

cfgAbrtOther. Indicates that group has received unsupported far-end group parameters besides unsupported IMA frame length and incompatible symmetry.

insuffLnks. Indicates that group has completed negotiation with the far-end side of the IMA group but the number of transmit and receive active links are less than the currently-configured **Minimum Transmit Links** and **Minimum Receive Links** fields (see *Displaying the Summary Status of a Single IMA Group* on page 43-38 to display these fields).

blocked. Indicates that the IMA group is administratively disabled (i.e., the group has been inhibited by the IMA group unit management entity). The group can be blocked for maintenance purposes or for insufficient links.

Far-end State. The current operational state of the far-end of the IMA group. See the **Near-end State** field description above for possible values.

Failure Status. The reason why an IMA group failed. If the IMA group is running, then **noFailure** is displayed. The following are possible values.

noFailure. Indicates that there is no failure on this group.

startUpNE. Indicates that near-end side of the group is in a start-up state.

startUpFE. Indicates that far-end side of the group is in a start-up state.

invalidMValNe. Indicates that the near-end side of the IMA group has received an invalid IMA frame length value.

invalidMValFe. Indicates that the far-end IMA group has received an invalid IMA frame length value.

invalidVValNe. Indicates that the near-end side of the IMA group has received an invalid value for IMA version.

invalidVValFe. Indicates that the far-end IMA group has received an invalid value for IMA version.

failedAsymNe. Indicates that the near-end side of the group has received an incompatible symmetry mode.

failedAsymFe. Indicates that the far-end group has received an incompatible symmetry mode.

insuffLnksNe. Indicates that the number of active transmit and receive links in the near-end side of the group is less than the values in the current configurable **Minimum Transmit Links** and **Minimum Receive Links** fields (see *Displaying the Summary Status of a Single IMA Group* on page 43-38 to display these fields).

insuffLnksFe. Indicates that the number of active transmit and receive links in the far-end side of the group is less than the values in the current configurable **Minimum Transmit Links** and **Minimum Receive Links** fields (see *Displaying the Summary Status of a Single IMA Group* on page 43-38 to display these fields).

blockedNe. Indicates that local state of the IMA group is in a blocked state (i.e., the group has been inhibited by the IMA group unit management entity). The group can be blocked for maintenance purposes or for insufficient links.

blockedFe. Indicates that far-end group state of the IMA group is in a blocked state (i.e., the group has been inhibited by the IMA group unit management entity). The group can be blocked for maintenance purposes or for insufficient links.

otherFailure. Indicates that local group is experiencing other unknown failures.

Near-end Num of failures. The number of near-end IMA group failures reported since power-up or reboot.

Far-end Num of Failures. The number of far-end IMA group failures reported since power-up or reboot.

Displaying the Summary Status of a Single IMA Group

To view the summary configuration and operational status of a single IMA group, enter **igps** followed by the IMA group number (or the CSM slot/port number). For example, to view the status of IMA Group 0, enter

```
igps 0
```

at the system prompt. A screen similar to the following will be displayed.

```

                IMA Group Status for Group 0
Description                : IMA Group 0
Admin Status                : up
Failure Status              : noFailure
Near-end State              : operational
Far-end State               : operational
Minimum Transmit Links     : 1           Minimum Receive Links : 1
Near-end Tx Clock Mode     : CTC         Far-end Tx Clock Mode  : CTC
Tx Frame Length            : 128        Rx Frame Length       : 128
Max Diff Delay (ms)       : 25         Max Diff Delay Obs (ms) : 0
Far-end IMA Group ID      : 20         Rx Timing Ref. Link   : 5/4
Invalid ICP before HUNT   : 2         Tx Timing Ref. Link   : 5/4
Cons Err ICP before HUNT  : 2
Cons Valid ICP before SYNC : 1
Status Change Time        : 0 days, 00:01:02.31
Group Memberships         : 5/4, 5/5, 5/8
CSM Port                  : 5/3
Least Delay Link           : 5/5
Most Delay Link            : 5/4
Test Pattern               : AnyPattern
Test Link                  : AnyLink
Test Pattern Procedure     : disabled
```

The fields displayed by the **igps** command for a single IMA group are described below.

Description. The configured description of the IMA group that was set by the **igpa** or **igpm** command.

Admin Status. The configured administrative status of the IMA group, which can be enabled (**up**) or disabled (**down**).

Failure Status. The current operational failure status of the IMA group (i.e., reason why an IMA group failed). See *Displaying the Summary Status of All IMA Groups* on page 43-35 for descriptions of possible values.

Near-end State. The current operational state of the near-end side of the IMA group. See *Displaying the Summary Status of All IMA Groups* on page 43-35 for descriptions of possible values.

Far-end State. The current operational state of the far-end of the IMA group. See *Displaying the Summary Status of All IMA Groups* on page 43-35 for descriptions of possible values.

Minimum Transmit Links. The configured minimum number of active transmit links required for the IMA group to be in an Up state.

Minimum Receive Links. The configured minimum number of active receive links required for the IMA group to be in an Up state.

Near-end Tx Clock Mode. The configured transmit clocking mode used by the near-end of the IMA group, which can be Common Transmit Clock (CTC) mode, where all the IMA links have the same transmit clock source, or Independent Transmit Clock (ITC), where at least one IMA link has a unique transmit clock source.

Far-end Tx Clock Mode. The configured transmit clocking mode used by the far-end of the IMA group, which can be Common Transmit Clock (CTC) mode, where all the IMA links have the same transmit clock source, or Independent Transmit Clock (ITC), where at least one IMA link has a unique transmit clock source.

Tx Frame Length. The configured frame length (in bytes) used by the IMA group in the transmit direction. This field will always display **128** since frame lengths of 128 bytes are the only ones currently supported.

Rx Frame Length. The configured frame length (in bytes) used by the IMA group in the receive direction. This field will always display **128** since frame lengths of 128 bytes are the only ones currently supported.

Max Diff Delay (ms). The configured maximum (in milliseconds) differential delay among the links that will be tolerated on this interface. The default is **25** milliseconds.

Max Diff Delay Obs (ms). The latest operational maximum differential delay observed (in milliseconds) among the receive links that are currently configured in this IMA group. This value indicates the most recent differential observed between the receive link with the least propagation delay and the receive link with the most propagation delay.

Far-end IMA Group ID. The IMA group ID used by the far end of the link.

Rx Timing Ref. Link. The receive reference link for deriving the IMA Data Cell Rate (the rate at which IMA data cells should be exchanged between the IMA sublayer and the ATM layer).

Invalid ICP before HUNT. The configured number of invalid IMA Control Protocol (ICP) cells before moving to the ICP hunt mode.

Tx Timing Ref. Link. The transmit reference link for deriving the IMA Data Cell Rate (rate at which IMA data cells should be exchanged between the IMA sublayer and the ATM layer).

Cons Err ICP before HUNT. The configured number of consecutive invalid IMA Control Protocol (ICP) cells before moving to the ICP hunt.

Cons Valid ICP before SYNC. The configured number of consecutive valid IMA Control Protocol (ICP) cells detected before moving from a pre-synchronized state to a synchronized state. The default value is **5**.

Status Change Time. The amount of time (in days, hours, minutes, seconds, and hundredths of seconds) observed since this IMA group was last modified.

Group Memberships. The configured physical ports used by this IMA group.

CSM Port. The configured CSM port number assigned to this IMA group.

Least Delay Link. The link observed with the least differential delay in the IMA group, compared to other links in this IMA group.

Most Delay Link. The link observed with the greatest differential delay in the IMA group, compared to other links in this IMA group. This value only has meaning if at least one link has been configured in the IMA group.

Test Pattern. The value observed for the IMA Test Pattern Procedure, which can be set from 0 to 255. If **AnyPattern** is displayed, then the IMA software will randomly select a value from 0 to 255.

Displaying the Summary Status of IMA Groups

Test Link. The beginning link used by the IMA test procedure. If **AnyLink** is displayed, then the IMA software will randomly select a link when it starts an IMA test.

Test Pattern Procedure. The configured state of the IMA test procedure, which can one of the following values:

disabled. Indicates that the current test procedure is disabled.

operating. Indicates that the current test procedure is active and the receive pattern on all links in the group match the transmit pattern.

linkFail. Indicates that the current test procedure is active but the receive pattern on one or more link does not match the transmit pattern.

Displaying the Detailed Status of a Single IMA Group with Link Status

To view the detailed status of a single IMA group with the status of the group's links, enter **igps** followed by the IMA group number or the CSM slot/port number and the word **all**. (See *Adding and Modifying IMA Group Membership* on page 43-18 for more information on assigning a CSM port number to an IMA group.) For example, to view the status of IMA Group 0 and its links, enter

igps 0 all

at the system prompt. A screen similar to the following will be displayed.

IMA Group Status for Group 0

```

Description                : IMA Group 0
Admin Status                : up
Failure Status              : noFailure
Near-end State              : operational
Far-end State               : operational
Minimum Transmit Links     : 1           Minimum Receive Links : 1
Near-end Tx Clock Mode    : CTC           Far-end Tx Clock Mode : CTC
Tx Frame Length           : 128          Rx Frame Length       : 128
Max Diff Delay (ms)       : 25           Max Diff Delay Obs (ms) : 0
Far-end IMA Group ID      : 20           Rx Timing Ref. Link   : 5/4
Invalid ICP before HUNT   : 2           Tx Timing Ref. Link   : 5/4
Cons Err ICP before HUNT  : 2
Cons Valid ICP before SYNC : 1
Status Change Time        : 1 days, 21:11:02.48
Group Memberships         : 5/4, 5/5, 5/6
CSM Port                  : 5/3
Least Delay Link          : 5/2
Most Delay Link           : 5/1
Test Pattern              : 255
Test Link                 : AnyLink
Test Pattern Procedure     : disabled
    
```

Slot	Port	Phy. Status	Tx LID	Rx LID	Rel Dly	Transmit State		Receive State	
====	====	=====	===	===	===	=====	=====	=====	=====
5	1	up	0	0	0	active	active	active	active
5	2	up	1	1	0	active	active	active	active
5	3	up	2	2	0	active	active	active	active
5	4	up	3	3	0	active	active	active	active
5	5	up	4	4	0	active	active	active	active
5	6	up	5	5	0	active	active	active	active
5	7	up	6	6	0	active	active	active	active
5	8	up	7	7	0	active	active	active	active

Slot	Port	Rx Test Pattern	Test Proc. Status	Failure Status	
====	====	=====	=====	=====	=====
5	1	0	disabled	noFailure	noFailure
5	2	0	disabled	noFailure	noFailure
5	3	0	disabled	noFailure	noFailure
5	4	0	disabled	noFailure	noFailure
5	5	0	disabled	feRxUnuse	noFailure
5	6	0	disabled	feRxUnuse	noFailure
5	7	0	disabled	feRxUnuse	noFailure
5	8	0	disabled	feRxUnuse	noFailure

Displaying the Summary Status of IMA Groups

The **igps** command with the **all** option groups the fields into three sets. See *Displaying the Detailed Status of a Single IMA Group with Link Status* on page 43-41 for the first set of fields (i.e., **Description** through **Test Pattern Procedure**). The second and third sets of fields display the summary status for every port in the group. These fields are described on the pages that follow.

Phy. Status. This field displays whether the IMA link is active (**up**) or inactive (**down**). For example, if the link is free of active major alarms (e.g., LOS, Red alarm), then it is declared to be in an **up** state; otherwise, it will be declared to be in a **down** state.

Tx LID. The transmit link ID for this link.

Rx LID. The receive link ID number for this link (used by the far-end transmitter). A value of **-1** indicates that the far-end of the link has not been configured.

Rel Dly. The latest measured delay (in milliseconds) on this link as compared to the link with the least delay in the same IMA group.

Near-end Transmit State. The current state of the near-end IMA transmit link. The following are possible values:

- notInGroup.** Indicates that this link is currently not configured to any IMA group.
- unuseNoRsn.** Indicates that this link is not usable because of unknown reason.
- unuseFault.** Indicates that this link is not usable because it is experiencing a fault.
- unuseMisco.** Indicates that this link is not usable because it is misconnected.
- unuseInhibit.** Indicates that this link is administratively brought down while the link is in active state.
- unuseFail.** Indicates that this link is not usable because it is experiencing a failure.
- usable.** Indicates that this link is usable (e.g., free of alarms and faults, etc.).
- active.** Indicates that this link is in active state; it is transmitting ATM layer cells and is part of the data round robin.

Far-end Transmit State. The current state of the far-end IMA transmit link. See the **Near-end Transmit State** field description above for possible values.

Near-end Receive State. The current state of the near-end IMA receive link. See the **Near-end Transmit State** field description above for possible values.

Far-end Receive State. The current state of the far-end IMA receive link. See the **Near-end Transmit State** field description above for possible values.

Rx Test Pattern. The value of the test pattern, which can be from 0 to 255.

Test Proc. Status. This field displays the current status of the IMA test procedure. Possible values include:

- disabled.** Indicates that the current test procedure has been disabled.
- operating.** Indicates that the test procedure is active and the receive pattern on this link matches the transmit pattern.
- linkFail.** Indicates that the test procedure is active and the receive pattern on this link does not match the transmit pattern. When an error occurs, **linkFail** will be displayed until a subsequent read reports the value of **operating** or this field changes to **disabled**, which means that the test procedure was terminated.

Near-end Failure Status. The current link failure status of the near-end receive link. The following are possible values:

noFailure. Indicates that there is no failure on this link.

lnkFail. Indicates that this link is experiencing general failure.

lifFail. Indicates that this link is experiencing loss of IMA failure.

lodsFail. Indicates that this link is experiencing loss of delay synchronization failure.

misCnnctd. Indicates that this link is being misconnected.

blocked. Indicates that this link is being administratively brought down while it is in an active state.

fault. Indicates that this link is experiencing a fault, such as a link alarm.

feTxUnuse. Indicates that the far-end transmit state is not usable.

feRxUnuse. Indicates that the far-end receive state is not usable.

Far-end Failure Status. The current link failure status of the far-end receive link, as reported via the IMA Control Protocol (ICP). See the **Near-end Failure Status** field description above for possible values.

Displaying the Summary Status of IMA Links

To view the status of IMA links, use the **ilks** command. The syntax for this command is as follows:

```
ilks [<slot>/<port>]
```

The **<slot>/<port>** option will give you the status for a single IMA link (see *Displaying the Detailed Status of a Single IMA Link* on page 43-46). If you do not use this option, then you will see a list of the status for every IMA link (see the subsection below).

Displaying the Summary Status of All IMA Links

To view the summary status of every IMA link, enter

```
ilks
```

at the prompt. A screen similar to the following will be displayed.

IMA Links Status									
SI	Prt	Grp	Transmit State		Receive State		Failure Status		
			Near-end	Far-end	Near-end	Far-end	Near-end	Far-end	
5	1	1	Active	Active	Active	Active	noFailure	noFailure	
5	2	1	Inactive	Inactive	Inactive	Inactive	blocked	blocked	
5	9	2	Active	Active	Active	Active	noFailure	noFailure	
5	10	2	Active	Active	Active	Active	noFailure	noFailure	

The fields displayed by the **ilks** command for all IMA links are described below.

SI. The link's slot number.

Prt. The port number, as determined by the switch's software, of the IMA link. For example, the port number printed on a CSM-AB-IMA-DS1/E1-8W submodule does not necessarily correspond with this number. See Chapter 40, "Cell Switching Modules (CSMs)," for more information on CSM-U and CSM-U+ submodule port numbering.

Grp. The IMA group number for this IMA link.

Near-end Transmit State. The current state of the near-end transmit link. The following are possible values:

- notInGroup.** Indicates that this link is currently not configured to any IMA group.
- unuseNoRsn.** Indicates that this link is not usable because of unknown reason.
- unuseFault.** Indicates that this link is not usable because it is experiencing a fault.
- unuseMisco.** Indicates that this link is not usable because it is misconnected.
- unuseInhibit.** Indicates that this link is administratively brought down while the link is in active state.
- unuseFail.** Indicates that this link is not usable because it is experiencing a failure.
- usable.** Indicates that this link is usable (e.g., free of alarms and faults, etc.).
- active.** Indicates that this link is in active state; it is transmitting ATM layer cells and is part of the data round robin.

Far-end Transmit State. The current state of the far-end transmit link, as determined by IMA Control Protocol (ICP) cells. See the **Near-end Transmit State** field description on the previous page for possible values.

Near-end Receive State. The current state of the near-end receive link. See the **Near-end Transmit State** field description above for possible values.

Far-end Receive State. The current state of the far-end receive link, as determined by IMA Control Protocol (ICP) cells. See the **Near-end Transmit State** field description above for possible values.

Near-end Failure Status. The current link failure status of the near-end receive link. The following are possible values:

noFailure. Indicates that there is no failure on this link.

lnkFail. Indicates that this link is experiencing general failure.

lifFail. Indicates that this link is experiencing loss of IMA failure.

lodsFail. Indicates that this link is experiencing loss of delay synchronization failure.

misCnnctd. Indicates that this link is being misconnected.

blocked. Indicates that this link is being administratively brought down while it is in an active state.

fault. Indicates that this link is experiencing a fault, such as a link alarm.

feTxUnuse. Indicates that the far-end transmit state is not usable.

feRxUnuse. Indicates that the far-end receive state is not usable.

Far-end Failure Status. The current link failure status of the far-end receive link, as determined by IMA Control Protocol (ICP) cells.

Displaying the Detailed Status of a Single IMA Link

To view the detailed status of a single IMA link, enter **ilks** followed by the slot and port number. For example, to view to status of Port 1 in Slot 5, enter

```
ilks 5/1
```

at the prompt. A screen similar to the following will be displayed.

Link Status of 5/1

Description	: IMA Link		
Admin Status	: up	Oper Status	: up
Group Index	: 0		
Near-end Tx State	: active	Near-end Rx State	: active
Far-end Tx State	: active	Far-end Rx State	: active
NE Rx Failure Status	: feTxUnuse	FE Rx Failure Status	: noFailure
Tx Link ID	: 0	Rx Link ID	: 0
Relative Delay (ms)	: 0		
Rx Test Pattern	: 255		
Test Proc. Status	: disabled		

The fields displayed by the **ilks** command for a single IMA link are described below.

Description. The configured text description (up to 30 characters) of the IMA link. This field can be modified by the **ilkm** command, which is described in *Configuring IMA Link Parameters* on page 43-28).

Admin Status. The configured administrative status of the IMA link, which can be enabled (**up**) or disabled (**down**).

Oper Status. The operational status of this IMA link, which can be active (**up**) or inactive (**down**).

Group Index. The configured IMA group number on this IMA link.

Near-end Tx State. The current state of the near-end transmit link. See the **Near-end Transmit State** field description in *Displaying the Summary Status of All IMA Links* on page 43-44 for descriptions of possible values.

Near-end Rx State. The current state of the near-end IMA receive link. See the **Near-end Transmit State** field description in *Displaying the Summary Status of All IMA Links* on page 43-44 for descriptions of possible values.

Far-end Tx State. The current state of the far-end transmit link. See the **Near-end Transmit State** field description in *Displaying the Summary Status of All IMA Links* on page 43-44 for descriptions of possible values.

Far-end Rx State. The current state of the far-end IMA receive link. See the **Near-end Transmit State** field description in *Displaying the Summary Status of All IMA Links* on page 43-44 for descriptions of possible values.

NE Rx Failure Status. The current link failure status of the near-end receive link. See the **Near-end Failure Status** field description in *Displaying the Summary Status of All IMA Links* on page 43-44 for descriptions of possible values.

FE Rx Failure Status. The current link failure status of the far-end receive link, as reported via the IMA Control Protocol (ICP). See the **Near-end Failure Status** field description in *Displaying the Summary Status of All IMA Links* on page 43-44 for descriptions of possible values.

Tx Link ID. The configured ID number for the near-end of the IMA link.

Rx Link ID. The receive link ID number for this link (used by the far-end transmitter). A value of **-1** indicates that the far-end of the link has not been configured.

Relative Delay (ms). The latest observed measured delay (in milliseconds) on this link relative to the link, in the same IMA group, with the least delay.

Rx Test Pattern. The value of the test pattern, which can be from 0 to 255.

Test Proc. Status. This field displays the current status of the IMA test procedure. See the **Test Proc. Status** field description in *Displaying the Summary Status of All IMA Links* on page 43-44 for descriptions of possible values.

Displaying the Statistics for an IMA Group

To view the statistics for an IMA group, use the **igpsts** command. The syntax for this command is as follows:

```
igpsts <IMA group id> | <CSM slot/port> [all]
```

The **all** option will give you a detailed list of statistics for an IMA group (see *Displaying Detailed Statistics for an IMA Group* on page 43-50). If you do not use this option, then you will see summary statistics for an IMA group (see *Displaying Summary Statistics for an IMA Group* on page 43-48).

Displaying Summary Statistics for an IMA Group

To view summary statistics for an IMA group, enter **igpsts** followed by the IMA group number or the CSM slot/port number. (See *Adding and Modifying IMA Group Membership* on page 43-18 for more information on assigning a CSM port number to an IMA group.) For example, to view a brief list of statistics for IMA Group 0, enter

```
igpsts 0
```

at the system prompt. A screen similar to the following will be displayed:

```
IMA Group Statistics for Group 0
Near-end Num of Failures : 0          Far-end Num of Failures : 0
Tx Available Cell Rate   : 28976      Rx Available Cell Rate  : 28976
Tx Config Links         : 8           Rx Config Links        : 8
Tx Active Links         : 8           Rx Active Links        : 8
Running Seconds         : 0           Unavailable Seconds    : 0
Rx User Cells           : 0           Tx User Cells          : 0
Tx Buffer Overflow       : 0
```

The fields displayed by the **igpsts** without the **all** option are described below.

Near-end Num of Failures. The observed number of near-end IMA group failures reported since power-up or reboot. A near-end IMA group failure can be caused by an insufficient number of links or a config-abort during startup.

Far-end Num of Failures. The observed number of far-end IMA group failures reported since power-up or reboot. A far-end IMA group failure can be caused by an insufficient number of links at the far end of the link, a blocked operational state at the far end of the link, or a config-abort at the far end of the link during startup.

Tx Available Cell Rate. The observed current rate (in cells per second) provided by this IMA group in the transmit direction. The rate only includes transmitting links in the active state.

Rx Available Cell Rate. The observed current rate (in cells per second) provided by this IMA group in the receive direction. The rate only includes receiving links in the active state.

Tx Config Links. The configured number of links to transmit in this IMA group.

Rx Config Links. The configured number of links to receive in this IMA group.

Tx Active Links. The configured number of active links that can transmit ATM cells in this IMA group (i.e., Tx state OK).

Rx Active Links. The configured number of active that can receive ATM cells in this IMA group (i.e., Rx state OK).

Running Seconds. The observed amount of time (in seconds) since this IMA group has been in operation, or the amount of time (in seconds) since this IMA group ceased operating. Basically, this field displays the amount of time since links have been assigned to this IMA group.

Unavailable Seconds. The observed number of one-second intervals where the IMA group traffic state machine is down.

Rx User Cells. The observed number of ATM layer cells received at the near end.

Tx User Cells. The observed number of ATM layer cells transmitted by the near-end side of the IMA link.

Tx Buffer Overflow. The observed number of cells exceeding the near-end of the IMA link's buffer.

Displaying Detailed Statistics for an IMA Group

To view detailed statistics for an IMA group, enter **igpsts** followed by the IMA group number or the CSM slot/port number and the word **all**. (See *Adding and Modifying IMA Group Membership* on page 43-18 for more information on assigning a CSM port number to an IMA group.) For example, to view a detailed list of statistics for IMA Group 0, enter

igpsts 0 all

at the system prompt. A screen similar to the following will be displayed:

IMA Group Statistics for Group 0

Near-end Num of Failures	:	0	Far-end Num of Failures	:	0
Tx Available Cell Rate	:	28976	Rx Available Cell Rate	:	28976
Num of Tx Config Links	:	8	Num of Rx Config Links	:	8
Num of Tx Active Links	:	8	Num of Rx Active Links	:	8
Running Seconds	:	0	Unavailable Seconds	:	0
Rx User Cells	:	0	Tx User Cells	:	0
Tx Buffer Overflow	:	0			

Slot	Port	Rx ICP Cells	Tx ICP Cells	Rx Filler Cells	Tx Filler Cells	Rx User Cells	Tx User Cells
5	1	7801	23401	990688	2971908	0	0
5	2	7800	23400	990587	2971826	0	0
5	3	7799	23399	990472	2971716	0	0
5	4	7798	23398	990367	2971605	0	0
5	5	7797	23398	990258	2971495	0	0
5	6	7792	23397	989555	2971387	0	0
5	7	7788	23394	989142	2970985	0	0
5	8	7782	23393	988445	2970878	0	0

Slot	Port	Rx Stuff Events	Tx Stuff Events	IMA Violations	OIF Anomalies	Rx Bad ICP Cells	Rx ICP w/ CRC-10 Err
5	1	0	0	0	0	0	0
5	2	0	0	0	0	0	0
5	3	0	0	0	0	0	0
5	4	0	0	0	0	0	0
5	5	0	0	0	0	0	0
5	6	0	0	0	0	0	0
5	7	0	0	0	0	0	0
5	8	0	0	0	0	0	0

—Output continues on next page—

Slot	Port	Tx UUS Near-end	Tx UUS Far-end	Rx UUS Near-end	Rx UUS Far-end	SES Near-end	SES Far-end
5	1	0	0	0	0	0	0
5	2	0	0	0	0	0	0
5	3	0	0	0	0	0	0
5	4	0	0	0	0	0	0
5	5	0	0	0	0	0	0
5	6	0	0	0	0	0	0
5	7	0	0	0	0	0	0
5	8	0	0	0	0	0	0

Slot	Port	UAS Near-end	UAS Far-end	Tx Fails Near-end	Tx Fails Far-end	Rx Fails Near-end	Rx Fails Far-end
5	1	0	0	0	0	0	0
5	2	0	0	0	0	0	0
5	3	0	0	0	0	0	0
5	4	0	0	0	0	0	0
5	5	0	0	0	0	0	0
5	6	0	0	0	0	0	0
5	7	0	0	0	0	0	0
5	8	0	0	0	0	0	0

Slot	Port	Cell In Rx Buffer	Rx Buffer Flushes	Rx Buffer Overflow	Rx Cells Discarded
5	1	0	0	0	0
5	2	0	0	0	0
5	3	0	0	0	0
5	4	0	0	0	0
5	5	0	0	0	0
5	6	1	0	0	0
5	7	0	0	0	0
5	8	0	0	0	0

The **igpsts** command with the **all** option groups the fields into six sets. See *Displaying Summary Statistics for an IMA Group* on page 43-48 for the first set of fields (i.e., **Near-end Num of Failures** through **Tx Buffer Overflow**) shown on the previous page. The second through sixth set of fields display operational statistics for every port in the group. These fields are described below.

Rx ICP Cells. The number of IMA Control Protocol (ICP) cells received at the near-end side of the IMA link. (See *IMA Process Overview* on page 43-4 for more information on ICP cells.)

Tx ICP Cells. The number of IMA Control Protocol (ICP) cells transmitted by the near-end side of the IMA link. (See *IMA Process Overview* on page 43-4 for more information on ICP cells.)

Rx Filler Cells. The number of filler cells received at the near-end side of the IMA link. (See *IMA Process Overview* on page 43-4 for more information on filler cells.)

Tx Filler Cells. The number of filler cells transmitted by the near-end side of the IMA link. (See *IMA Process Overview* on page 43-4 for more information on filler cells.)

Rx User Cells. The number of ATM layer cells for one port received at the near-end side of the IMA link.

Tx User Cells. The number of ATM layer cells for one port transmitted by the near-end side of the IMA link.

Rx Stuff Events. The number of stuff events (i.e., repetition of ICP cells over one IMA link to compensate for timing differences with other links within the IMA group) inserted in the receive direction.

Tx Stuff Events. The number of stuff (i.e., repetition of ICP cells over one IMA link to compensate for timing differences with other links within the IMA group) events inserted in the transmit direction.

IMA Violations. The total number of IMA Control Protocol (ICP) cells with errors, invalid ICP cells, and missing ICP cells that occurred during non-Severely Errored Second (SES) IMA conditions. IMA violations in SES-IMA conditions are not included in this count.

An SES-IMA condition is a condition in which severely-errored seconds (SES) are occurring. An SES is a second during which 30% or more of the ICP cells contain IMA violations or one or more link defect states exist (e.g., loss of signal, out of frame/loss of frame, or loss of cell delineation).

OIF Anomalies. The total number of Out of IMA Frame (OIF) anomalies that have occurred during normal traffic conditions (i.e., non-SES-IMA) at the near end of the link. OIF anomalies in SES-IMA conditions are not included in this count. (See the **IMA Violations** field description above for more information on SES-IMA conditions.)

An OIF anomaly occurs when the IMA frame synchronization mechanism exists in the IMA SYNC state (i.e., the IMA working state). When OIF anomalies persist for at least two (2) IMA frames, the Loss of IMA Frame (LIF) defect state is entered.

Rx Bad ICP Cells. The number of invalid IMA Control Protocol (ICP) cells received at the near-end side of the IMA link.

Rx ICP w/ CRC-10 Err. The number of IMA Control Protocol (ICP) cells with bad CRC-10 received at the near-end side of the IMA link.

Near-end Tx UUS. Near-end transmit unusable seconds. The number of unusable seconds at the near-end transmitting Link State Machine (LSM). The unusable state indicates that the link is configured within an IMA group but is not in use due to a fault, incorrect connectivity revealed by the test pattern procedure, or administrative inhibition for application-dependent or implementation-reasons, etc. (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Far-end Tx UUS. Far-end transmit unusable seconds. The number of unusable seconds at the far-end transmitting Link State Machine (LSM). (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Near-end Rx UUS. Near-end receive unusable seconds. The number of unusable seconds at the near-end receiving Link State Machine (LSM). (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Far-end Rx UUS. Far-end receive unusable seconds. The number of unusable seconds at the far-end receiving Link State Machine (LSM). (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Near-end SES. Near-end severely-errored seconds. The number of one-second intervals in which 30% or more of the IMA Control Protocol (ICP) cells contain IMA violations or one or more link defect states exists (e.g., loss of signal, out of frame/loss of frame, or loss of cell delineation) during non-Unavailable Seconds (UAS)-IMA conditions.

The UAS-IMA condition begins at the onset of ten (10) contiguous severely-errored seconds (SES) and ends at the onset of ten (10) contiguous seconds with no SES.

Far-end SES. Far-end severely-errored seconds. The number of one-second intervals containing one or more Remote Defect Indicator (RDI) IMA defects (which includes IMA link-specific defects).

Near-end UAS. Near-end unavailable seconds. The number of unavailable seconds, which begins at the onset of 10 contiguous Severely Errored Second (SES) IMA conditions and ends at the onset of 10 contiguous non-SES-IMA conditions, at the near end of the link.

An SES is a second during which 30% or more of the IMA Control Protocol (ICP) cells contain IMA violations or one or more link defect states exists. (See the **IMA Violations** field description on page 43-52 for more information on SES-IMA conditions.)

Far-end UAS. Far-end unavailable seconds. The number of unavailable seconds, which begins at the onset of 10 contiguous Severely Errored Second (SES) IMA conditions and ends at the onset of 10 contiguous non-Severely Errored Second (SES) IMA conditions, at the far end (FE) of the link.

An SES-IMA-FE condition is a second during which one or more Remote Defect Indicator (RDI)-IMA defects occurs. The RDI indicates remote defects (which includes IMA link-specific defects).

Near-end Tx Fails. The number of times a near-end transmit failure alarm condition has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Far-end Tx Fails. The number of times a far-end transmit failure alarm condition (e.g., link defect, loss of an IMA frame, loss LODS) has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Near-end Rx Fails. The number of times a near-end receive failure alarm condition has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Far-end Rx fails. The number of times a far-end receive failure alarm condition (e.g., link defect, loss of an IMA frame, loss LODS) has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Cells In Rx Buffer. The number of cells that are currently in the receive buffer.

Rx Buffer Flushes. The number of times that this link's receive buffer has been flushed. The buffer will be flushed if the IMA software internally detects fatal errors.

Rx Buffer Overflow. The number of times that this link's receive buffer has overflowed. For example, the receive buffer can overflow from timing differences.

Rx Cells Discarded. The number of cells discarded. For example, cells can be discarded due to bad ICP cells.

Displaying 24-Hour Performance Statistics on a Local Group

To view the local IMA group performance statistics over the most recently-completed 24-hour period, use the **igplts** command. (If the IMA interface was brought on-line within the last 24 hours, then the current 24-hour period will be displayed.) The syntax for this command is as follows:

```
igplts <IMA group id> | <CSM slot/port>
```

For example, to display the local IMA group performance for IMA group 10 over the most recently-completed 24-hour period, enter

```
igplts 10
```

at the system prompt. A screen similar to the following will be displayed.

```
                24-hour Period Statistics for group 10
Valid Intervals      : 83 of 96           Elapsed Time   : 559 of 900
GR-UAS-IMA         GP-FC-NE         GP-FC-FE
=====
                   4                 1                 1
```

The fields displayed by the **igplts** command are described below.

Valid Intervals. The number of valid 15-minute intervals of for which valid data was collected. The number of intervals will be 96 unless the IMA interface was brought on-line within the last 24-hours.

GR-UAS-IMA. IMA group unavailable seconds. The number of 1-second intervals where the IMA Group Traffic State Machine (GTSM), which indicates the capability of the group to transmit cells from the ATM layer, is down.

GP-FC-NE. The number of times a near-end IMA group failure has been reported. (Invalid intervals will not be counted.) These failures include the following:

Config-Aborted. This failure occurs when the far-end link attempts to use unacceptable configuration parameters.

Insufficient-Links. This failure occurs when there are insufficient transmit or receive links that are in an Active state.

GP-FC-FE. The number of times that a far-end group failure has been reported. These failures include the following:

Config-Aborted-FE. This failure occurs when the far-end link reports to use unacceptable configuration parameters.

Insufficient-Links-FE. This failure occurs when the far-end link reports that there are insufficient transmit or receive links.

Blocked-FE. This failure occurs when the far-end link reports that it is blocked.

Displaying Current Performance Statistics on a Local Group

To view the current local IMA group performance statistics, use the **igpls** command. The syntax for this command is as follows:

```
igpls <IMA group id> | <CSM slot/port>
```

For example, to display the current local performance statistics for IMA group 10, enter

```
igpls 10
```

at the system prompt. A screen similar to the following will be displayed.

```

Current 15-minute Measurement for group 10
Valid Intervals      : 83 of 96      Elapsed Time   : 556 of 900
GR-UAS-IMA         GP-FC-NE      GP-FC-FE
=====
                   0                0                0
    
```

The fields displayed by the **igpls** command are described in *Displaying 24-Hour Performance Statistics on a Local Group* on page 43-54.

Displaying Performance Statistics Intervals on a Local Group

To view up to 96 15-minute intervals of local IMA group performance statistics, use the **igplis** command. The syntax for this command is as follows:

```
igplis <IMA group id> | <CSM slot/port>
```

For example, to display 96 15-minute intervals of local performance statistics for IMA group 10, enter

```
igplis 10
```

at the system prompt. A screen similar to the following will be displayed.

```
15-minute Interval Statistics for group 10

Valid Intervals      : 83 of 96           Elapsed Time   : 561 of 900

Intv#  GR-UAS-IMA  GP-FC-NE  GP-FC-FE
=====  =====  =====
  1           4           1           1
  2           0           0           0
  3           0           0           0
  4           0           0           0
  5           0           0           0
  6           0           0           0
  7           0           0           0
  8           0           0           0
  9           0           0           0
 10           0           0           0
 11           0           0           0
 12           0           0           0
 13           0           0           0
 14           0           0           0
 15           0           0           0
```

Press any key to see next screen.

All of the fields displayed by the **igpcls** command except for the **Intv#** field, which is described below, are described in *Displaying 24-Hour Performance Statistics on a Local Group* on page 43-54.

Intv#. The interval number for this instance, which can be from 1 to 96. A **1** in this field indicates the most recently completed 15-minute interval and a **96** indicates the least recently completed 15-minute interval (assuming that all 96 intervals are valid).

Displaying Detailed Statistics for IMA Links

To display detailed operational statistics of the link associated with a particular port use the **ilksts** command. The syntax for this command is as follows:

```
ilksts <slot/port>
```

Enter **ilksts** followed by the slot and port. For example, to display the statistics of the link on Port 1 in Slot 5, enter

```
ilksts 5/1
```

at the system prompt. A screen similar to the following will be displayed:

```

                                IMA Link Statistics for 5/1
Rx ICP Cells           :    2624374      Tx ICP Cells           :    2624374
Rx Filler Cells        :    333295510    Tx Filler Cells        :    333295510
Tx Stuffs              :           0      Rx Stuff               :           0
Rx User Cells          :           0      Tx User Cells          :           0
Rx Bad ICP Cells       :           0      Rx ICP w/ Bad CRC-10 :           0
Cells In Rx Buffer     :           0      Rx Buffer Flushes     :           0
Rx Buffer Overflow     :           0      Rx Cells Discarded    :           0
IMA Violations        :           0      OIF Anomalies        :           0
Far-end SES           :           0      Near-end SES          :           0
Far-end UAS           :           0      Near-end UAS          :           0
Near-end Tx UUS       :           0      Near-end Rx UUS       :           0
Far-end Tx UUS        :           0      Far-end Rx UUS        :           0
Near-end Tx Failures  :           0      Near-end Rx Failures  :           0
Far-end Tx Failures   :           0      Far-end Rx Failures   :           0

```

The fields displayed by the **ilksts** command are described below.

Rx ICP Cells. The number of IMA Control Protocol (ICP) cells received at the near-end side of the IMA link. (See *IMA Process Overview* on page 43-4 for more information on filler cells.)

Tx ICP Cells. The number of IMA Control Protocol (ICP) cells transmitted by the near-end side of the IMA link. (See *IMA Process Overview* on page 43-4 for more information on filler cells.)

Rx Filler Cells. The number of filler cells received at the near-end side of the IMA link. (See *IMA Process Overview* on page 43-4 for more information on filler cells.)

Tx Filler Cells. The number of filler cells transmitted by the near-end side of the IMA link. (See *IMA Process Overview* on page 43-4 for more information on filler cells.)

Tx Stuffs. The number of stuff events (i.e., repetition of ICP cells over one IMA link to compensate for timing differences with other links within the IMA group) inserted in the transmit direction.

Rx Stuff. The number of stuff events (i.e., repetition of ICP cells over one IMA link to compensate for timing differences with other links within the IMA group) inserted in the receive direction.

Rx User Cells. The number of ATM layer cells received at the near-end side of the IMA link.

Tx User Cells. The number of ATM layer cells transmitted by the near-end side of the IMA link.

Rx Bad ICP Cells. The number of invalid IMA Control Protocol (ICP) cells received at the near-end side of the IMA link.

Rx ICP w/ Bad CRC-10. The number of IMA Control Protocol (ICP) cells with a CRC-10 error received at the near-end side of the IMA link.

Cells In Rx Buffer. The number of cells that are currently in the receive buffer.

Rx Buffer Flushes. The number of times that this link's receive buffer has been flushed. The buffer will be flushed if the IMA software internally detects fatal errors.

Rx Buffer Overflow. The number of times that this link's receive buffer has overflowed. For example, the receive buffer can overflow from timing differences.

Rx Cells Discarded. The number of cells discarded. For example, cells can be discarded due to bad ICP cells.

IMA Violations. The total number of IMA Control Protocol (ICP) cells with errors, invalid ICP cells, and missing ICP cells that occurred during non-Severely Errored Second (SES) IMA conditions. IMA violations in SES-IMA conditions are not included in this count.

An SES-IMA condition is a second in which severely-errored seconds (SES) are occurring. An SES is second during which 30% or more of the ICP cells contain IMA violations or one or more link defect states exist (e.g., loss of signal, out of frame/loss of frame, or loss of cell delineation).

OIF Anomalies. The total number of Out of IMA Frame (OIF) anomalies that have occurred during normal traffic conditions (i.e., non-SES-IMA) at the near end of the link. OIF anomalies in SES-IMA conditions are not included in this count. (See the **IMA Violations** field description above for more information on SES-IMA conditions.)

An OIF anomaly occurs when the IMA frame synchronization mechanism exists in the IMA SYNC state (i.e., the IMA working state). When OIF anomalies persist for at least two (2) IMA frames, the Loss of IMA Frame (LIF) defect state is entered.

Far-end SES. Far-end severely-errored seconds. The number of one-second intervals containing one or more Remote Defect Indicator (RDI) IMA defects (which includes IMA link-specific defects).

Near-end SES. Near-end severely-errored seconds. The number of one-second intervals in which 30% or more of the IMA Control Protocol (ICP) cells contain IMA violations or one or more link defect states exist (e.g., loss of signal, out of frame/loss of frame, or loss of cell delineation) during non-Unavailable Seconds (UAS)-IMA conditions.

The UAS-IMA condition begins at the onset of ten (10) contiguous severely-errored seconds (SES) and ends at the onset of ten (10) contiguous seconds with no SES.

Far-end UAS. Far-end unavailable seconds. The number of unavailable seconds, which begins at the onset of 10 contiguous Severely Errored Second (SES) IMA conditions and ends at the onset of 10 contiguous non-Severely Errored Second (SES) IMA conditions, at the far end (FE) of the link.

An SES-IMA-FE condition is a second one or more Remote Defect Indicator (RDI)-IMA defects. The RDI indicates remote defects (which includes IMA link-specific defects).

Near-end UAS. Near-end unavailable seconds. The number of unavailable seconds, which begins at the onset of 10 contiguous Severely Errored Second (SES) IMA conditions and ends at the onset of 10 contiguous non-Severely Errored Second (SES) IMA conditions, at the near end of the link.

An SES is a second in which 30% or more of the IMA Control Protocol (ICP) cells contain IMA violations or one or more link defect states exist. (See the **IMA Violations** field description above for more information on SES-IMA conditions.)

Near-end Tx UUS. Near-end transmit unusable seconds. The number of unusable seconds at the near-end transmitting Link State Machine (LSM). The unusable state indicates that the link is configured within an IMA group but is not in use due to a fault, incorrect connectivity revealed by the test pattern procedure, or administrative inhibition for application-dependent or implementation-reasons, etc. (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Near-end Rx UUS. Near-end receive unusable seconds. The number of unusable seconds at the near-end receiving Link State Machine (LSM). (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Far-end Tx UUS. Far-end transmit unusable seconds. The number of unusable seconds at the far-end transmitting Link State Machine (LSM). (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Far-end Rx UUS. Far-end receive unusable seconds. The number of unusable seconds at the near end receiving Link State Machine (LSM). (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Near-end Tx Failures. The number of times a near-end transmit failure alarm condition has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Near-end Rx Failures. The number of times a near-end receive failure alarm condition has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Far-end Tx Failures. The number of times a far-end transmit failure alarm condition (e.g., link defect, loss of an IMA frame, loss LODS) has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Far-end Rx Failures. The number of times a far-end receive failure alarm condition (e.g., link defect, loss of an IMA frame, loss LODS) has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Displaying 24-Hour Performance Statistics on a Local Link

To display performance statistics of the local link associated with a particular port over a 24-hour period, use the `ilkIts` command. The syntax for this command is as follows:

```
ilkIts <slot/port>
```

Enter `ilkIts` followed by the slot and port. For example, to display the statistics of the link on Port 4 in Slot 5, enter

```
ilkIts 5/4
```

at the system prompt. A screen similar to the following will be displayed:

```
24-hour Period Statistics for port 4 on slot 5

Valid Intervals      : 96 of 96      Elapsed Time      : 25 of 900

Ima Violations      :          2      Oif Anomalies     :          0
Far-end SES         :          0      Near-end SES      :          0
Far-end UAS         :          0      Near-end UAS     :          0
Near-end Tx UUS     :          4      Near-end Rx UUS  :          1
Far-end Tx UUS     :          2      Far-end Rx UUS   :          0
Near-end Tx Failures :          0      Near-end Rx Failures :          0
Far-end Tx Failures :          0      Far-end Rx Failures :          0
Tx Stuffs           :    107841      Rx Stuff         :    107840
```

The fields displayed by the `ilkIts` command are described below.

Valid Intervals. The number of valid 15-minute intervals of for which valid data was collected. The number of intervals will be 96 unless the IMA interface was brought on-line within the last 24-hours.

Elapsed Time. The number of seconds that have elapsed since the beginning of the current measurement period.

IMA Violations. The total number of ICP cells with errors, invalid ICP cells, and missing ICP cells that occurred during non-Severely Errored Second (SES) IMA conditions. IMA violations in SES-IMA conditions are not included in this count.

An SES-IMA condition is a second during which severely-errored seconds (SES) are occurring. An SES is second in which 30% or more of the IMA Control Protocol (ICP) cells contain IMA violations or one or more link defect states exist (e.g., loss of signal, out of frame/loss of frame, or loss of cell delineation).

OIF Anomalies. The total number of Out of IMA Frame (OIF) anomalies that have occurred during normal traffic conditions (i.e., non-SES-IMA) at the near end of the link. OIF anomalies in SES-IMA conditions are not included in this count. (See the **IMA Violations** field description above for more information on SES-IMA conditions.)

An OIF anomaly occurs when the IMA frame synchronization mechanism exists in the IMA SYNC state (i.e., the IMA working state). When OIF anomalies persist for at least two (2) IMA frames, the Loss of IMA Frame (LIF) defect state is entered.

Far-end SES. Far-end severely-errored seconds. The number of one-second intervals containing one or more Remote Defect Indicator (RDI) IMA defects (which includes IMA link-specific defects).

Near-end SES. Near-end severely-errored seconds. The number of one-second intervals in which 30% or more of the IMA Control Protocol (ICP) cells contain IMA violations or one or more link defect states exists (e.g., loss of signal, out of frame/loss of frame, or loss of cell delineation) during non-Unavailable Seconds (UAS)-IMA conditions.

The UAS-IMA condition begins at the onset of ten (10) contiguous severely-errored seconds (SES) and ends at the onset of ten (10) contiguous seconds with no SES.

Far-end UAS. Far-end unavailable seconds. The number of unavailable seconds, which begins at the onset of 10 contiguous Severely Errored Second (SES) IMA conditions and ends at the onset of 10 contiguous non-Severely Errored Second (SES) IMA conditions, at the far end (FE) of the link.

An SES-IMA-FE condition is a second one or more Remote Defect Indicator (RDI)-IMA defects. The RDI indicates remote defects (which includes IMA link-specific defects).

Near-end UAS. Near-end unavailable seconds. The number of unavailable seconds, which begins at the onset of 10 contiguous Severely Errored Second (SES) IMA conditions and ends at the onset of 10 contiguous non-Severely Errored Second (SES) IMA conditions, at the near end of the link.

An SES is a second in which 30% or more of the IMA Control Protocol (ICP) cells contain IMA violations or one or more link defect states exists. (See the **IMA Violations** field description on the previous page for more information on SES-IMA conditions.)

Near-end Tx UUS. Near-end transmit unusable seconds. The number of unusable seconds detected at the near-end transmitting Link State Machine (LSM). The unusable state indicates that the link is configured within an IMA group but is not in use due to a fault, incorrect connectivity revealed by the test pattern procedure, or administrative inhibition for application-dependent or implementation-reasons, etc. (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Near-end Rx UUS. Near-end receive unusable seconds. The number of unusable seconds at the near-end receiving Link State Machine (LSM). (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Far-end Tx UUS. Far-end transmit unusable seconds. The number of unusable seconds at the far-end transmitting Link State Machine (LSM). (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Far-end Rx UUS. Far-end receive unusable seconds. The number of unusable seconds at the near end receiving Link State Machine (LSM).

Near-end Tx Num of Failures. The number of times a near-end transmit failure alarm condition has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Near-end Rx Num of Failures. The number of times a near-end receive failure alarm condition has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Far-end Tx Num of Failures. The number of times a far-end transmit failure alarm condition (e.g., link defect, loss of an IMA frame, loss LODS) has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Far-end Rx Num of Failures. The number of times a far-end receive failure alarm condition (e.g., link defect, loss of an IMA frame, loss LODS) has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Tx Stuffs. The number of stuff events (i.e., repetition of ICP cells over one IMA link to compensate for timing differences with other links within the IMA group) inserted in the transmit direction.

Rx Stuff. The number of stuff events (i.e., repetition of ICP cells over one IMA link to compensate for timing differences with other links within the IMA group) inserted in the receive direction.

Displaying Current Performance Statistics on a Local Link

To display the current performance statistics of the local link associated with a particular port, use the **ilkcls** command. The syntax for this command is as follows:

ilkcls <slot/port>

Enter **ilkcls** followed by the slot and port. For example, to display the statistics of the link on Port 4 in Slot 5, enter

ilkcls 5/4

at the system prompt. A screen similar to the following will be displayed:

```

Current 15-minute Measurement for port 4 on slot 5

Valid Intervals      : 96 of 96      Elapsed Time      : 23 of 900
Ima Violations      :          0      Oif Anomalies     :          0
Far-end SES         :          0      Near-end SES      :          0
Far-end UAS         :          0      Near-end UAS     :          0
Near-end Tx UUS     :          0      Near-end Rx UUS  :          0
Far-end Tx UUS      :          0      Far-end Rx UUS   :          0
Near-end Tx Failures :          0      Near-end Rx Failures :          0
Far-end Tx Failures :          0      Far-end Rx Failures :          0
Tx Stuffs           :          41      Rx Stuff         :          4
    
```

The fields displayed by the **ilkcls** command are described in *Displaying 24-Hour Performance Statistics on a Local Link* on page 43-60.

Displaying Performance Statistics Intervals on a Local Link

To display up to 96 15-minute intervals of performance statistics of the local link associated with a particular port, use the **ilkliis** command. The syntax for this command is as follows:

ilkliis <slot/port>

Enter **ilkliis** followed by the slot and port. For example, to display the statistics of the link on Port 4 in Slot 5, enter

ilkliis 5/4

at the system prompt. A screen similar to the following will be displayed:

15-minute Interval Statistics for port 4 on slot 5

Valid Intervals	: 2 of 96	Elapsed Time	: 285 of 900					
Intv#	IMA Violations	OIF Anomalies	SES Near-end	SES Far-end	UAS Near-end	UAS Far-end	Rx UUS Near-end	Rx UUS Far-end
1	0	0	0	0	0	0	0	0
2	2	2	4	3	0	0	702	701
Intv#	Tx UUS Near-end	Tx UUS Far-end	Rx Fails Near-end	Rx Fails Far-end	Tx Fails Near-end	Tx Fails Far-end	Rx Stuff Events	Tx Stuff Events
1	0	0	0	0	0	0	0	0
2	702	701	0	0	0	0	343	1576

The fields displayed by the **ilkliis** command are described below.

Valid Intervals. The number of valid 15-minute intervals of for which valid data was collected. The number of intervals will be 96 unless the IMA interface was brought on-line within the last 24-hours.

Elapsed Time. The number of seconds that have elapsed since the beginning of the current measurement period.

Intv#. The interval number for this instance, which can be from 1 to 96. A **1** in this field indicates the most recently completed 15-minute interval and a **96** indicates the least recently completed 15-minute interval (assuming that all 96 intervals are valid).

IMA Violations. The total number of ICP cells with errors, invalid ICP cells, and missing ICP cells that occurred during non-Severely Errored Second (SES) IMA conditions. IMA violations in SES-IMA conditions are not included in this count.

An SES-IMA condition is a second during which severely-errored seconds (SES) are occurring. An SES is a second in which 30% or more of the IMA Control Protocol (ICP) cells contain IMA violations or one or more link defect states exist (e.g., loss of signal, out of frame/loss of frame, or loss of cell delineation).

OIF Anomalies. The total number of Out of IMA Frame (OIF) anomalies that have occurred during normal traffic conditions (i.e., non-SES-IMA) at the near end of the link. OIF anomalies in SES-IMA conditions are not included in this count. (See the **IMA Violations** field description on the previous page for more information on SES-IMA conditions.)

An OIF anomaly occurs when the IMA frame synchronization mechanism exists in the IMA SYNC state (i.e., the IMA working state). When OIF anomalies persist for at least two (2) IMA frames, the Loss of IMA Frame (LIF) defect state is entered.

SES Near-end. Near-end severely-errored seconds. The number of one-second intervals in which 30% or more of the IMA Control Protocol (ICP) cells contain IMA violations or one or more link defect states exists (e.g., loss of signal, out of frame/loss of frame, or loss of cell delineation) during non-Unavailable Seconds (UAS)-IMA conditions.

The UAS-IMA condition begins at the onset of ten (10) contiguous severely-errored seconds (SES) and ends at the onset of ten (10) contiguous seconds with no SES.

SES Far-end. Far-end severely-errored seconds. The number of one-second intervals containing one or more Remote Defect Indicator (RDI) IMA defects (which includes IMA link-specific defects).

UAS Near-end. Near-end unavailable seconds. The number of unavailable seconds, which begins at the onset of 10 contiguous Severely Errored Second (SES) IMA conditions and ends at the onset of 10 contiguous non-Severely Errored Second (SES) IMA conditions, at the near end of the link.

An SES is a second in which 30% or more of the IMA Control Protocol (ICP) cells contain IMA violations or one or more link defect states exists. (See the **IMA Violations** field description on the previous page for more information on SES-IMA conditions.)

UAS Far-end. Far-end unavailable seconds. The number of unavailable seconds, which begins at the onset of 10 contiguous Severely Errored Second (SES) IMA conditions and ends at the onset of 10 contiguous non-Severely Errored Second (SES) IMA conditions, at the far end (FE) of the link.

An SES-IMA-FE condition is a second one or more Remote Defect Indicator (RDI)-IMA defects. The RDI indicates remote defects (which includes IMA link-specific defects).

Rx UUS Near-end. Near-end receive unusable seconds. The number of unusable seconds at the near-end receiving Link State Machine (LSM). (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Rx UUS Far-end. Far-end receive unusable seconds. The number of unusable seconds at the near end receiving Link State Machine (LSM).

Tx UUS Near-end. Near-end transmit unusable seconds. The number of unusable seconds detected at the near-end transmitting Link State Machine (LSM). The unusable state indicates that the link is configured within an IMA group but is not in use due to a fault, incorrect connectivity revealed by the test pattern procedure, or administrative inhibition for application-dependent or implementation-reasons, etc. (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Tx UUS Far-end. Far-end transmit unusable seconds. The number of unusable seconds at the far-end transmitting Link State Machine (LSM). (See *IMA Link State Machine (LSM)* on page 43-11 for more information on the LSM.)

Rx Fails Near-end . The number of times a near-end receive failure alarm condition has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Rx Fails Far-end. The number of times a far-end receive failure alarm condition (e.g., link defect, loss of an IMA frame, loss LODS) has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Tx Fails Near-end. The number of times a near-end transmit failure alarm condition has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Tx Fails Far-end. The number of times a far-end transmit failure alarm condition (e.g., link defect, loss of an IMA frame, loss LODS) has occurred on this link. A failure alarm occurs when a required function cannot be performed and the defect persists for a set amount of time.

Rx Stuff Events. The number of stuff events (i.e., repetition of ICP cells over one IMA link to compensate for timing differences with other links within the IMA group) inserted in the receive direction.

Tx Stuff Events. The number of stuff (i.e., repetition of ICP cells over one IMA link to compensate for timing differences with other links within the IMA group) events inserted in the transmit direction.

Clearing IMA Group Statistics

You clear IMA group statistics with the **igpcls** command. The syntax for this command is as follows:

```
igpcls <IMA group id> | <CSM slot/port> [all]
```

To clear the group's statistics but not its links, enter **igpcls** followed by the IMA Group number or the CSM slot/port number. (See *Adding and Modifying IMA Group Membership* on page 43-18 for more information on assigning a CSM port number to an IMA group.) For example, to clear the statistics for IMA Group 0 but not its links, enter

```
igpcls 0
```

at the system prompt. If the statistics were successfully cleared, then the following will be displayed.

```
Statistics of group 0 have been cleared.
```

The **all** option will clear the statistics of an IMA group and all of its links. For example, to clear the statistics for IMA Group 0 and the statistics for all of its links, enter

```
igpcls 0 all
```

at the system prompt. If the statistics were successfully cleared, then a screen similar to the following will be displayed.

```
Statistics of group 0 have been cleared.  
Statistics of link 5/1 have been cleared.  
Statistics of link 5/2 have been cleared.  
Statistics of link 5/3 have been cleared.  
Statistics of link 5/4 have been cleared.  
Statistics of link 5/5 have been cleared.  
Statistics of link 5/6 have been cleared.  
Statistics of link 5/7 have been cleared.  
Statistics of link 5/8 have been cleared.
```

Clearing IMA Link Statistics

You clear the accumulated statistics for an IMA link with the **ilkcls** command. The syntax for this command is as follows:

```
ilkcls <slot/port>
```

Enter **ilkcls** followed by the slot on port of the link. For example, to clear all the statistics of the IMA link on Port 1 of Slot 5, enter

```
ilkcls 5/1
```

at the system prompt. If the statistics were successfully cleared, the following will be displayed.

```
Statistics of port 5/1 have been cleared.
```

Troubleshooting IMA Networks

Refer to the steps below for general guidelines on troubleshooting problems in IMA networks. In general, always look to simple problems first (e.g., T1 or E1 connection problems).

1. Check the summary and/or statistics of all IMA groups with the **igps** command to find the IMA group(s) with non-operational status (see *Displaying the Summary Status of All IMA Groups* on page 43-35).
2. Check the IMA group's link status with the **igps** command using the group ID (or CSM slot/port number) with the **all** option to find the link(s) with non-operational status (see *Displaying the Detailed Status of a Single IMA Group with Link Status* on page 43-41).
3. Check specific links with the **ilks** command (see *Displaying the Summary Status of IMA Links* on page 43-44) and/or the **ilksts** command (see *Displaying Detailed Statistics for IMA Links* on page 43-57) to determine link status and/or statistics. If you discover a problem with one of the links, proceed to Step 4.

If you do not find any problems with IMA links, use the **igps** command with the group ID (or CSM slot/port) to check the configuration of the IMA group(s) and use the **igpm** command to correct any problems.

4. Check the T1/E1 port status and/or statistics with the status/statistics commands in the **te** submenu (e.g., the **tes**, **telts**, and **terts** commands). (See Chapter 53, "Managing T1 and E1 Ports," for more information on the **te** submenu.) Correct any problems with physical connections and use the **igpm** and/or **temod** commands to correct any software problems.

If you still cannot determine the nature of the problem(s), you can try restarting the IMA group(s) with the **igprst** command, which is described in *Restarting an IMA Group* on page 43-32. However, restarting an IMA group may cause loss of data and might not solve the problems. If you have determined that there are absolutely no physical or configuration problems, contact Alcatel technical support for assistance.

44 ATM Accounting

ATM Accounting allows you to keep track of resources used by a switch's connections. This includes not only length of time and amount of data transmitted while the connection is established, but detailed information about the connection itself, local and remote side parameters, user-to-network and network-to-user traffic, call release information, and cell counter data. Such information is valuable for generating statistics and for creating billing reports.

ATM Accounting can be configured using either of the following tools:

- the Command Line Interface (CLI)
- the Accounting application within OmniVista, Alcatel's network management system.

For setting configuration parameters, either of these methods is acceptable. To view and manage call accounting data, however, you will need to use OmniVista's Accounting application.

This chapter gives an overview of ATM Accounting and discusses concepts you need to understand in order to configure this feature. It also provides examples on how to configure the accounting function using CLI commands.

For a complete list of ATM accounting commands, along with detailed information on each of the parameters, refer to chapter titled "ATM Accounting Commands" in the *Text-Based Configuration* manual.

For information on how to configure ATM Accounting using OmniVista, refer to OmniVista's Accounting online Help.

Hardware Support

ATM accounting is only supported on CSMs with the IOP2 ASIC. See the table below for more information.

CSMs with the IOP2 ASIC

CSM Module	Part Number	CSM Module	Part Number
CSM-155-6M2S	P/N 050113-76	CSM-622FSH-2E	P/N 050133-88
CSM-155-6M2SL	P/N 050113-81	CSM-A25-12	P/N 050134-68
CSM-155-8	P/N 050113-75	CSM-A25-24	P/N 050134-69
CSM-155-8S	P/N 050113-73	CSM-U	P/N 050157-88
CSM-155C-8	P/N 050113-74	FCSM-I-4C	P/N 050129-68
CSM-155-FSL-8	P/N 050113-80	FCSM-IIW-4C	P/N050181-68
CSM-622-2E	P/N 050133-90	FCSM-IIW-4C	P/N 050181-66
CSM-622-2SE	P/N 050133-89	CSM-U+	P/N 050345-66

Accounting Overview

By default, the accounting function is disabled. Therefore, you must begin first by enabling this feature, specifically at the switch level. Accounting can be enabled at the node (or switch) level, the port level, or the PVC/Soft PVC level.

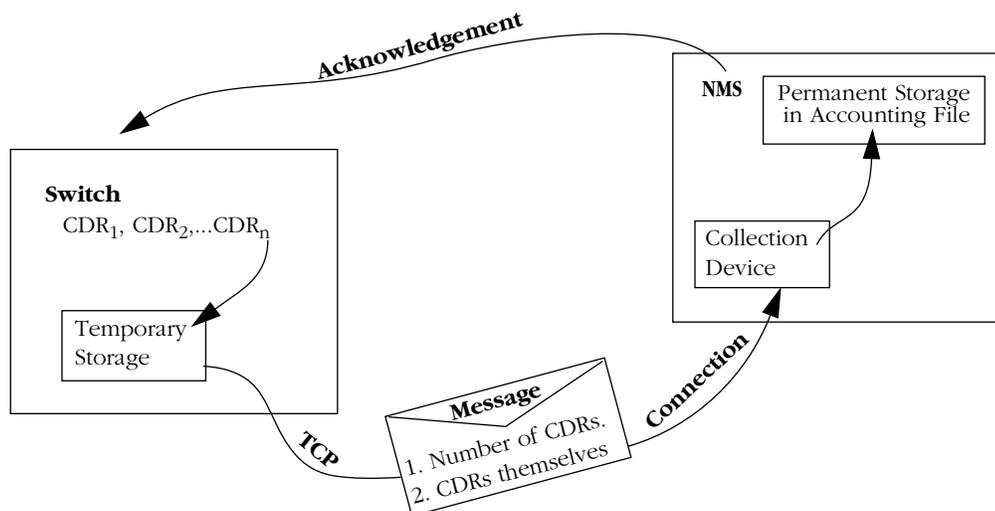
You can also configure parameters such as how frequently accounting information is collected, how often it is sent to the network management system, and how accounting information should be managed during periods of congestion.

The accounting process can be summarized as follows. As data passes through the network, the switch generates accounting information in the form of a Charging Detail Record or “CDR,” also known as a “ticket.” CDRs are generated at both ingress and egress, allowing the switch to record how much traffic is being sent into and out of the network at each endpoint.

A CDR provides data about a single connection. It includes information such as CDR sequence number, ATM identifier, start time, duration, connection type, local and remote VPI and VCI, etc.

As CDRs are generated, they are held in a temporary storage area within the switch. At user-configurable intervals, they are sent, via a TCP connection, to the collection device at the network management system (NMS). CDRs are sent in the form of a message. Each message consists of two parts: the number of CDRs contained in the message, and the CDRs themselves.

After CDRs reach the collection device, they are saved in a permanent storage area, in an accounting file on the NMS. The NMS then sends an acknowledgement to the switch, indicating that it successfully received the CDRs. At that point, the switch deletes those CDRs from its temporary storage, thus freeing up space for new CDRs. The figure below illustrates the process.



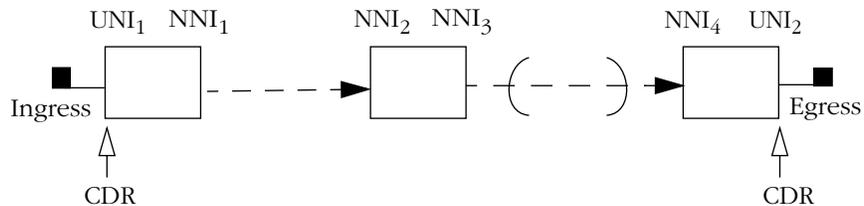
How the Accounting Process Works

After the CDRs are securely stored in the accounting file on the NMS, you can search for and view individual CDRs or groups of CDRs using OmniVista's Accounting application. Each switch has its own accounting file on the NMS, and using the Accounting application, accounting files can be backed up, converted to other file formats, and transferred to an external host, such as a billing center. Discussion of these topics is beyond the scope of this chapter. However, detailed information can be found in the Accounting online Help.

CDRs and the Concept of "Charging"

Charging Detail Records (CDRs) can be generated for both physical and logical ATM interfaces, and for all types of ATM virtual circuits, including Permanent Virtual Circuits (PVCs), Soft Permanent Virtual Circuits (SPVCs), and Switched Virtual Circuits (SVCs).

In a simple network configuration, such as the one represented by the following logical topology, data enters at one endpoint, passes through an intermediate switch, travels through a transit network, then reaches its destination at the far end.



CDR Generation at Ingress and Egress

CDRs are generated at the network ingress point (UNI₁) and at the network egress point (UNI₂).

It is possible to configure the switch to generate a CDR at every ingress and egress point along the network path. However, in the case of a transit switch, this is unnecessary. Doing so would only result in the creation of large numbers of CDRs and could well contribute to network congestion.

If, however, a connection were to span multiple network vendors, you might then want to configure CDR generation for other points along the network path. For example, between UNI₁ and NNI₃, and between NNI₄ and UNI₂, assuming that a transit network exists between NNI₃ and NNI₄.

For point-to-multipoint connections, a CDR would be generated at the connection root and at each of the leaves.

Terminated CDRs and Intermediate CDRs

To understand what conditions trigger a switch to generate a CDR, either for an SVC, or for a PVC or Soft PVC (SPVC), you need to distinguish between two types of CDRs: a “Terminated CDR” and an “Intermediate CDR.”

A “Terminated CDR” is a CDR which is generated whenever a connection is released (“ended”) or terminated (“deleted”).

An “Intermediate CDR” is a CDR which is generated either at the end of a user-configured periodic collection interval (for example, at the end of every 3-hour period), or whenever a “tariff period” occurs (for instance, at 9:00 am or 5:30 pm, assuming those are the times when a rate change occurs). A CDR is characterized as “intermediate” because the CDR is generated before the connection has been released or terminated. For more information on collection intervals and tariff periods, refer to the section *Periodic Collection of CDRs* on page 44-6.

The tables below list the events which cause a CDR to be generated for an SVC or for a PVC or Soft PVC. CDR type (Terminated or Intermediate) is also indicated.

Note that a switch will generate a CDR for an unsuccessful SVC call attempt, but not for an unsuccessful Soft PVC (SPVC) call attempt.

Events that Trigger a CDR for an SVC

Event	CDR Type
1. A call ended or the connection was deleted.	Terminated CDR
2. Either a collection interval or a tariff period (i.e., rate change) occurred.	Intermediate CDR
3. A call establishment attempt was unsuccessful.	Terminated CDR

Events that Trigger a CDR for a PVC or Soft PVC

Event	CDR Type
1. A PVC or Soft PVC was cleared or deleted.	Terminated CDR
2. Either a collection interval or a tariff period (i.e., rate change) occurred.	Intermediate CDR
3. PVC or Soft PVC configuration parameters were modified. (Parameter modification is comparable to the current PVC or Soft PVC connection ending or being completed. Immediately thereafter a new CDR reflecting the modified configuration parameters will automatically be opened.)	Terminated CDR

Periodic Collection of CDRs

The Benefits of Using Periodic Collection

Instead of configuring the switch to always wait for a connection to terminate before generating a CDR, you can configure periodic collection of CDRs. This is the difference between configuring the switch to generate *only* Terminated CDRs and configuring the switch to generate Terminated CDRs *and* Intermediate CDRs.

As explained earlier, a CDR is characterized as “intermediate” because the CDR is generated before the connection has been released or terminated.

Some of the benefits of using periodic collection include the following:

- If the switch is accidentally reset, a strategy of more frequent, periodic collection of CDRs will prevent you from losing large amounts of accounting data.
- Counter rollover of fast-changing values can be avoided. If counter rollover were to occur, this would result in collection of erroneous cell count information.
- By configuring the switch to generate a CDR at the time at which a rate change occurs, different tariff rates can be accommodated.

Two types of periodic collection are available: those based on a collection interval, and those based on a tariff period. Each is described below.

Collection Interval

A collection interval is a regular interval of time, at the end of which a CDR is generated. You may configure only one collection interval. The available interval values are: 1, 2, 3, or 12 hours. The default collection interval is 3 hours.

Tariff Period

A tariff period is a specific time at which a rate change occurs. You may configure up to 8 tariff periods in a single day. A tariff period represents a specific time of day, whereas a collection interval spans a duration of time.

A tariff period must be a multiple of 15 minutes, and no less than 1 hour since the last tariff period or since the last collection interval expired. For example, a tariff period could be set for 4:00 pm, 5:00 pm, 6:15 pm, 7:45 pm, etc. In reality, however, tariff periods would never change with that frequency.

How Periodic Collection is Computed

The accounting function uses the 24-hour system of timekeeping, beginning at 00:00 hours.

A collection interval is computed relative to the midnight hour (or 00:00). For example, if you configure a collection interval of 3 hours, the scheduled collection times are computed relative to, and beginning with, the hour 00:00. Hence, a collection would occur at 00:00, 03:00, 06:00, 09:00, 12:00, 15:00, 18:00, and 21:00.

Combining A Collection Interval With Tariff Periods

A collection interval and tariff periods are not mutually exclusive. Configuring one type of periodic collection does not preclude you from configuring the other type. The two can be combined quite effectively.

Note that if the end of a collection interval and a tariff period coincide, only one intermediate CDR will be generated, rather than two separate CDRs containing the identical information.

Example

Suppose you are concerned that, in the event the switch is reset or some other unforeseen problem occurs, you will lose large amounts of accounting data. As a precaution, you configure a collection interval, using the default interval of 3 hours. Thus, every three hours the switch will generate an intermediate CDR for each connection for which accounting has been enabled.

In addition, you want to accommodate two different tariff rates: the rate which is in effect during regular business hours (9 am - 5 pm), and the rate in effect during off-peak hours (5 pm - 9 am). You accomplish this by configuring two tariff periods, one at 9 am and the other at 5 pm.

The table below shows the times at which a 3-hour collection interval generates an intermediate CDR. It also indicates the times when a tariff period collection occurs. Notice that at 9 am the collection interval coincides with the tariff period, making it unnecessary to generate a separate CDR for the tariff period. However, at 5 pm the collection interval does not coincide with the tariff period; therefore, a separate CDR will be generated for the tariff period.

Combining A Collection Interval With Two Tariff Periods

3-Hour Collection Interval	Tariff Period	Comments
Midnight		
3 am		
6 am		
9 am	9 am	Tariff rate change occurs. Collection interval and tariff period coincide. Only one CDR will be generated, not two.
Noon		
3 pm		
	5 pm	Tariff rate change occurs. Tariff period does not coincide with a collection interval. A new CDR will be generated.
6 pm		
9 pm		

At the end of a tariff period, the switch collects all accounting data for that period in an intermediate CDR. Immediately thereafter, the switch opens up a new CDR for the next tariff period. Without this capability, you would be limited to charging the same rate for the entire duration of the connection, or else manually computing it afterwards.

Maximum Number of Collects

There can be no more than 24 collects per day. This includes both collection intervals and tariff periods.

For example, suppose you configure a collection interval of one hour. This is equivalent to 24 collects in a single day. This makes it impossible to add any tariff periods, as doing so would exceed the 24-collect-per-day maximum.

However, if you were to configure a collection interval of two hours (i.e., 12 collects per day), that would make it possible to configure as many as twelve 1-hour tariff periods. Realistically, though, tariff periods would not occur with that frequency.

How CDRs Are Stored

Storage Strategy

As CDRs are being generated, they are held in a temporary storage area within the switch. The switch establishes a TCP connection to the network management system, then sends the CDRs to the NMS, where they are permanently stored on disk in an accounting file. To confirm that the CDRs were received successfully, the NMS sends the switch an acknowledgment. At that point, the switch deletes the acknowledged CDRs from its temporary storage. (See also the explanation of storage in the *Accounting Overview* on page 44-2).

Size of Temporary Storage

The size of the switch's temporary storage is determined by the maximum number of taxable (i.e., "chargeable") connections you choose to configure. The range is 0-8000 connections, with the default being 3000.

In determining the size of temporary storage, the accounting application requires the following:

1. The switch must be able to store 10 minutes worth of CDRs at a rate of 5 CDRs per second. This is equivalent to storing 3000 CDRs, or, in other words, being able to accommodate a maximum of 3000 taxable connections:

$$(5 \text{ CDRs/sec}) \times (60 \text{ seconds}) \times (10 \text{ minutes}) = 3000 \text{ CDRs}$$
2. In addition, the switch must also store a "holdCDR" for each connection. The "holdCDR" contains information needed to calculate the differences between successive intermediate CDRs. Whereas the regular CDR is sent to the NMS to be included in the switch's accounting file, the holdCDR is "held" or stored in the switch for a certain length of time, so that the switch can later compute and record information such as duration of the connection and volume of data transmitted.

In effect, the switch is storing two CDRs for each connection. Hence, the switch's temporary storage must be large enough to accommodate two times the maximum number of taxable connections. Thus, if the maximum number of taxable connections is 3000, and assuming that each CDR requires approximately 150 bytes of storage, the switch must set aside 900 kilobytes of memory for temporary storage. This figure is arrived at using the following calculation:

$$\begin{aligned}
 &\text{Memory needed for temporary storage of CDRs} \\
 &= (2 \text{ CDRs/taxable connection}) \times (3000 \text{ taxable connections}) \times (150 \text{ bytes/CDR}) \\
 &= 900,000 \text{ bytes} \\
 &= 900 \text{ KB}
 \end{aligned}$$

Congestion Strategy

To deal with the problem of congestion, when the switch may no longer have enough memory to store additional CDRs, the accounting function uses the following strategy:

- It establishes threshold levels for temporary storage of CDRs.
- It allows you to set the congestion strategy to “Accept Calls” or “Refuse Calls.”

Establishing Threshold Levels for Temporary Storage

After the switch allocates the amount of memory needed for temporary storage of CDRs, it establishes three threshold levels for this storage area. These threshold levels are defined as follows and illustrated in the figure below:

$$0 \leq \text{threshold 1} \leq \text{threshold 2} \leq \text{threshold 3} \leq 100\%$$



Threshold Levels Defined for Temporary Storage

The default values for threshold 1, 2, and 3, are 30%, 60%, and 90%, respectively. You can modify these threshold values as needed.

Threshold 1. Defines a warning level. Under normal operating conditions, temporary storage should not fill above Threshold 1.

Threshold 2. Defines a transport error level. If temporary storage fills above Threshold 2, the switch takes action to correct a suspected transport problem. The switch will close the current TCP connection and open a new one directed towards the alternate collection device, provided that an alternate collection device has been configured.

Threshold 3. Defines a congestion level. If temporary storage fills above Threshold 3, the switch takes action based on the congestion strategy (“Accept Calls” or “Refuse Calls”) which you have configured. See the discussion below.

Accept Calls, Refuse Calls

During periods of congestion, when temporary storage exceeds threshold level 3, the switch may or may not accept new connections, depending on how you have configured the congestion strategy.

If you have set the congestion strategy to “Refuse Calls,” the switch will refuse any new SVC connections. However, as soon as temporary storage returns to its “normal” range, that is, as soon as it returns to below threshold level 1, the switch will resume accepting new connections.

If the congestion strategy is set to “Accept Calls,” the switch will accept new connections, and CDRs will continue to be taken into temporary storage until such time when storage becomes completely filled. At that point, new connections will continue to be accepted, but CDRs will not be generated.

Traps

If the switch detects that a certain threshold level has been exceeded, it will generate a trap to signal this event. The switch will also generate a trap when it detects that temporary storage is lowering below a threshold level, to indicate that a problem is being corrected.

CDR Parameters

The table below provides a description of each of the fields that appears in a CDR.

CDR Parameter Descriptions

Parameter	Description
CDR sequence number	The number of the CDR. This number increments with each new CDR.
ATM identifier	Port and slot number of the ATM interface. (Currently not implemented.)
Node identifier	The IP address of the switch that generated this CDR.
Start time	The beginning of the time period covered by this CDR.
Duration	The length of time covered by this CDR, in seconds.
Equipment identifier	A means of identifying the switch that generated the CDR. (The switch identifier is provided by the manufacturer.)
CDR version	The version of this CDR.
CDR length	Currently, all CDRs are 140 bytes.
CDR possibly duplicated	Indicates whether a CDR may be a duplicate. This can occur when the switch does not receive an acknowledgement for the CDR it has sent. As a result, the switch sends the same CDR a second time. Possible values are Yes and No . <i>Yes</i> means that this is the second the time the CDR has been sent. <i>No</i> means that the CDR was sent only once and should therefore not be a duplicate.
CDR type	The type of CDR. Possible values are Terminated and Intermediate . For more information on Terminated and Intermediate CDRs, refer to <i>Terminated CDRs and Intermediate CDRs</i> on page 44-5.
CDR location	The port where the CDR is generated. Possible values are Ingress , Egress , and Transit . <i>Ingress port</i> is the port where a VC enters the switch. <i>Egress port</i> is where the VC leaves the switch. <i>Transit</i> means that the VC does not begin or end at this switch.
Connection type	The type of virtual connection. Possible values are PVC , Soft PVC , and SVC .

continued on next page

CDR Parameter Descriptions (continued)

Parameter	Description
Connection typology	The type of connection topology. Possible values are ptop (point-to-point) and ptomp (point-to-multipoint).
PVC/endpoint identifier	An internal identifier used by the accounting software to differentiate leaves CDR from point-to-multipoint connection.
Local slot number	In the switch, the slot number of the module that contains the ingress port through which the VC (Virtual Circuit) passes.
Local port number	The ingress port number through which the VC passes.
Local VPI	The virtual path identifier on the ingress side of the VC.
Local VCI	The virtual channel identifier on the ingress side of the VC.
Remote slot number	In the switch, the slot number of the module that contains the egress port through which the VC (Virtual Circuit) passes.
Remote port number	The egress port number through which the VC passes.
Remote VPI	The virtual path identifier on the egress side of the VC.
Remote VCI	The virtual channel identifier on the egress side of the VC.
Calling party number	The ATM address of the origination side of the VC.
Called party number	The ATM address of the destination side of the VC.
Calling numbering plan	Possible values are E.164 and NSAP .
Calling address length	The number of hexadecimal digits in the calling number.
Called numbering plan	Possible values are E.164 and NSAP .
Called address length	The number of hexadecimal digits in the called number.
I/F type	The type of ATM interface. Possible values are Pub UNI , Priv UNI , PNNI , IISP User , and IISP Netw .
Release clearing cause	The ATM release clearing cause code.
Release clearing diagnostic	The ATM release clearing diagnostic code.

continued on next page

CDR Parameter Descriptions (continued)

Parameter	Description
U2N ATM traffic descriptor	<p>The traffic descriptor defined for a connection in the direction of User-to-Network. Possible values are:</p> <ul style="list-style-type: none"> • None • NoCLPNoSCR • CLPNoTagNoSCR • CLPTagNoSCR • NoCLPSCR • CLPNoTagSCR • CLPTagSCR <p>For a description of each of the ATM traffic descriptor types, refer to the chapter “Managing Cell Switching Modules” in your switch manual.</p>
U2N param 1	<p>If the U2N ATM traffic descriptor is None, then U2N param 1 is not applicable.</p> <p>If the U2N ATM traffic descriptor is any other value, then the U2N param 1 value is the PCR (Peak Cell Rate) for CLP0 and CLP1 cells.</p>
U2N param 2	<p>If the U2N ATM traffic descriptor is (a) None or (b) NoCLPNoSCR, then U2N param 2 is not applicable.</p> <p>If the U2N ATM traffic descriptor is (a) CLPNoTagNoSCR or (b) CLPTagNoSCR, then the U2N param 2 value is the PCR (Peak Cell Rate) for CLP0 cells.</p> <p>If the U2N ATM traffic descriptor is NoCLPSCR, then the U2N param 2 value is the SCR (Sustained Cell Rate) for CLP0 and CLP1 cells.</p> <p>If the U2N ATM traffic descriptor is (a) CLPNoTagSCR or (b) CLPTagSCR, then the U2N param 2 value is the SCR (Sustained Cell Rate) for CLP0 cells.</p>
U2N param 3	<p>If the U2N ATM traffic descriptor is (a) None, (b) NoCLPNoSCR, (c) CLPNoTagNoSCR, or (d) CLPTagNoSCR, then U2N param 3 is not applicable.</p> <p>If the U2N ATM traffic descriptor is NoCLPSCR, then the U2N param 3 value is the MBS (Maximum Burst Size) for CLP0 and CLP1 cells.</p> <p>If the U2N ATM traffic descriptor is (a) CLPNoTagSCR or (b) CLPTagSCR, then the U2N param 3 value is the MBS (Maximum Burst Size) for CLP0 cells.</p>

continued on next page

CDR Parameter Descriptions (continued)

Parameter	Description
U2N best effort	Possible values are Yes and No . <i>Yes</i> indicates that UBR (Unspecified Bit Rate) is defined for User-to-Network. <i>No</i> indicates that UBR is not defined for User-to-Network.
U2N tagging option	Indicates whether tagging is enabled or disabled for this User-to-Network direction. Tagging is a function of the traffic descriptor used. For more information on tagging, refer to the chapter “Managing Cell Switching Modules” in your switch manual.
U2N packet discard for AAL5	The type of packet discard used for User-to-Network AAL5 PDU cells. The possible values are: <ul style="list-style-type: none"> • None (no packet discard) • EPD (early packet discard) • PPD (partial packet discard) • RED (random early discard)
U2N QoS class	The User-to-Network QoS (Quality of Service) class used. Possible values are: <ul style="list-style-type: none"> • UBR (Unspecified Bit Rate) • CBR (Constant Bit Rate) • rt-VBR (Real-Time Variable Bit Rate) • nrt-VBR (Non-Real-Time Variable Bit Rate) • ABR (Available Bit Rate)
N2U ATM traffic descriptor	The traffic descriptor defined for a connection in the direction of Network-to-User. Possible values are: <ul style="list-style-type: none"> • None • NoCLPNoSCR • CLPNoTagNoSCR • CLPNoTagNoSCR • NoCLPSCR • CLPNoTagSCR • CLPNoTagSCR For a description of each of the ATM traffic descriptor types, refer to the chapter “Managing Cell Switching Modules” in your switch manual.

continued on next page

CDR Parameter Descriptions (continued)

Parameter	Description
N2U param 1	<p>If the N2N ATM traffic descriptor is None, then N2U param 1 is not applicable.</p> <p>If the N2N ATM traffic descriptor is any other value, then the N2N param 1 value is the PCR (Peak Cell Rate) for CLP0 and CLP1 cells.</p>
N2U param 2	<p>If the N2N ATM traffic descriptor is (a) None or (b) NoCLPNoSCR, then N2U param 2 is not applicable.</p> <p>If the N2N ATM traffic descriptor is (a) CLPNoTagNoSCR or (b) CLPTagNoSCR, then the N2N param 2 value is the PCR (Peak Cell Rate) for CLP0 cells.</p> <p>If the N2N ATM traffic descriptor is NoCLPSCR, then the N2N param 2 value is the SCR (Sustained Cell Rate) for CLP0 and CLP1 cells.</p> <p>If the N2N ATM traffic descriptor is (a) CLPNoTagSCR or (b) CLPTagSCR, then the N2N param 2 value is the SCR (Sustained Cell Rate) for CLP0 cells.</p>
N2U param 3	<p>If the N2N ATM traffic descriptor is (a) None, (b) NoCLPNoSCR, (c) CLPNoTagNoSCR, or (d) CLPTagNoSCR, then N2U param 3 is not applicable.</p> <p>If the N2N ATM traffic descriptor is NoCLPSCR, then the N2N param 3 value is the MBS (Maximum Burst Size) for CLP0 and CLP1 cells.</p> <p>If the N2N ATM traffic descriptor is (a) CLPNoTagSCR or (b) CLPTagSCR, then the N2N param 3 value is the MBS (Maximum Burst Size) for CLP0 cells.</p>
N2U best effort	<p>Possible values are Yes and No.</p> <p><i>Yes</i> indicates that UBR (Unspecified Bit Rate) is defined for Network-to-User. <i>No</i> indicates that UBR is not defined for Network-to-User.</p>
N2U tagging option	<p>Indicates whether tagging is enabled or disabled for this Network-to-User direction. Tagging is a function of the traffic descriptor used. For more information on tagging, refer to the chapter “Managing Cell Switching Modules” in your switch manual.</p>

continued on next page

CDR Parameter Descriptions (continued)

Parameter	Description
N2U packet discard for AAL5	<p>The type of packet discard used for Network-to-User AAL5 PDU cells. The possible values are:</p> <ul style="list-style-type: none"> • None (no packet discard) • EPD (early packet discard) • PPD (partial packet discard) • RED (random early discard)
N2U QoS class	<p>The Network-to-User QoS (Quality of Service) class used.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • UBR (Unspecified Bit Rate) • CBR (Constant Bit Rate) • rt-VBR (Real-Time Variable Bit Rate) • nrt-VBR (Non-Real-Time Variable Bit Rate) • ABR (Available Bit Rate)
Cells discarded by UPC/NPC	<p>The number of cells discarded by UPC/NPC (Usage Parameter Control/Network Parameter Control) because the traffic did not correspond to the traffic descriptor being used.</p>
Cells tagged by the network	<p>The number of cells tagged by the network due to congestion. When a cell is tagged, it means that its CLP bit has been changed from "0" (high priority) to "1" (low priority). A low-priority cell is more likely to be discarded.</p>
Ingress CLP0+1 cells	<p>The total number of cells received on this VC.</p>
Egress CLP0+1 cells	<p>The total number of cells received and forwarded on this VC.</p>

Enabling the Accounting Function

By default, the accounting function is disabled. Therefore, to make use of this function, you must first enable it, specifically at the node, or switch, level.

Note

Enabling accounting at the node, or switch, level requires an MPM restart. See also *Software Requirements* on page 44-20 for configuring ATM accounting using the CLI.

Accounting can be enabled at any of three different levels:

- node (or switch) level
- port level
- PVC or Soft PVC level.

Depending on how these parameters are configured, the switch will or will not generate a CDR for a given SVC, PVC, or Soft PVC.

The possible enabled/disabled combinations and their corresponding CDR-generation behaviors are summarized in the table below. Note that The PVC/Soft PVC column does not apply to SVCs, therefore SVC-related cells are grayed out. SVCs can only be enabled at the node (or switch) level, or the port level.

Enabling and Disabling Accounting at the Node, Port, and PVC/Soft PVC Level

Node/Switch Level	Port Level	PVC/Soft PVC Level	CDR Behavior for SVC, PVC, and Soft PVC
Disabled (default)	Either enabled or disabled	Either enabled or disabled	CDRs will <i>not</i> be generated in the switch at all.
Enabled	Disabled (default)		CDRs will not be generated for an SVC on this port.
Enabled	Disabled	• Enabled	• CDRs will be generated for this PVC or Soft PVC.
		• Disabled	• CDRs will <i>not</i> be generated for this PVC or Soft PVC.
		• UsePortValue (default)	• CDRs will <i>not</i> be generated for this PVC or Soft PVC.
Enabled	Enabled		CDRs will be generated for an SVC on this port.
Enabled	Enabled	• Enabled	• CDRs will be generated for this PVC or Soft PVC.
		• Disabled	• CDRs will <i>not</i> be generated for this PVC or Soft PVC.
		• UsePortValue (default)	• CDRs will be generated for this PVC or Soft PVC.

In the above table, the parameter setting “UsePortValue” instructs the switch to use whatever value has been set at the port level. UsePortValue enables or disables accounting for all PVCs and Soft PVCs on a given port simultaneously. This parameter value eliminates the need to configure each connection individually.

If accounting is *disabled* at the node level, it makes no difference how it is configured at the port level or PVC/Soft PVC level. It will always result in accounting being disabled, and CDRs *not* being generated.

If accounting is *enabled* at the node level, it does matter how port level and PVC/Soft PVC level are configured. The value for PVC/Soft PVC level takes precedence over the value for port level.

The default values for each of the different levels at which accounting can be enabled or disabled are as follows:

- Node/Switch-level - *Disabled*
- Port-level - *Disabled*
- PVC/Soft PVC level - *UsePortValue*

Use the table above (“Enabling and Disabling Accounting at the Node, Port, and PVC/Soft PVC Level”) to determine at which level you should enable or disable accounting, depending on whether you do, or do not, want CDR generation to occur.

Keep in mind, if you want CDR generation to occur at the port and/or PVC/Soft PVC level, not only do you have to enable accounting on these individual levels, you must also enable accounting at the node or switch level. If accounting is disabled at the switch level, CDRs will not be generated at the port or PVC/Soft PVC level, regardless of having enabled them at those levels.

Using the CLI to Configure ATM Call Accounting

The CLI is a form of text-based configuration in which you connect to an active switch, then manually enter single-line, CLI configuration commands. You can enter these commands using one of two methods:

- (a) **On-Line Configuration**, entering commands at the CLI prompt.
- (b) **Off-Line Configuration**, entering commands in a standalone text editor, such as Microsoft Word, WordPad, or NotePad.

When Off-Line Configuration is used, the resulting configuration file is placed in the switch's **/flash** or **/simm** directory, and changes are applied to the switch by issuing a **configuration** command.

Off-Line Configuration is useful in that a configuration file can be viewed or edited offline at any time, then uploaded and applied to additional switches in the network. This makes it easy for users to clone switch configurations. Also, the ability to store comprehensive network information in a single file facilitates troubleshooting, testing, and overall understanding of the network configuration.

For information on using the CLI, along with a list of all the ATM accounting commands, refer to chapter titled "ATM Accounting Commands" in the *Text-Based Configuration* manual.

Software Requirements

Before you can use the CLI to configure ATM accounting, you must have the following software installed:

1. The switch must be running Software Release 4.1x or later.
2. The **text_cfg.img** file must be loaded into your switch's flash file system.
3. The **acct.img** file must be loaded into your switch's flash file system.

Items (1) and (2) are requirements for using the Text-Based Configuration feature. Item (3) is a requirement of the ATM Accounting function.

For information on how to use FTP or ZMODEM to load files onto the switch, refer to the chapter "Installing Switch Software," located in your switch manual.

CLI Conventions

The ATM accounting commands are documented using the following CLI syntax conventions:

CLI Conventions

boldface	Indicates a CLI command. Example: accounting memory
<i>italicized text</i>	Indicates variable information entered by the user. Example: IP addresses, port numbers, etc.
< > (Brackets)	Indicate <i>required</i> command parameters. Example: accounting memory <pdest>. Here the user must enter a value for the parameter <i>pdest</i> .
[] (Straight Brackets)	Indicate <i>optional</i> command parameters. Commands themselves may have bracketed portions, indicating that the command can be entered in an abbreviated form and still be recognized by the system.
{ } (Curly Braces)	Indicate that the user must choose between one or more parameters. Example: congestion strategy {accept call refuse call}
(Vertical Line)	Used to separate parameter choices within a command string. See example for “curly braces.”

Global Definitions

The CLI accounting commands also use certain global definitions.

Global Definitions

port_id	slot/port A port identifier is defined by slot and port number, separated from each other by a slash (/). Example: 5/3
port_list	<i>slot/port1 [-port2, [, [slot2/port1 [-port2] ,...]]]</i> A port list consists of one or more port IDs. A hyphen is used to indicate a range of consecutively-numbered ports on the same slot. A comma is used to separate distinct port IDs. Examples: 3/1 3/4-8 3/3, 3/6, 4/1, 5/8-12

Configuration Examples

This section offers examples on how to configure ATM Accounting using the CLI. Examples provided in this section are grouped as follows:

- Node-Level Configuration
- Port-Level Configuration
- PVC- and Soft PVC-Level Configuration
- Collection Interval and Tariff Periods
- Configuration Queries

Each example begins with a statement of the full CLI command, along with all its optional parameters. However, only certain of these optional parameters are illustrated. For a detailed explanation of each of the parameters, refer to chapter titled “ATM Accounting Commands” in the *Text-Based Configuration* manual.

Node-Level Configuration

Enabling Accounting at the Node Level

```
accounting memory < pdest > [ sdest ] [ max [ connection ] max_cnx ] [ port TCPport ]  
[ threshold threshold1 [ threshold2 ] [ threshold3 ] ] [ hold [ timer ] hold_timer ]
```

By default, the accounting function is disabled. To make use of this function, you must first enable it.

Note

This command requires an MPM restart in order to take effect. Be aware that, at restart, accounting will be disabled by default on all ports.

As an example, enable accounting at the node (or switch) level, specify both a primary and secondary collection device, and accept the default configuration settings for maximum number of connections, TCP port, threshold levels, and hold timer duration. At the CLI prompt, enter the following command:

```
accounting memory 172.23.8.0. 172.23.8.41 default
```

The **accounting memory** command requires an MPM restart in order to take effect. This can be accomplished either by manually resetting the switch, or by using the **reboot** command. To use the **reboot** command, first end your CLI session by typing **exit** at the CLI prompt. When the switch’s UI prompt (*l%*) appears, type **reboot**. When asked to confirm your request, indicate (**y**)es.

```
-> -> exit  
l% reboot  
Confirm? (n) : y
```

Upon executing the **reboot** command, you will lose connection to the switch and will need to reconnect. After restoring the switch connection, use the **accounting dump** command to confirm that the IP addresses you just configured actually took effect. This command can be issued for **node**, **port**, **pvc**, or **all**. When either the **node**, **port**, or **pvc** option is used, only node, port, or pvc parameters are displayed. When the **all** option is used, node, port, *and* pvc parameters are displayed. A screen similar to the following displays when you enter the command **accounting dump node**.

```
-> accounting dump node
! Node configuration for accounting
accounting memory 172.23.8.0 172.23.8.41 max connection 3000, port 2804, threshold 30 60 90,
hold timer 120
accounting congestion strategy accept call, tcp timer 2
accounting interval 1
accounting period 12:0
```

->

To verify that these are the default values for maximum connections, TCP port, threshold levels, and hold time duration, refer to the parameter descriptions in chapter titled “ATM Accounting Commands” of the *Text-Based Configuration* manual.

As an additional configuration exercise, try reconfiguring two of the accounting parameters. Set the maximum connections to 3200 and the hold timer duration to 100 ms. At the CLI prompt, enter the following command:

```
-> accounting memory 172.23.8.0. 172.23.8.41 max 3200 hold 100
```

To make this command take effect, reset the switch or use the **reboot** command.

Disabling Accounting

```
accounting no node
```

To disable accounting at the node (or switch) level, enter the following command:

-> **accounting no node**

This command takes effect immediately.

Forcing a Switchover to the Alternate Collection Device

```
accounting switch
```

During periods of congestion, or in the event of a problem with the TCP connection, you may want to force a switchover to the alternate collection device (provided that you previously configured an alternate collection device). To force a switchover, enter the following command:

-> **accounting switch**

This command takes effect immediately.

Collecting CDRs From All Established Connections

```
accounting collect
```

Rather than waiting for a regularly scheduled and automatic CDR collection to occur, you can instead do a manual collect. The following are two example scenarios.

1. Assume that, for whatever reason, it is necessary for you to reset the switch. Prior to resetting the switch, it will be useful to do a manual collect, because once the switch is reset, CDR information will be lost and will not be recoverable.
2. You may have a need to collect statistics on CDRs from all established connections as of a particular time of day. A manual collect would be an appropriate action.

To manually collect CDRs from all established connections, enter the following command:

-> **accounting collect**

This command takes effect immediately.

Defining a Congestion Strategy

```
accounting { [congestion [strategy] { accept [call] | refuse [call] } ] [tcp [timer] tcp_write_timer]
| default }
```

Developing a congestion strategy at the node level involves specifying how SVC calls are handled during periods of congestion. This includes specifying whether the switch “accepts” or “refuses” SVC calls, and, optionally, indicating the interval at which completed CDRs are sent over the TCP connection to the collection device. For detailed information on how calls are handled when the congestion strategy is set to “Accept” or to “Refuse,” refer to the section in this chapter called *Accept Calls, Refuse Calls* on page 44-11.

To define a congestion strategy set to accept calls, and a TCP timer interval of 100 milliseconds, enter the following command

-> **accounting congestion accept tcp 1**

◆ Note ◆

When entering the **tcp timer** command, the tcp interval of 100 milliseconds is represented by the value 1.

This command takes effect immediately.

Port-Level Configuration

Enabling Accounting at the Port Level and Defining Its Congestion Strategy

```
accounting port { port_list | all } { accept [call] | refuse [call] }
```

To enable accounting at the **port** level, and to define its congestion strategy as **refuse calls**, enter the following command, substituting an appropriate slot and port ID:

```
accounting port 3/1 refuse
```

Port-level accounting and its associated congestion strategy can be enabled for either a specified list of ATM interfaces or for all ports.

This command takes effect immediately.

Disabling Accounting

```
accounting no port { port_list | all }
```

To disable accounting at the port level, enter the following command:

```
accounting no port all
```

Port-level accounting can be disabled for either a specified list of ATM interfaces or for all ports.

This command takes effect immediately.

PVC- and Soft PVC-Level Configuration

Enabling Accounting at the PVC and Soft PVC Level

```
accounting pvc < port_id vpi > [ vci ] { ON | PORT }
```

To enable accounting at the PVC and Soft PVC level, enter the following command, substituting an appropriate port ID, VPI, and VCI:

```
accounting pvc 3/7 100 16 ON
```

Use the **ON** option to enable accounting at the PVC/Soft PVC level.

Use the **PORT** option to enable PVC/Soft PVC level accounting at whatever value (ON or OFF) was set for the port.

To make this command take effect, reset the switch or use the **reboot** command. For information on how to use the **reboot** command, refer to *Node-Level Configuration* on page 44-22.

Disabling Accounting at the PVC and Soft PVC Level

```
accounting no pvc < port_id vpi > [ vci ]
```

To disable accounting at the PVC and Soft PVC level, enter the following command, substituting an appropriate port ID, VPI, and VCI:

```
accounting no pvc 3/7 100 16
```

To make this command take effect, reset the switch or use the **reboot** command.

Collection Interval and Tariff Periods

Define a Collection Interval

```
accounting interval { { 1 | 2 | 3 | 12 } | default }
```

A collection interval is a regular interval of time, at the end of which a CDR is generated. You may configure only one collection interval. The permitted values are: 1, 2, 3, or 12 hours. The default collection interval is 3 hours.

To define a collection interval with a value of 2 hours, enter the following command:

```
accounting interval 2
```

For detailed information on how accounting intervals are computed, refer to the section in this chapter called *How Periodic Collection is Computed* on page 44-6.

Define a Tariff Period

```
accounting period { p1 [ p2 [ p3 [ p4 [ p5 [ p6 [ p7 [ p8 ] ] ] ] ] ] ] | default }
```

A tariff period is a specific time at which a rate change occurs. You may configure up to 8 tariff periods in a single day. A tariff period represents a specific time of day, whereas a collection interval spans a duration of time.

A tariff period must be a multiple of 15 minutes and no less than 1 hour. For example, a tariff period can be set for 4:00 pm, 5:00 pm, 6:15 pm, and 7:45 pm. Each configured tariff period is a multiple of 15 minutes and the interval between tariff periods is at least one hour. In reality, however, tariff periods would never change with that frequency.

Tariff periods are specified using the 24-hour format. They should be entered as hours and minutes (hh:mm) or, if the tariff period begins precisely on the hour, entered in hours (hh) only. Tariff periods must be entered in chronological order.

The default is 00:00, indicating that no tariff period is defined.

To define tariff periods, enter the following command, substituting appropriate hours and minutes for each tariff period to be configured, and entering a space between each successive tariff period:

```
accounting period 09 15 17 21:45
```

In this example, tariff periods have been configured for 09:00 (9 am), 15:00 (3 pm), 17:00 (5 pm), and 21:45 (9:45 pm).

Configuration Queries

```
accounting dump { all | node | port | pvc }
```

To display the configuration parameters currently in use at the node, port, and pvc level, enter the following command:

```
accounting dump all
```

The **accounting dump** command can be issued for **node**, **port**, **pvc**, or **all**. When the **node**, **port**, or **pvc** option is used, only node, port, or pvc parameters are displayed. When the **all** option is used, node, port, *and* pvc parameters are displayed. In the sample screen display which follows, note that the parameters are listed as a set of CLI configuration commands.

```
-> accounting dump all
! Node configuration for accounting
accounting memory 143.209.113.64 172.22.2.137 max connection 3000, port 2804,
threshold 30 60 90, hold timer 120
accounting congestion strategy refuse call, tcp timer 2
accounting interval 1
! ATM ports configuration for accounting
accounting port 3/1 accept call
accounting port 6/5 accept call
accounting port 7/2 accept call
accounting port 8/2 accept call
! ATM PVC configuration for accounting
accounting pvc 7/1 1 ON
```


Selecting Clocking Sources

The flexibility designed into the OmniSwitch allows it to implement a variety of possible reference clocking schemes. The design also provides for alternate clocking sources in the event of a primary source failure.

You configure clocking at two levels, port level and bus level. Port-level configuration specifies the source of the transmit clock driving the port. Bus-level clock configuration specifies the clock source to the backplane of the system.

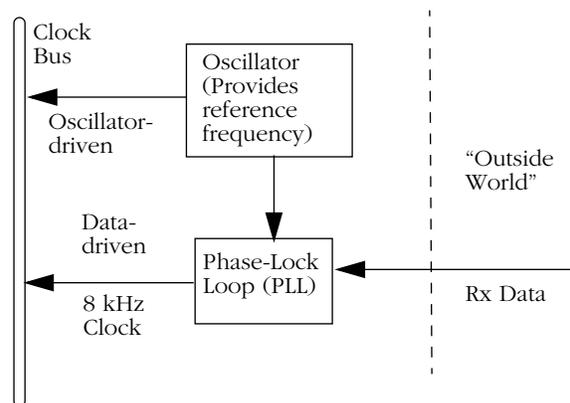
Configuring Transmit Clocking (Port-Level Clocking)

In port-level clocking, you are specifying a clock source for the port to “use” (i.e., drive its transmit data). All ports on all modules use either 8 kHz or 19.44 MHz reference timing. A different clock source can be specified for every port in the system.

When the clock comes from the receive data, the term “derive” means that the clocking signal is separated from the receive data by a Phase-Lock Loop, then sent to a bus on the backplane. When the clock comes from an onboard oscillator, the oscillator provides clocking directly to the bus.

Modules can derive reference timing from either:

- the receive data stream (data-driven clocking)
- in some cases, from an onboard oscillator (oscillator-driven clocking)
- an optionally-installed Stratum 3 hardware clocking module.



Modules that Require 8 kHz Timing

The following types of modules use an 8 kHz clock for driving their data:

- E1/T1
- DS1
- E3
- ATM-25
- CE-E1/T1
- IMA-DS1/E1

Modules that use an 8 kHz clock can derive their timing from:

- The locally-generated clock from the 19.44 MHz onboard oscillator on the CSM module (divided down to 8 kHz by the PLL module),
- The receive data, or
- The optionally-installed X-Cell Clocking Module (CSM-AB-CM; for more information on this module, see Chapter 40, “Cell Switching Modules (CSMs).”)

Modules that Require 19.44 MHz Timing

The following types of modules use a 19.44 MHz clock for driving their data:

- OC3
- OC12
- CE-E1/T1

Modules that use a 19.44 MHz clock can derive their timing from:

- The locally-generated clock from the 19.44 MHz onboard oscillator on the CSM module,
- The receive data, or
- The optionally-installed X-Cell Clocking Module (CSM-AB-CM)

Timing Considerations for DS3/E3 and PLCP

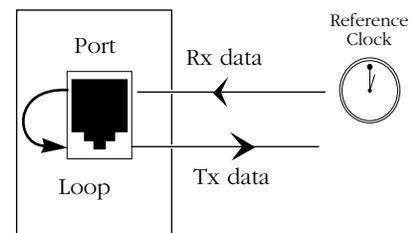
The DS3/E3 data format may be managed by the Physical Layer Convergence Protocol (PLCP), which incorporates its own clocking information. While PLCP is an optional method for providing clocking, it is required for data requiring synchronization of clocking. PLCP provides services to map the ATM cells into the DS3 frame structure. Timing data for an 8 kHz clock is encoded into the PLCP data, and is derived independently from the carrier frequency. The DS3 and E3 modules are capable of utilizing this timing data for both source clocking of receive data to the bus and as a reference clock for transmit data at 8 kHz.

Timing Modes

Two transmit timing mode options are available: loop timing and local timing. For details on setting the timing mode, see *Configuring Clocking* on page 45-10.

Loop Timing

Loop timing is typically implemented with public network connections. In loop timing, the reference clock is derived from the receive data, then fed back out with the transmit data.



Local Timing

For local timing mode, you set which source a port is to use to drive its transmit data. The options are:

- The local oscillator. Using the local oscillator (located on the CSM module) will provide the backplane with a Stratum 4-level clock.
- The bus (backplane). You can select either the 8 kHz or 19 MHz bus, depending upon the port type. Select this option if you are planning to provide a single reference clock across the network.
- The optionally-installed X-Cell Clocking Module (CSM-AB-CM). This module provides a Stratum 3-level clock to the 8 kHz and 19.44 MHz buses.

Bus-Level Clocking

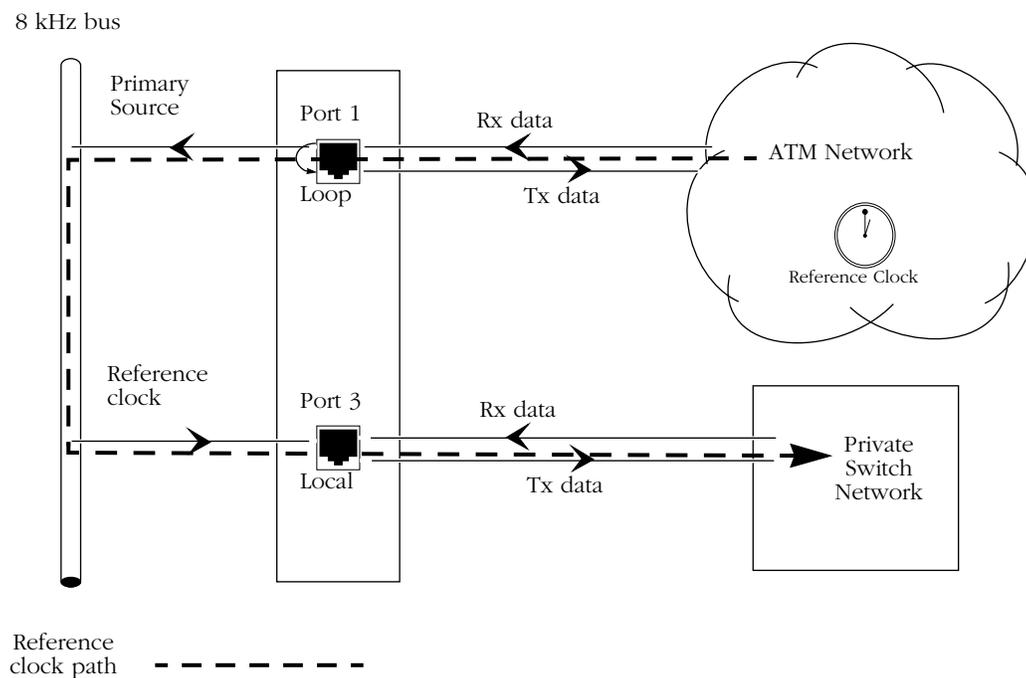
In bus-level clocking, you are specifying whether the clock that drives the bus on the backplane comes from a source within the switch, or from an external source. Some examples of external sources are:

- Commercial ATM services
- Public network T1 lines
- PBXs
- Other switching modules

Bus Lines

There are two clocking lines on the backplane; an 8 kHz clock and a 19.44 MHz clock.

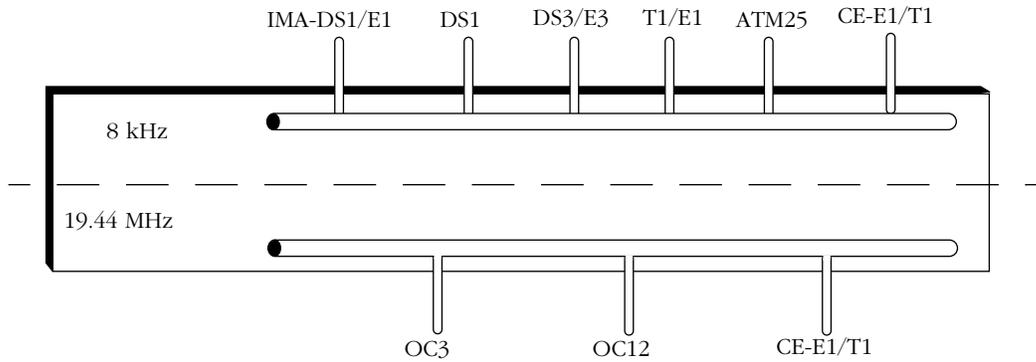
The following illustration shows an example of ports on a switch deriving their timing from a commercial ATM provider via loop timing, then passing that reference clock on through another port to synchronize a private network (local timing).



Synchronizing a Private Network Through Derived Timing

Clocking Summary

The following figure is a representation of the backplane clock sources and the CSM modules they support.



Backplane Clock Sources

The following tables summarize the port types and their reference clocking options:

In this table, the oscillator associated with the port is driving the bus.

Board	Line Clock (MBPS)	Rx Data Recovered (8 kHz)	Rx PLCP (8 kHz)	8 kHz Oscillator	Rx Data Recovered (19.44 MHz)	19.44 MHz Oscillator
OC12-2	622	Y	N/A	N	Y	Y
OC3-2, -8	155	Y	N/A	N	Y	Y
DS3-2	45	Y	Y	Y	N	Y
E3-2	34	Y	Y	Y	N	Y
DS1-4	1.544	Y	N/A	Y	N	Y
E1-4	2.048	Y	N/A	Y	N	Y
ATM25-12, -24	25.6	Y	N/A	N	N	N
CE-T1/E1	1.544/2.048	Y	N/A	N	Y	Y
IMA-DS1-8	1.544	Y	N/A	Y	N	Y
IMA-E1-8	2.048	Y	N/A	Y	N	Y

Selecting Clocking Sources

This table lists which buses can drive the ports associated with the particular board.

Board	Line Clock (MBPS)	Tx Regenerated Line Clock from 8 kHz	Tx PLCP 8 kHz from 8 kHz	Tx Regenerated Line Clock 19.44 MHz)	Tx PLCP 8 kHz from 19.44 MHz
OC12-2	622	N	N/A	Y	N/A
OC3-2, -8	155	N	N/A	Y	N/A
DS3-2	45	N	Y	N	N
E3-2	34	N	Y	N	N
DS1-4	1.544	Y	N/A	N	N/A
E1-4	2.048	Y	N/A	N	N/A
CE-T1-4	1.544	Y	N/A	Y	N/A
CE-E1-4		Y	N/A	Y	N/A
ATM25-12, -24	25.6	Y	N/A	N	N/A
IMA-DS1-8	1.544	Y	N/A	N	N/A
IMA-E1-8	2.048	Y	N/A	N	N/A

Viewing/Configuring Clocking

The following commands are the commands to configure clocking and to view the clocking configuration. They are listed in the **Interface/ATM** menu.

- Use the **vap** command to view configuration information for all CSM ports, including the current clocking status. This command provides information on the timing mode and source for each port. (See *Viewing ATM Port Configurations* in Chapter 41 “Managing Cell Switching Modules (CSMs).”)
- Use the **map** command to set the timing mode (either loop or local) for ATM ports only. (See *Modifying the Transmit Clocking Source* on page 45-12.)
- Use the **vclk** command to view clocking status for configured CSM ports only. (See *Viewing Configured Ports* on page 45-8.)
- Use the **vclka** command to view clocking information on all CSM ports. (See *Viewing Clocking on All Ports* on page 45-9.)
- Use the **mclk** command to alter clock configuration settings for CSM ports. (See *Configuring Clocking* on page 45-10.)
- Use the **mcst** command to set the amount of time the backup clock source waits before it returns timing control back to the recovered primary clock source. (See *Modifying the Clock Switching Time (CSM Ports)* on page 45-11.)

Viewing the Clocking Configuration

Two commands, **vclk** and **vclka**, enable you to view the clocking sources of the buses at the backplane, as well as the clocking source for the port(s). The **vap** command enables you to view the configured transmit clocking source for the switch.

Viewing Configured Ports

The **vclk** command is listed in the Interface/ATM menu. It returns clocking information on only those CSM ports that have been configured as clock sources to the backplane.

To view all configured ports, type **vclk** at the prompt. The following screen is a sample a switch that has had only the primary clock source defined:

Clock Source				
Slot	Port	Timing Mode	Configured Source	Current Source
5	1	Local	19.44 MHz	19.44 MHz

Reference Source	Primary	Secondary	Tertiary	Current
8 kHz	5/1	None	None	Primary
19.44 MHz	4/1	None	None	Primary

Note that only port 5/1 is displayed. If secondary and tertiary ports had been defined as clocking sources, they, too, would have been displayed. The following information is displayed for the configured port(s):

Slot/Port. Indicates the CSM module and the port number for which statistical information is provided. Each row in the table gives information for a single CSM port.

Timing Mode. Can be set to either **Loop** or **Local**. If the port is set to **Loop**, it is deriving its clocking directly from the receive data, not from the bus. If the port is set to **Local**, it is deriving its clocking from the bus.

Configured Source. Refers to the bus from which the port is configured to be receiving its reference clock. Options are 8 kHz and 19.44 MHz.

Current Source. Refers to the bus from which the port is currently receiving its reference clock. Options are 8 kHz and 19.44 MHz.

Note

If Configured Source and Current Source are different, it is a probable indicator that the port's configured source has failed.

The second table shows what ports (if any) are configured as the primary, secondary, and tertiary reference clocks. The table also shows what level is currently active.

Viewing Clocking on All Ports

The **vclka** command is listed in the Interface/ATM menu. It returns information on the clocking source for all CSM ports on the system. The following screen is a sample of the output from the **vclka** command:

Clock Source				
Slot	Port	Timing Mode	Configured Source	Current Source
4	1	Local	Oscillator	Oscillator
4	2	Local	Oscillator	Oscillator
5	1	Local	19.44 MHz	19.44 MHz
5	2	Local	Oscillator	Oscillator
5	3	Local	Oscillator	Oscillator
5	4	Local	Oscillator	Oscillator
5	5	Local	Oscillator	Oscillator
5	6	Local	Oscillator	Oscillator
5	7	Local	Oscillator	Oscillator
5	8	Local	Oscillator	Oscillator

Reference Source	Primary	Secondary	Tertiary	Current
8 KHz	5/1	None	None	Primary
19.44 MHz	4/1	None	None	Primary

Field Descriptions

The following section describes the fields and their optional values.

Slot/Port. The slot within the chassis and the port on that module for which information will be displayed. This command displays information for a single port in one row.

Timing Mode. This field has two options: **Loop** and **Local**. **Loop**, means the port is deriving its clocking directly from the receive data. **Local**, means the port is deriving its clocking from the bus.

Configured Source. This field will indicate that the current source for the port is either its local oscillator (the default setting), or one of the buses.

Current Source. This field indicates that the configured source for the port is either its local oscillator (the default setting), or one of the buses.

Note

If Configured Source and Current Source are different, it is a probable indicator that the port's configured source has failed.

The second table provides a summary of what ports (if any) are providing the primary, secondary, and tertiary clock source to each of the bus lines at the backplane.

Configuring Clocking

The **mclk** command enables you to modify the clocking sources to the backplane. The **mcsk** command enables you to set the amount of delay before the backup clock source returns control to the recovered primary clocking source. The **map** command enables you to specify the transmit clocking source(s) for the switch.

Modifying the Clocking Configuration (CSM Ports)

To alter the clocking configuration settings for CSM ports, use the **mclk** command. **mclk** is listed in the Interface/ATM menu. To view the format and valid ranges for **mclk**, type the command without any parameters, then press **<return>**, as shown below:

```
mclk <return>
```

A screen similar to that shown below is displayed:

```
/Interface/atm% map 2/1

Usage: mclk bus level source
Valid ranges:
bus: 8k OR 19m for OC3 and OC12
      8k for DS3/E3, ATM25, T1E1, IMA, and T1E1-CE
level: p for Primary, s for Secondary, OR t for Tertiary
source: slot/port OR slot/port osc OR none
```

To modify a clocking configuration, enter the command in the following format:

```
mclk <bus> <backup level> <slot>/<port> (osc)
```

Field Descriptions

The following section describes the valid options to enter and their associated parameters.

bus: Enter the bus to which you want to provide the source clock. Available options are **8k** (for the 8kHz bus) and **19m** (for the 19.44 MHz bus). For OC3, OC12 or CE-E1/T1 ports, you can set the clock to either 8k or 19m. For all other port types, the clock must be set to 8k.

level: Set to **p** (primary), **s** (secondary), or **t** (tertiary). For more information on backup levels, see *Backup Design* on page 45-14.

Note

If you define a secondary clocking source without defining a primary source, the switch will automatically derive its clocking from the secondary source. Similarly, if you define a tertiary source only, the system will use that source.

source. The slot within the chassis and the port on that module that will drive the bus. Available options are: **<slot>/<port>**, **<slot>/<port> osc**, and **none**. Include the **osc** option if you want to specify the onboard oscillator as the clock source.

If you have the optional hardware clocking module installed in your switch, and you select the slot/port that corresponds to the module, its module's external T1/E1 port will drive the backplane. If you add the **osc** option, the module's onboard Stratum 3 clock will drive the backplane.

Select the **none** option if this port will not be used as a source of clocking. The **none** option may also be used to deconfigure a port that was previously configured as a source to the backplane.

Examples

For example, to specify slot 5, port 1 (5/1) as the primary (p) source to drive the 8 kHz bus (8k) at the backplane, enter:

```
mclk 8k p 5/1
```

In this example, slot 4 is occupied by a CSM. The following command specifies slot 4, port 1 (4/1) as the secondary (s) source to drive the 19 MHz bus (19m) at the backplane, and the onboard oscillator as the secondary (backup) clock source:

```
mclk 19m s 4/1 osc
```

For this example, the hardware clocking module is installed in slot/port 6/1. The following command specifies the clocking module as the primary source to drive bus 8k at the backplane, using the onboard Stratum 3 clock.

```
mclk 8k p 6/1 osc
```

Modifying the Clock Switching Time (CSM Ports)

The **mcst** command provides an additional configuration option for the clock module. The setting for this command comes into play in the event of the loss of the primary clocking source. Should the primary clocking source go down, then subsequently come up again, the switch will wait the specified amount of time (in seconds) before switching back from the backup clocking source to the restored primary clocking source. The purpose of this delay is to avoid having the switch repeatedly switching between the primary and backup clocking sources in the event of an unstable or unreliable primary clocking source.

This command is listed in the Interface/ATM menu. The only parameter that is set on the **mcst** command is the amount of switchover delay. This delay can be set anywhere in the range of 1 to 10000 seconds. The delay applies to the entire clocking system. The default value is 5 seconds.

To use the **mcst** command, enter **mcst**, followed by the amount of delay. For example, to set the switchover delay to 10 seconds, you would enter:

```
mcst 10
```

A screen similar to the following now displays, showing both the current configured clock sources and switchover time:

```

                Clock Source
                -----
                Timing   Configured   Current
                Slot Port Mode   Source       Source
                =====
                5      1   Local    19.44 MHz   19.44 MHz

Reference Source Primary Secondary Tertiary Current
=====
 8 kHz           5/1     None     None     Primary
19.44 MHz        4/1     None     None     Primary

Clock switching time (seconds)
=====
10
    
```

See *Viewing Clocking on All Ports* on page 45-9 for more information on the parameters displayed by the **mcst** command.

Modifying the Transmit Clocking Source

To modify the transmit clocking source, use the Timing Mode option (parameter 9) of the **map** command. The **map** command is listed in the Interface/ATM menu. The valid options for the Timing Mode option are **Loop (1)** and **Local (2)**.

If the Local option of the Timing Mode parameter is selected, a subparameter called Local Source (parameter 90) must be set. The valid options are **Osc (1)** (for the onboard oscillator, or in the case where the port corresponds to the optional hardware clocking module, the Stratum 3 clock), or **Bus (2)** (meaning the clock is derived from either the 8 kHz or 19.44 MHz backplane, depending upon the type of module being configured and its timing requirements).

To use the **map** command, enter **map**, followed by **<slot>/<port>**. For example, to modify the first port on slot two, enter:

```
map 2/1
```

A screen similar to the following displays:

```
/Interface/atm% map 2/1

Slot 2 Port 1 Configuration

1) Description (30 chars max)           : CSM PORT
2) ATM Address (40 hex-chars)         :
000000000000000000000000000000000000
3) Max VPI bits (1..12)                : 2
4) Max VCI bits (1..12)                : 10
5) I/F Type {Pub UNI (1), Pri UNI (2),
PNNI (3), IISP user (4), IISP netw (5): Private
6) Phy Protocol {SONET (1), SDH (2)}   : SONET
7) Signaling Ver {3.0 (1), 3.1 (2)}    : 3.0
8) ILM I Enable {False (1), True (2)}  : Enable
9) Timing Mode {Local (1), Loop (2)}   : Local
90) Local Source {Osc(1), Bus(2)}      : Bus
```

```
Enter (option=value/save/cancel) :
```

To set or change the Timing Mode for the selected port, enter 9={1/2}. ‘1’ sets the port to **Loop** timing; ‘2’ sets the port to **Local** timing. For example:

```
9= 1
```

Sets port 2/1 to Local timing. To save the new configuration, type **save**, then press **<Enter>**. For more detailed information on Local vs Loop timing, see *Configuring Transmit Clocking (Port-Level Clocking)* on page 45-2.

If you set the Timing Mode to Local, you must next set the subparameter called Local Source (subparameter 90). The options are **Osc (1)** and **Bus (2)**. **1** sets the port’s clocking source to the onboard oscillator, or to the Stratum 3 clock, if the port you selected corresponds to the hardware clocking module. **2** sets the clocking source to the bus (the system will automatically select either the 8 kHz or 19.44 MHz bus, as required by the port being configured).

See Chapter 41, “Managing Cell Switching Modules (CSMs), for more information on the **map** command.

Modifying the Transmit Clocking Source (T1/E1 Ports)

For most CSM modules, when the timing mode is set to **Local**, the software automatically selects the bus with the appropriate clock for that module (e.g., 8k for an ATM-25 port; 19M for an OC3 port). Since T1/E1 ports can be clocked off of either bus, T1/E1 ports are user-configurable for that option. Suboption 90, **Local Source**, provides three options: **Osc(1)**, **8KBus(2)**, and **19MBus (3)**. When you invoke the **map** command for a T1 or E1 port, a screen similar to that shown below is displayed:

```

/Interface/atm% map 2/1

Slot 2 Port 1 Configuration

1)   Description (30 chars max)           : CSM PORT
2)   ATM Address (40 hex-chars)          :
0000000000000000000000000000000000000000
3)   Max VPI bits (1..12)                 : 2
4)   Max VCI bits (1..12)                 : 9
9)   Timing Mode {Local (1), Loop (2) }    : Local
90)  Local Source {Osc(1), 8KBus(2)
      19MBus (3) }                         : 8KBus

```

Enter (option=value/save/cancel) :

If you set Timing Mode (Option 9) to the **Local** option, you must specify which Local Source you want to use: the onboard oscillator (**Osc(1)**), the 8 kHz bus (**8KBus(2)**), or the 19 MHz bus (**19MBus (3)**).

See Chapter 41, “Managing Cell Switching Modules (CSMs), for more information on the **map** command.

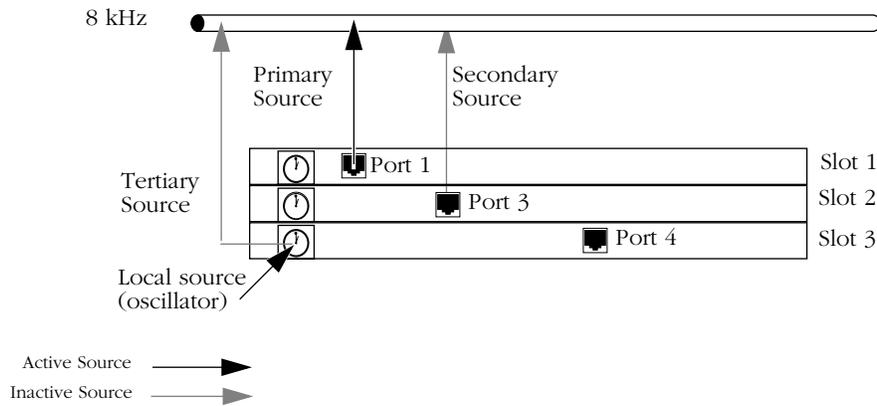
Clock Backup

The system software is capable of handling clock backup tasks when communication over a port fails in the system. To set backup levels for one or more ports, use the **mclk** command (see *Configuring Clocking* on page 45-10).

Backup Design

You can configure the system to provide up to three levels of clock backup in the event of port failure by configuring primary, secondary, and tertiary sources to the backplane reference source (8k or 19m). By default, the local oscillator drives the ports in the system. If the primary source fails, the system will automatically switch to the secondary source to drive the backplane. If the primary source should come back up, it will take over and drive the backplane. If both the primary and secondary sources fail, the system will switch to the tertiary backup (usually a local oscillator). If all three sources fail, the system will switch to a local oscillator for local timing. If any of the failed sources comes back up, the tertiary source hands the clock back to it. If no source is driving the backplane, the system will switch the ports to their local oscillator.

In the example below, Slot 1/Port 1 is configured as the primary source. It is driving the 8 kHz bus (8k) at the backplane. Slot2/Port 3 is configured as the backup to Primary Source, and is referred to as the secondary source. If the primary source should fail, the system will automatically switch to the secondary source, which will immediately begin driving bus 8k.



Sample Backup Configuration

If the secondary source should subsequently fail, and a tertiary source has been configured (in this example, the local oscillator on slot 3), the system would switch to the oscillator to drive the backplane. Thus, the onboard oscillator would become the tertiary source. If the tertiary source were not configured, the ports relying on the 8k clock bus as a reference source would be switched to their local onboard oscillators.

If at any time port 1 or 3 should come back up, it will resume its responsibility for driving bus 8k (after the configured Clock Switching Time (**mcst**) has elapsed).

46 Configuring and Monitoring PNNI

The Private Network-to-Network Interface (PNNI) is the routing protocol for building world-wide ATM networks. It uses a hierarchical structure to efficiently distribute information about ATM network topology (i.e., ATM nodes and links), compute routes that meet requested bandwidth and Quality of Service (QoS) requirements, establish connections between ATM End Systems across the network, and scale from small local networks to large global networks.

The OmniSwitch with ATM switching functionality supports PNNI version 1.0. In addition, it supports the Interim Inter-Switch Signalling Protocol (IISP); see Chapter 47 for information on IISP. Both PNNI and IISP are ATM routing protocols that support interoperable multi-vendor ATM networks.

IISP is a static routing protocol in which addressing information about ATM devices is statically defined at each ATM switch interface, and signalling is used to forward connection messages hop-by-hop through the network. In contrast, PNNI is a dynamic routing protocol that intelligently determines routes through the network based on connection requirements, and uses source routing to forward call setup requests through the network.

This chapter is for users with a basic familiarity of the PNNI routing protocol. It provides a brief overview of PNNI, but it focuses on the implementation of PNNI within the OmniSwitch. More extensive information on PNNI can be found in the ATM Forum PNNI 1.0 specification.

◆ Important Note ◆

In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. Chapter 8, “The User Interface,” includes documentation on changing from CLI mode to UI mode.

OmniSwitch PNNI Self-Configuration

The OmniSwitch implementation of PNNI is self-configuring while also providing commands that configure a diverse range of parameters. This chapter provides instructions on how to configure PNNI within the OmniSwitch at the global, node, and port level. Commands are provided that allow you to configure topology metrics, such as Administrative Weight, for each Class of Service supported on a port. In addition, various timers can be configured. Several other commands display extensive configuration information, status information, and statistics on neighboring nodes, adjacent links, and topology information packets.

Connection Admission Control (CAC) and Call Overbooking

The OmniSwitch supports Connection Admission Control (CAC) and Call Overbooking features.

CAC (Connection Admission Control)

CAC is a control function of the ATM Traffic Contract established between the source and the network during the call set-up phase that determines whether a connection can be established at the ingress switch. When CAC is enabled (default), the network calculates whether enough resources are available to support the connection at the desired QoS level without negatively impacting the QoS of any previously-established connections. CAC can be disabled on a per-link basis with the **map** UI command. See Chapter 41, “Managing Cell Switching Modules (CSMs)” for more information on modifying CSM port configurations.

Call Overbooking

To minimize traffic congestion and optimize access to network resources for different QoS classes, a switch needs to be able to monitor available bandwidth. The Call Overbooking feature allows available bandwidth on a CSM virtual port to be calculated by modifying the port's Overbooking Factor, to reduce or increase bandwidth on a logical or physical link, as needed. In addition to viewing available bandwidth on a single or multiple CSM virtual port(s), Call Overbooking can be viewed and configured with the **vap** and **map** UI commands, respectively. See Chapter 41, “Managing Cell Switching Modules (CSMs)” for more information on viewing and modifying CSM port configurations.

Load Balancing

The OmniSwitch supports Load Balancing, which is a technique for distributing traffic across the ATM network more efficiently. In Load Balancing, traffic is distributed between two or more paths, and routed on the less congested PNNI link based on available bandwidth. The PNNI routing process uses the ATM destination address and QoS information to calculate the shortest path to the destination and verify that all nodes on the path can support the connection. Once the path has been calculated, a table of available output ports that can forward the traffic is assembled. *(If only a single port is available, the available bandwidth database will not be consulted.)* The port with the greatest available bandwidth will be used to forward the traffic, provided that CAC is enabled (default) and accepts the traffic; if more than one port matches these parameters, the initial port will be used. As a result of load balancing, greater throughput is achieved across the network.

◆ Note ◆

CAC status can be viewed and modified with the **vap** and **map** commands. See Chapter 41, “Managing Cell Switching Modules (CSMs)” for more information on viewing and modifying ATM port configurations.

Summarization and Reachability

PNNI allows address reachability information to be summarized, reducing the number of addresses that must be stored in topology databases. OmniSwitch PNNI nodes advertise a single address prefix to represent a group of ATM End System or node addresses that share a common prefix. See *Summarization and Reachability* on page 46-18 for more information.

PNNI Path Limitations

The OmniSwitch implementation of PNNI supports at most 5 parallel paths between any two nodes. These paths can be physical CSM links or logical links (i.e., VP tunnels). Using factory-configured defaults, any one node, or OmniSwitch, should not have more than 30 neighbor nodes. If a node has more than 30 neighbor nodes, then performance may be affected unless you increase the hello or shortest path first timers. In addition, the maximum diameter of an OmniSwitch PNNI network should not exceed 50 nodes. If a larger diameter is required, then IISP links should be used.

PNNI Configuration

The OmniSwitch implementation of PNNI is self-configuring. In releases prior to 4.1, the only user configuration required is to specify a CSM port as a PNNI port using the **map** command or through SNMP-based network management software.

In Release 4.1 and later, you can enable CSM auto-port configuration, which does not require user configuration. If CSM auto-port configuration has been enabled, then two CSM ports connected together will automatically become PNNI ports. You must disable CSM auto-port configuration to manually configure a CSM port. See Chapter 41, “Managing Cell Switching Modules (CSMs)” for more information on CSM auto-port configuration.

PNNI Port Type Configuration

OmniSwitch PNNI contains carefully chosen defaults that enable you to bring up a PNNI node and begin communicating immediately. If you wish to fine tune the default configuration, several commands are available to configure PNNI parameters at the general, node, and port levels. Instructions for using these configuration commands begin on page 46-32. Other important PNNI variables, such as timer values and topology metrics, have defaults that are reasonable for most network environments.

In Release 4.1 and later, no reset is required for changing port type. In releases prior to 4.1, if you change the ATM port type from a PNNI port back to a UNI port (or vice versa) you *must* reset the switch if the port has already been used before.

Running PNNI Software

Different sets of image files are required depending on whether you need to configure just a single-peer group network, or if you also need to configure a multiple-peer group network. To configure a single-peer group network, you must load the following files into your switch:

asm.img (MPM-1G or MPM-III and an FCSM-I or FCSM-II) *or* **asmc.img** (MPM-C)
cell.img
sonet.img

To run the multiple-peer group version of PNNI, you must load the following files into your switch:

asm_mpg.img (MPM-1G or MPM-III and an FCSM-I or FCSM-II) *or* **asmc_mpg.img** (MPM-C)
cell_mpg.img
sonet.img

◆ Note ◆

If you are using the multiple-peer group files listed above, and you want to run LES/BUS software, you *must* use the **lsm_mpg.img** image file instead of the **lsm.img** image file.

In addition, you must add the following line to your command file (**mpm.cmd** on the MPM-1G, **mpmc.cmd** on the MPM-C, or **mpm3.cmd** on the MPM-III) if you load the **asm_mpg.img** (or **asmc_mpg.img**), **cell_mpg.img**, or **lsm_mpg.img** files:

```
atm_load_mpg=1
```

You *must* put this line before the **cmInIt** line, and you must reboot the switch to implement the change. In the single-peer group version of PNNI, either change this line to **atm_load_mpg=0** or leave it out of the command file. See Chapter 11, “Managing Files,” for information on editing the command file.

Loading the PNNI Module

PNNI functionality is built into the **cell.img** file in single-peer group configurations, and in the **cell_mpg.img** file in multiple peer group networks. When the **cell.img** or **cell_mpg.img** file is placed into the OmniSwitch’s flash memory file system, the switch will dynamically load the file once it senses the presence of a Cell Switching Module (CSM). During the initialization of the cell switching code, PNNI is enabled or disabled. Once the PNNI protocol is running in system memory, self-configuration begins and nodes can begin exchanging Hello packets, building topology databases, and establishing data connections (provided the associated port has been set to type PNNI). If the port type is set to any value other than PNNI, then PNNI will forward on that port based on user-defined static routes.

Default ATM Address

To allow PNNI nodes to communicate without user intervention, each node is automatically assigned a default ATM address at system start-up. This address includes a prefix of **3903488001bc90000101** followed by Alcatel-specific OID information. Other important PNNI identifiers, such as the Node IDs and Peer Group IDs, can automatically be derived from this default ATM address. You can optionally change this ATM address later through the **pncfg** command (described on page 46-40).

◆ Important Note ◆

The default ATM address for the node is locally defined and should not be used when attaching to a public network. To obtain a unique NSAP address for your enterprise consult RFC 1629 or ANSL.

In PNNI hierarchy levels 103 (hexadecimal 67) and lower in a multiple-peer group network, the Node ID and ATM address can be the same. In levels 104 (hexadecimal 68) and higher, the Node ID and ATM address *must* be different.

Static Routes/IISP

Static routes must be user configured. PNNI is a dynamic routing protocol that can determine path selection on its own, so static routes are optional. If static routes or the Interim Inter-Switch Signalling Protocol (IISP) are necessary, then use the Route Management menu (described in Chapter 47, “Managing IISP and PNNI Routes”) for configuration.

Elements of a PNNI Network

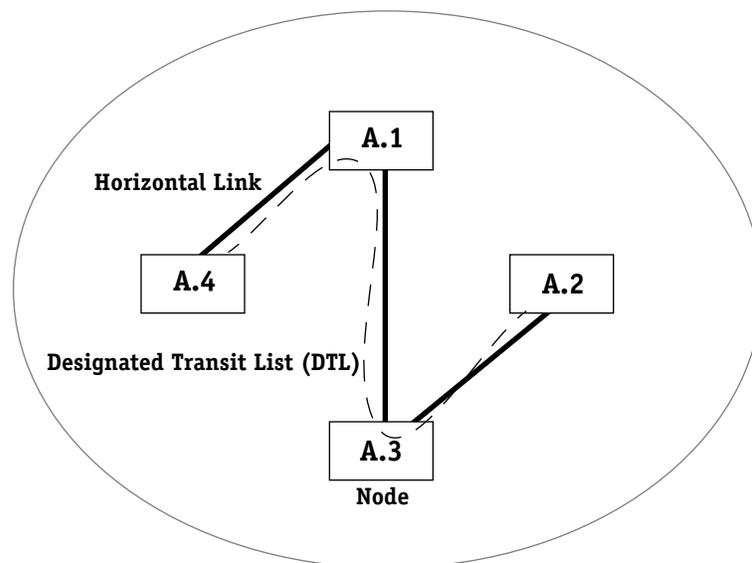
PNNI relies on a hierarchical model to distribute information throughout the network about all ATM nodes and links. Each node is part of one or more *peer groups* that serve as its local routing domain. All nodes in a single peer group continuously update each other on their current status.

Each node shares a common map of the peer group, including information on how nodes are connected, which End Systems (or the address summaries representing those devices) are attached to which nodes, and the topology attributes supported at each node. This information is kept in each node's *Topology Database*, which contains individual entries referred to as *PNNI Topology State Elements (PTSEs)*. Whenever there is a change within the peer group, all nodes are updated through regular exchanges of topology information. Topology information is exchanged between nodes via *PNNI Topology State Packets (PTSPs)*.

◆ More Information on Topology Exchanges? ◆

For more details about PNNI topology information exchanges, see *PNNI Network Initialization* on page 46-19. The packet types used in the PNNI protocol are described in *PNNI Packet Types* on page 46-15.

Within a single peer group, nodes are connected by *horizontal links*, which are physical links between the nodes. A *Designated Transit List (DTL)* is a source route between nodes through a peer group. A DTL provides a complete source route through the peer group and will be used to route call requests through the peer group.



A Single PNNI Peer Group

PNNI has the capability to support multiple peer groups. The OmniSwitch supports multiple peer group configurations in Release 4.1 and later.

Multiple Peer Group Networks

In Release 4.1 and later, multiple peer group configurations, where information on each peer group is summarized by *Peer Group Leader (PGL)* nodes and aggregated into virtual ATM nodes known as *Logical Group Nodes (LGNs)*, are supported. These Logical Group Nodes distribute summary information on their peer groups to other LGNs. Depending on the size of the network, there may be several levels of low-level nodes and Logical Group Nodes.

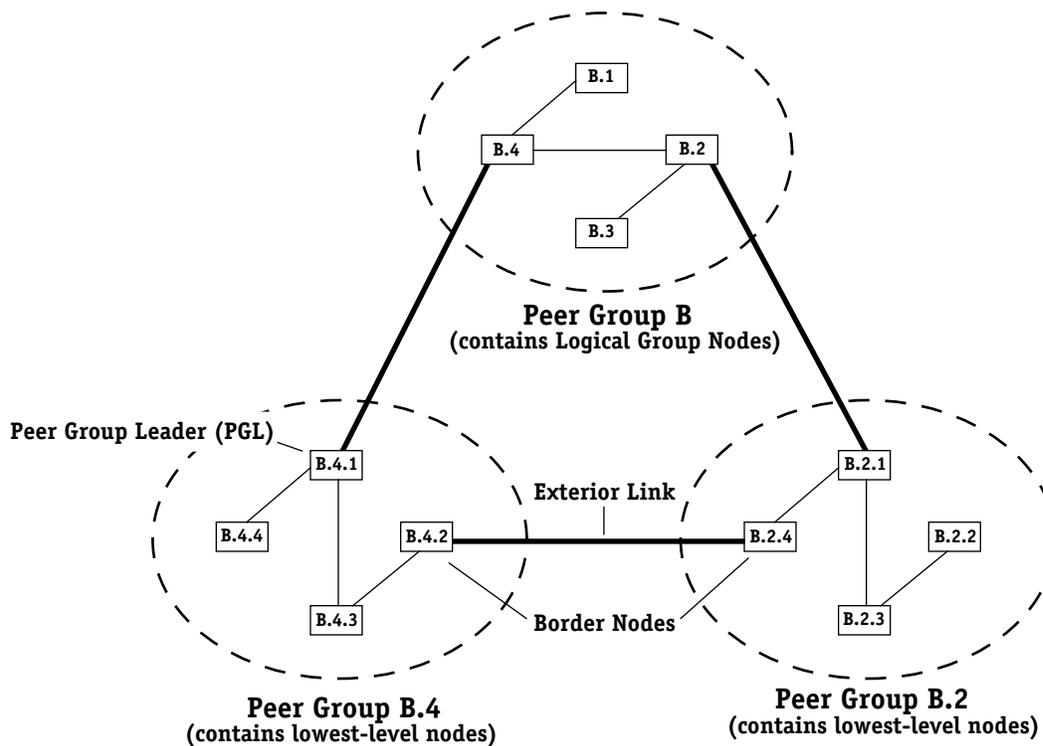
◆ Note ◆

Multiple peer group operation is an optional feature that is not included as part of the standard **cell.img** and image files. Instead, you must load the image files designed for this feature. See *Running PNNI Software* on page 46-4 for more information on multiple-peer group PNNI files.

The level of a peer group or node indicates the position of that peer group or node within the PNNI hierarchy. PNNI levels range from 0 to 104. A lower PNNI level number indicates a node that is higher up in the PNNI hierarchy (greater summarization of PNNI network topology information). A higher PNNI level number indicates a node that is lower in the hierarchy. Nodes that are located at the lowest-level of a particular chain in the PNNI hierarchy are referred to as *lowest-level nodes*.

In a single peer group network, just one peer group is supported and there is just one level in the PNNI hierarchy. The default number for this level is 80 decimal (50 hexadecimal). You must configure a node to operate at a specific level to implement multi-peer group operation.

Another type of node in a multiple peer group configuration is a *border node*. Border nodes lie on the edges of their respective peer groups and form physical links with border nodes in other peer groups. However, border nodes do not summarize information on their peer groups; summarization is left to the Peer Group Leader. Instead, border nodes inform other nodes in their peer group about their access to another peer group. These other nodes may use this link to set up connections to the neighboring peer group (or *through* the neighboring peer group). The border node's link is referred to as an *exterior link*.



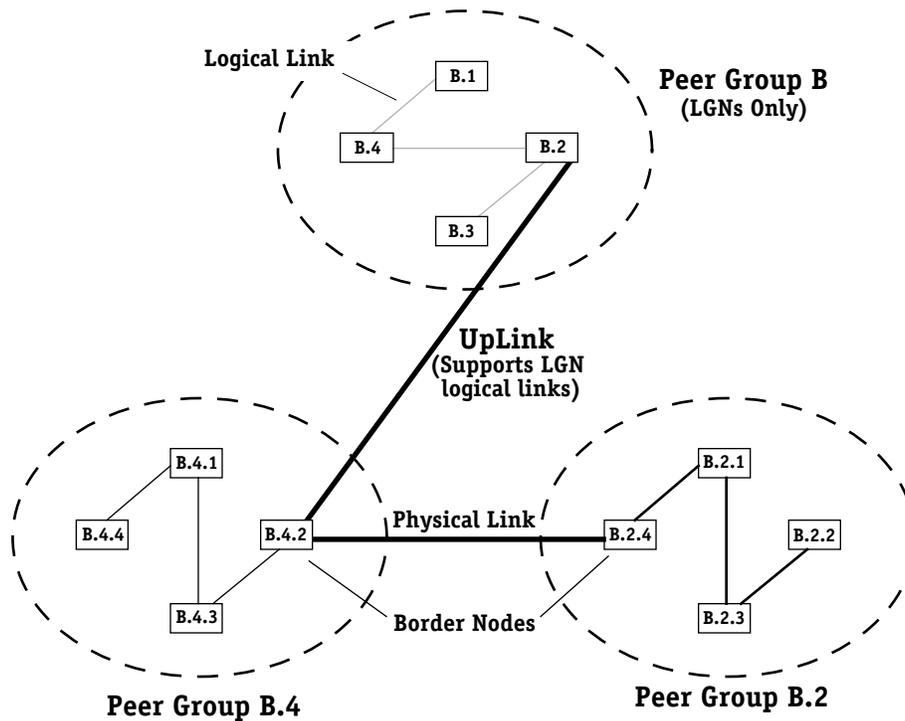
A PNNI Network With Multiple Peer Groups

Logical Group Nodes (LGNs) are virtual PNNI entities that aggregate information on an entire peer group. They are not physical nodes the way lowest-level PNNI nodes are physical nodes. In addition, LGNs do not have actual physical links with each other or with their child nodes. Instead, LGNs have logical links with each other that rely on physical links between border nodes in neighboring peer groups. These logical links between LGNs representing one peer group and border nodes in another peer group are called *uplinks*. The border nodes supporting these uplinks are called *upnodes*.

There must be a physical means for transporting topology information between LGNs. These LGNs depend on border nodes in other peer groups to provide information on the neighboring peer group. The example below shows a border node in peer group B.4 (node B.4.2) with a logical uplink to the LGN for peer group B.2. The LGN in peer group B.2 relies on this link to obtain topology information on peer group B.4.

◆ Note ◆

If you have a network with more than 30 PNNI nodes, you should upgrade the SIMM memory in your MPM II or MPM 1G to at least 32 MB.



Uplink in a PNNI Network

Peer Group Leader (PGL) Election Algorithm

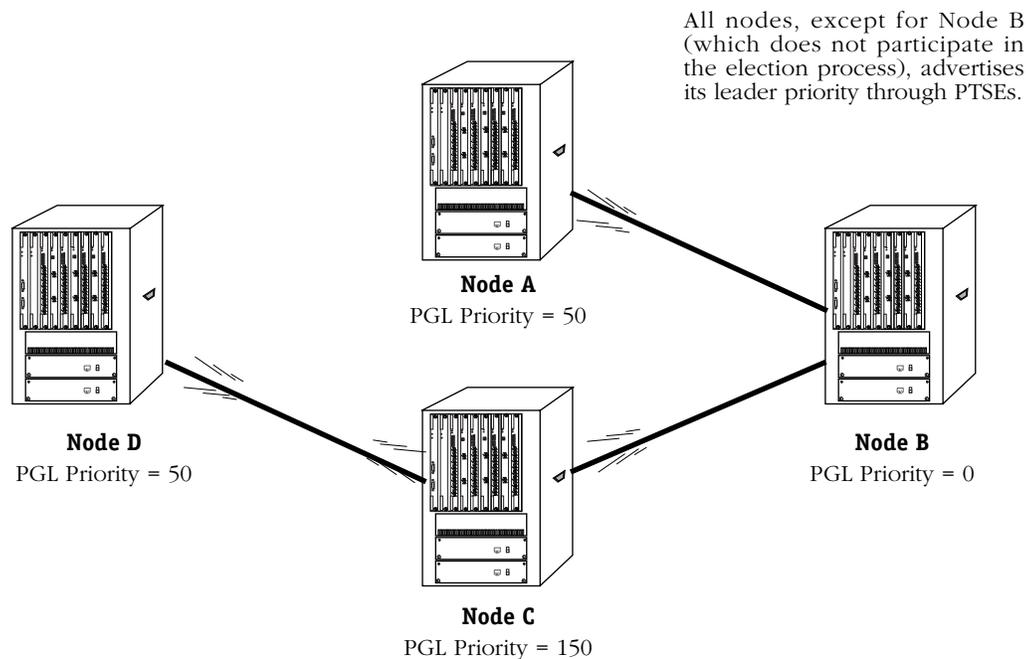
The nodes in a logical peer group use an election process to determine which node will be the peer group leader (PGL). A node participates by advertising its leadership priority to all the nodes in the peer group through PTSEs. Each node will elect the node with the highest non-zero PGL priority as PGL.

The peer group must have at least two nodes with non-zero PGL priorities for an election to take place. All nodes will participate in the election process unless their leadership priority and preferred PGL is set to zero. If the nodes cannot reach a unanimous decision, then a 2/3 vote will suffice. In the case of a tie, the node ID will be used as a tie breaker. Once a node is elected PGL, its leadership priority is incremented to ensure stability and prevent future election deadlocking.

As shown in the figure on the following page, all nodes, except for Node B (which does not participate in the election process), advertises its leadership priority through PTSEs. Node C, which has the highest leadership priority, will be elected PGL unanimously since Nodes A and D will elect Node C PGL and Node C will elect itself PGL.

◆ Note ◆

See *Configuring the Peer Group Leader Election Process on All Node Levels* on page 46-48 for documentation on configuring the PGL election process on all node levels.



How Nodes Elect a Peer Group Leader (PGL)

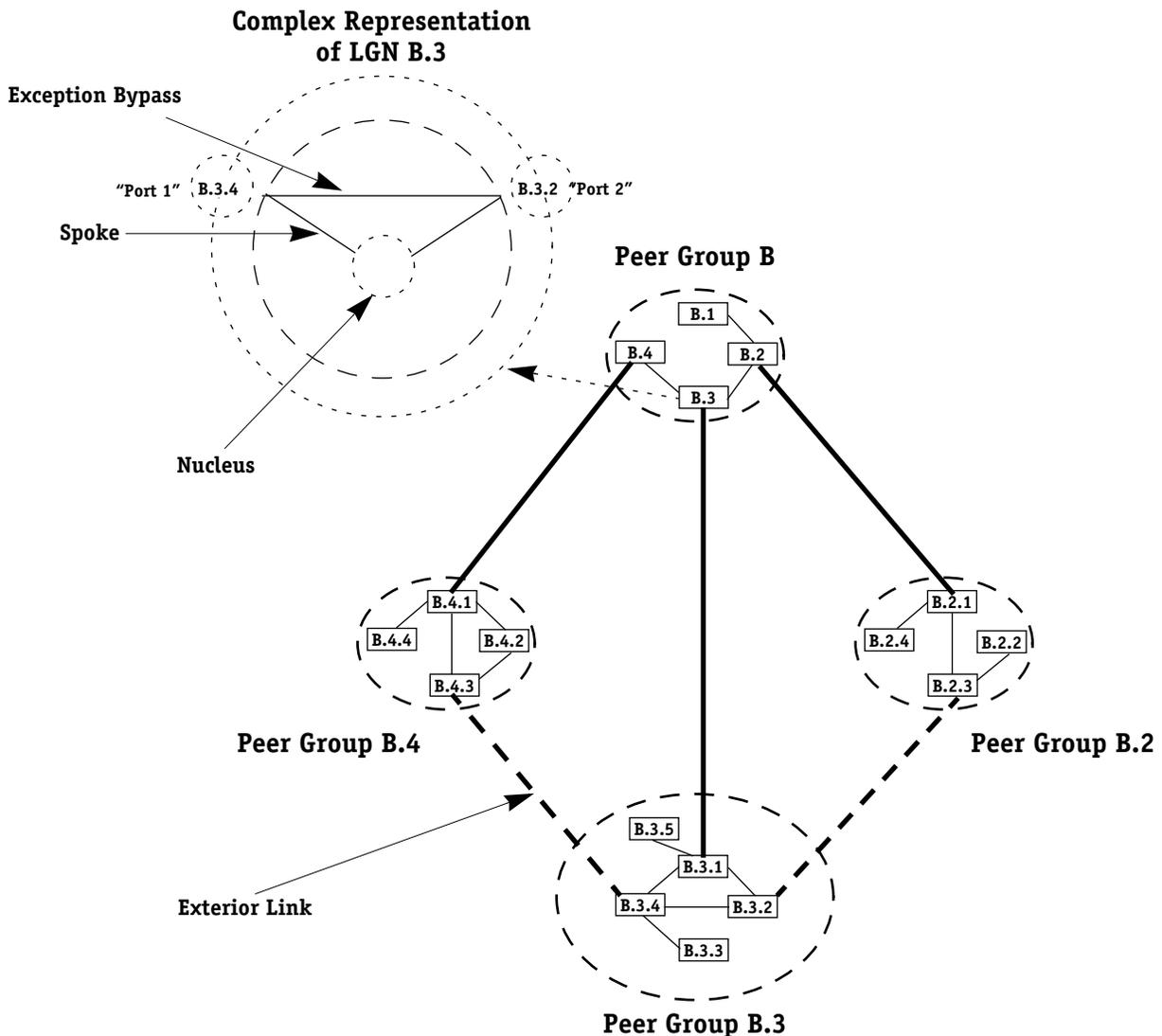
The PGL election algorithm is a continuously running process. If a node that is PGL fails or loses its connectivity, then the node with the next-highest leadership priority will become PGL. If a node with a higher priority leadership priority is added to the peer group, it will become the new PGL.

You can configure the PGL priority of a node with the **pncfg** command, which is described in *Configuring Node-Specific Parameters* on page 46-40. To view the current leadership priority of a node, use the **pninfo** command, which is described in *Viewing Node-Specific Information* on page 46-56.

Complex Representation

Topology aggregation is the process used in PNNI to summarize the topology information of a child peer group to its parent group. This summarization can greatly reduce the volume of information advertised in the parent peer group. Thus, effective topology aggregation is a necessity for PNNI to scale to large multiple-peer group networks. In PNNI, this concept of topology aggregation is known as *complex node representation*.

The figure on the following page shows the complex representation of logical group node (LGN) B.3 using a symmetric star topology. The *nucleus* is the interior reference point of the logical node. The logical connections between the nucleus and another node in the peer group are known as a *spoke*.



Complex Representation of a Logical Group Node

In most cases, peer groups are not symmetrical. Therefore, exceptions can be used to represent the connectivity of nodes that is significantly different from the default. For example, a node in a peer group could be in a different location from other nodes in a peer group. In complex representation, the local nodes would have spokes to the nucleus with default attributes whereas the remote node would have a spoke with exception attributes to the nucleus. A bypass exception represents connectivity between two nodes that bypasses the nucleus because it is more efficient.

You can configure complex representation with the **pnCFG** command, which is described in *Configuring Node-Specific Parameters* on page 46-40. To determine if a node is using complex representation, use the **pninfo** command, which is described in *Viewing Node-Specific Information* on page 46-56.

PNNI Identifiers

Node ATM addresses are important in the PNNI identification scheme. But PNNI requires additional methods of identification to describe its hierarchical structure and its peer groups. The following descriptions highlight some key PNNI identifiers that you are likely to encounter while configuring and monitoring your PNNI network.

Level Identifier

The level identifier is the level within the PNNI hierarchy where a node exists. This value may range from 0 to 104, with higher values indicating nodes lower in the PNNI hierarchy. This level is used to determine the default Node ID and the default Peer Group ID for a node. (The default node level is 80 decimal.) In a single-peer group configuration, all nodes will be at the same level.

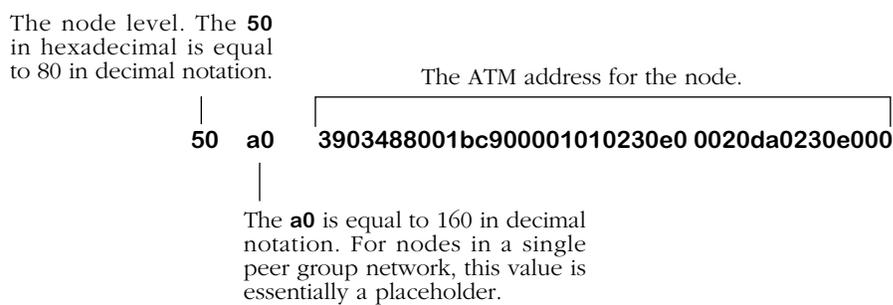
Node ID

The Node ID is a 22-octet identifier for an OmniSwitch node within the PNNI network. The first octet consists of the level of the node within the PNNI hierarchy. By default, OmniSwitch nodes reside at level 80 decimal.

◆ Important Note ◆

In releases previous to 3.2, the default node level was 96 decimal. In release 3.2 and later the default level is 80 decimal. Therefore, if you have an existing OmniSwitch network with PNNI nodes residing at the old default level, then you will have to reconfigure the Node IDs for either the new nodes or the old nodes if you want all nodes to be in the same peer group.

In a single-peer network, the next octet equals 160, and the remaining 20 bytes consist of the ATM address of the node itself. The following is an example of a single-peer network Node ID expressed in hexadecimal notation:

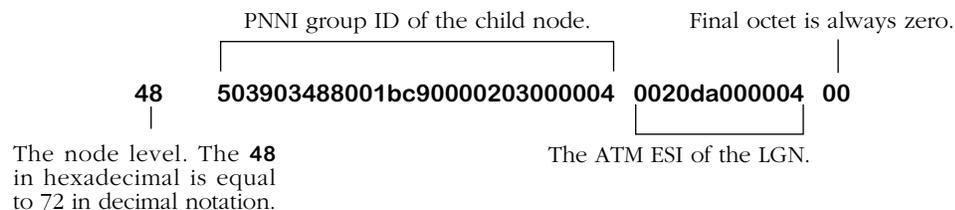


Typical Node ID in Single Peer Group Network

Logical Group Nodes (LGNs) use a slightly different Node ID structure. The first octet is the node level, the next 14 octets are equal to PNNI node peer group ID of the child node whose election as the Peer Group Leader (PGL) produced this LGN, the next 6 octets are the ATM End System Identifier (ESI) of the LGN, and the final octet is a zero.

In PNNI hierarchy levels 103 (hexadecimal 67) and lower in a multiple-peer group network, the Node ID and ATM address can be the same. In levels 104 (hexadecimal 68) and higher, the Node ID and ATM address *must* be different.

The following is an example of an LGN in a multiple-peer network expressed in hexadecimal notation:



Logical Group Node (LGN) ID in a Multi-Peer Group Network

Note on Default ATM Node Addresses

A default ATM address will be assigned to each PNNI node without user configuration. This default ATM address is equal to

3903488001bc90000101 xxyyzz 0020da xxyyzz 00

where **xxyyzz** is the Alcatel-specific OID for the MPM in this chassis.

Port ID

Port IDs identify each CSM port in an OmniSwitch, but also identify logical links between nodes. A link between two nodes is identified by the Node IDs of the two nodes as well as the Port IDs of the CSM ports on each end of the link.

PNNI uses Port IDs that are internal to the local switch. ATM switches use different methods for calculating Port IDs, but the values are relevant only to the local switch. In some screen displays, Port IDs may also use the standard OmniSwitch Slot/Port notation to identify ports on each end of a link. For example, the notation **5/2** would indicate port 2 on the CSM module located in slot 5 of the OmniSwitch. The **ppinfo** command displays the local mapping of the slot/port to the advertised PNNI port identification.

Peer Group ID

The Peer Group ID identifies a peer group within the PNNI hierarchy. The first octet is the level within the PNNI hierarchy where nodes in this peer group are located. The next 13 octets are the prefix for the ATM End System Address of the node. The prefix

3903488001bc90000101000000

is the default peer group ID for each node. As an example, the Peer Group ID for a node in a peer group located at level 80 would be

50 3903488001bc90000101000000

where **50** hexadecimal is equal to 80 in decimal notation.

Summary Addresses

PNNI use a summary address to represent end systems that are attached to a node. Nodes use these summary addresses during exchanges with other nodes in the same peer group. ILMI uses the summary address when satisfying registration requests to attached ATM devices.

The address summary is configurable through the **pncfg** command, which is described in *Configuring Node-Specific Parameters* on page 46-40.

Single-Peer Networks

In a single-peer group network, the default summary address used by a node is the 13-byte prefix:

3903488001bc90000101 xxyzz

where **xxyzz** is the 3-byte Alcatel-specific address in the MPM MAC address for that node.

Multiple-Peer Group Networks

In a multiple-peer group network, there are two summary addresses: the default summary address and the configured summary address. The configured summary address is taken as the ILMI prefix. The default summary address is derived when the higher node is configured.

PNNI Packet Types

There are five types of packets used by the PNNI routing protocol to maintain communication between nodes and keep node databases in synchronization. These five packet types are described below.

Hello packets

Hello packets are exchanged between a node and all of its neighboring nodes. These packets contain Node IDs, Peer Group IDs, Port IDs, and information on Hello protocol timers. The main purpose of Hello packets is to establish the state of the links connecting nodes. In a single peer group model, each link must attain a state of 2-WAY-INSIDE before database synchronization begins. See *Viewing Link Information* on page 46-66 for more information on Hello states.

Database Summary packets

After two nodes learn about each other through Hello packet exchanges, they inform each other about the entire contents of their topology databases through the exchange of Database Summary packets. Database Summary packets include information on all the PTSEs in a node's topology database.

PNNI Topology State Element (PTSE) Request packets

When a node receives a Database Summary packet from a neighboring node, it finds all the new PTSEs included in that packet. PNNI nodes need to keep up-to-date topology information, so any new PTSEs from the neighboring node must be obtained. The node sends a request for these new PTSEs in the form of PTSE Request packets. When the neighboring node receives these Request packets it forwards the PTSEs requested by the node.

PNNI Topology State Packets (PTSPs)

PTSPs bundle topology information from one node for transport to another node. Topology information about a peer group is propagated through a peer group via PTSPs. PNNI Topology State Elements (PTSEs) are individual pieces of information in a node's topology database. A PTSP bundles one or more of these PTSEs and sends them to a node that has requested the particular information included in the PTSE.

PNNI Topology State Element (PTSE) Acknowledgment packets

When a node receives a particular PTSE from another node it responds with a PTSE Acknowledgment packet. These packets inform the node that sent the PTSEs (bundled inside PTSPs) that the information was transported successfully.

Metrics and Attributes

PNNI frequently advertises information on the state of links and nodes by means of topology metrics and attributes. A topology *metric* is a parameter that is combined along a path to determine whether this path meets the requirements of a given call request. For example, the administrative weight of a path is the sum of the weights of all links and nodes along the path.

A topology *attribute* is a parameter that is considered individually at each node when determining whether a path meets requirements. For example, if any node along a path violates the Cell Loss Ratio (CLR) for a given call, then that entire path must be rejected.

The following metrics and attributes are used by PNNI for all ATM traffic types. You can configure values for all topology metrics (i.e., Administrative Weight, Cell Transfer Delay, and Cell Delay Variation) on a port-by-port basis via the **ppcfg** command (described in *Configuring Port Parameters* on page 46-50). Topology attributes are discovered dynamically by PNNI from the ATM switch fabric and do not require user configuration.

Metrics

Administrative Weight	Indicates the preference of a given link relative to other links. Lower administrative weight values have higher priority on the link than higher administrative weight values.
Cell Transfer Delay	The average time, in microseconds, it takes for cells to transmit from any incoming port to an outgoing port in the switch for a particular Class of Service. The default for CTD is 10.
Cell Delay Variation	Also referred to as “jitter,” this metric is the change that occurs in cell spacing from the time cells leave one node and arrive at another node.

Attributes

Maximum Cell Rate	The maximum bandwidth usable by a connection.
Available Cell Rate	The amount of bandwidth available on this link or node. This value is dynamic and changes depending on usage of the link or node.
Cell Loss Ratio	The ratio of the number of lost cells to the total number of cells transmitted across a link or node. There is a Cell Loss Ratio for CLP=0 traffic (CLR_0) and for CLP=0+1 traffic (CLR_{0+1}).
Cell Rate Margin	The difference, in cells per second, between the total bandwidth allocation and the sustainable cell rate allocation. This attribute indicates the “safety margin” of available bandwidth above the amount of bandwidth allocated for the sustainable cell rate. Not supported in the current release.
Variance Factor	A relative measure of the Cell Rate Margin normalized by the variance of the aggregate rate. Not supported in the current release.

The table on the next page describes how each ATM Class of Service uses these metrics and attributes. An Administrative Weight is always required to enable a particular Class of Service on a CSM port. However, the use of other metrics and attributes varies by Class of Service.

Topology Metrics and Attributes and ATM Service Classes

Metric/Attribute	User Configurable?	Service Classes				
		CBR	rt-VBR	nrt-VBR	ABR	UBR
Administrative Weight	Yes	Required	Required	Required	Required	Required
Cell Transfer Delay	Yes	Required	Required	Required	N/A	N/A
Cell Delay Variation	Yes	Required	Required	N/A	N/A	N/A
Maximum Cell Rate	No	Optional	Optional	Optional	Required	Required
Available Cell Rate	No	Required	Required	Required	(1)	N/A
Cell Loss Ratio	No	Required	Required	Required	N/A	N/A
Cell Rate Margin	No	N/A	Optional	Optional	N/A	N/A
Variance Factor	No	N/A	Optional	Optional	N/A	N/A

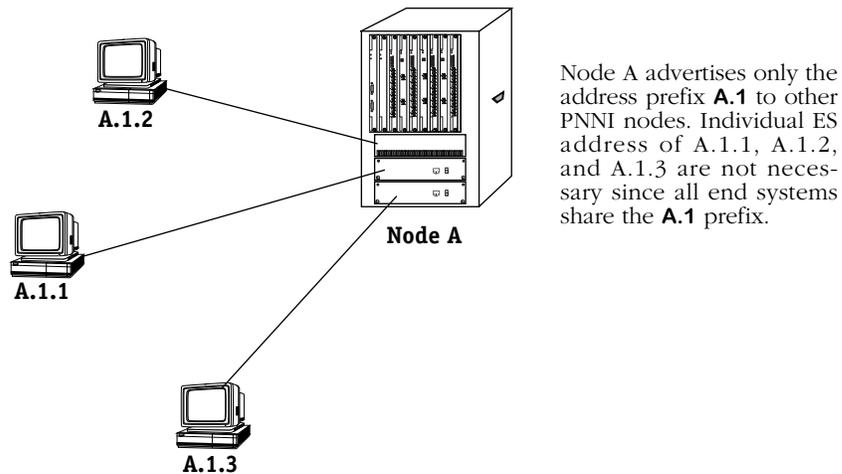
Table Note:

(1) For ABR traffic, the Available Cell Rate is the same as the Minimum Cell Rate.

Summarization and Reachability

PNNI allows address reachability information to be summarized. PNNI nodes can advertise a single address prefix to represent a group of ATM End System or node addresses that share a common prefix. This summarization reduces the amount of information each node needs to store in its topology database. PNNI matches n addresses with the summary address. If they match, then the summary address is advertised.

The following diagram illustrates how PNNI summarizes reachability information. In the diagram, Node A summarizes addresses for the three attached End Systems into a single address prefix of **A.1**. This address prefix is the shortest address common to all three systems.



How PNNI Summarizes Reachable Addresses

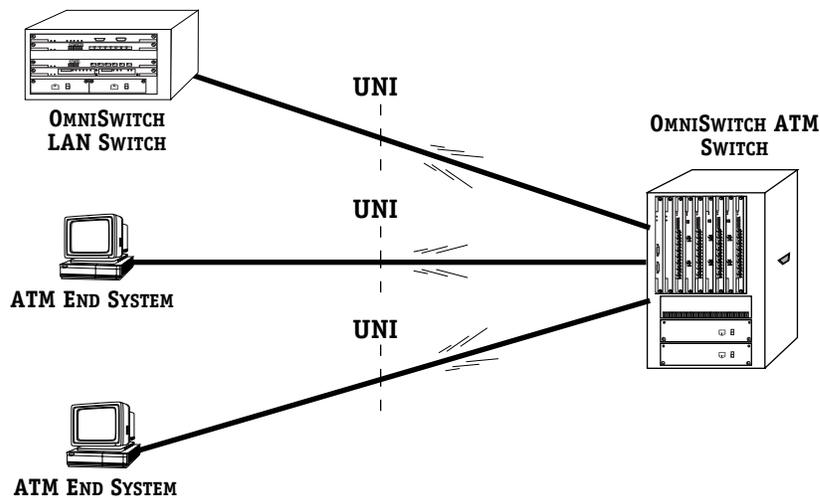
PNNI Network Initialization

Before OmniSwitch nodes can set up virtual connections between ATM end stations, they need to initialize properly. An OmniSwitch node needs to know its own private ATM address, its own Node ID, the ATM address prefixes of attached ATM End Systems, and information about nodes representing reachable ATM End Systems. Much of this information is self-configured by PNNI, but can also be user-configured through User Interface software or SNMP-based network management software.

Once an OmniSwitch node starts up, it must go through steps to build an accurate topology database. Building this database is essential for the proper functioning of the PNNI routing protocol. OmniSwitches use this topology information to select routes through the network before establishing virtual connections between end systems. In addition, the PNNI topology database is updated periodically to ensure that nodes have an accurate view of the network. The following steps outline what happens at network initialization for a single OmniSwitch where PNNI is enabled.

Step 1. Discover Attached ATM End Stations

The first step in OmniSwitch PNNI initialization is to discover the ATM end systems that are attached to the node. These end systems include directly attached stations and LAN switches with ATM uplinks to the OmniSwitch. The OmniSwitch can discover ATM end systems through Integrated Local Management Interface (ILMI) address registration. ILMI provides information on the addresses of attached ATM end systems. Address information can also be configured manually for End Systems that do not support ILMI; such configuration takes place at the End System.

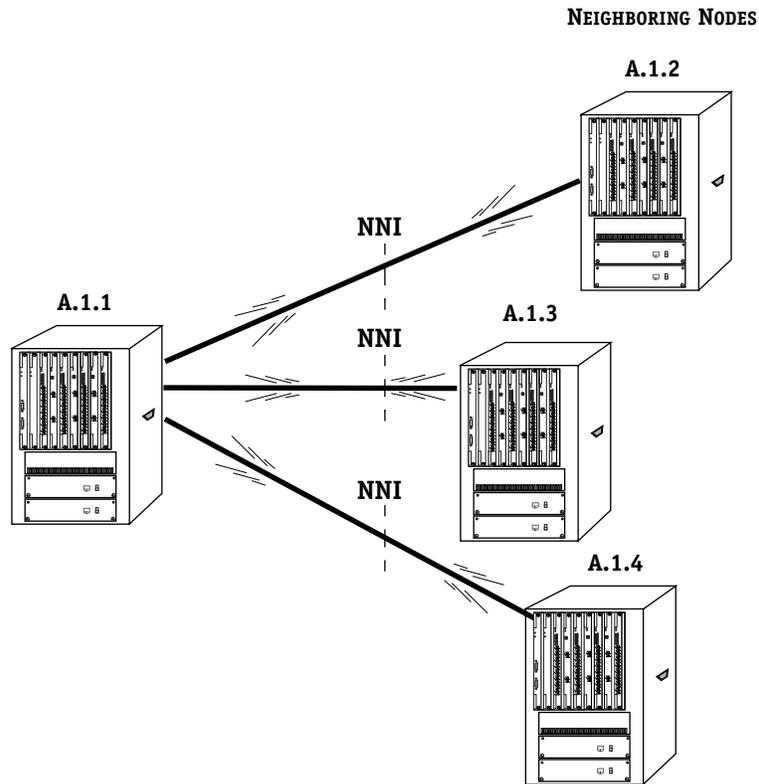


OmniSwitch ATM Switch Discovering Attached ATM Devices

Step 2. Discover Neighbor Nodes

In order to set up Routing Control Channel (RCC) virtual connections, each OmniSwitch needs to know about attached PNNI nodes in its peer group. It will be through these neighboring nodes that the OmniSwitch obtains information about the rest of the network. Each OmniSwitch node discovers the identity of its neighboring nodes, or adjacent nodes, and becomes a member of a peer group via the Hello protocol. Nodes in a single peer group exchange Hello messages on each physical link. A Hello message contains the ATM address of the sending node.

The diagram below illustrates the node discovery process. Through Hello message exchanges, Node A.1.1 discovers its neighboring nodes A.1.2, A.1.3, and A.1.4.



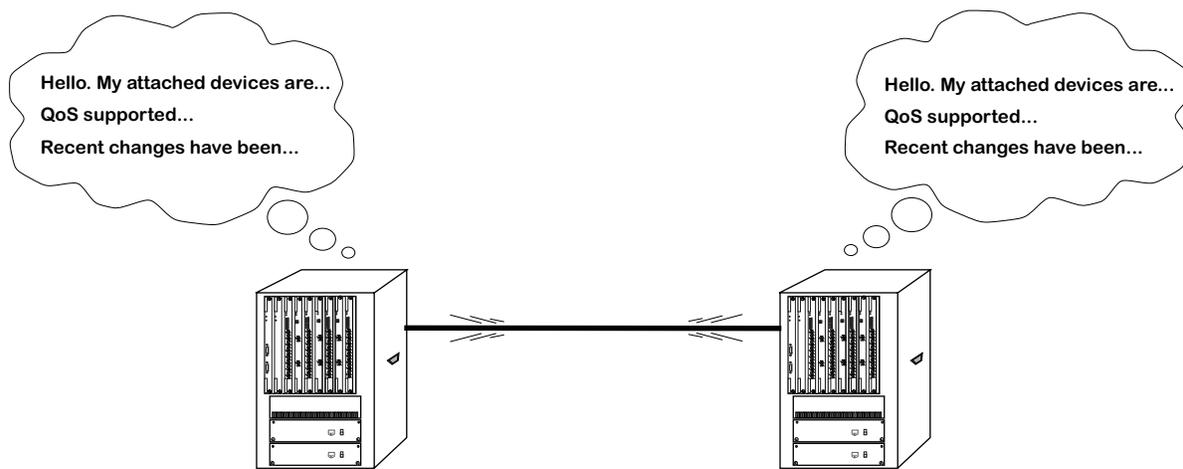
OmniSwitch Discovering Neighboring Nodes in a Single Peer Group

Step 3. Send Topology Information for Updating Other Nodes

Once nodes on both sides of a physical link know each other's identity through the exchange of Hello messages, they can begin exchanging topology information. The ATM network will change at times as nodes and devices are added and virtual connections are established and torn down. Because of these changes, the various OmniSwitch nodes need a way to advertise the current information in their topology databases. Entries within a node's topology database are referred to as PNNI Topology State Elements (PTSEs).

Topology information is exchanged via PNNI Topology State Packets (PTSPs). PTSPs contain information on nodes, links, and reachable addresses in the network. Periodically, an OmniSwitch node will send PTSPs that update other nodes of its current state (virtual connections, Quality of Service supported). The topology update messages—PTSPs—are flooded by a reliable hop-by-hop mechanism that ensures that all nodes in the network have updated topology information. In addition, each OmniSwitch can receive PTSPs from other nodes to help build its topology database.

OmniSwitch nodes use the information in their topology database to compute path selection for attached ATM devices that request virtual connections.



OmniSwitches Sending and Receiving PTSPs

Step 4. Compute the Topology of the Peer Group

Periodically an OmniSwitch will run a Shortest Path First (SPF) algorithm. The interval at which this algorithm is executed is configurable through the **pgcfg** command. If the OmniSwitch has not received any PTSEs from other nodes, then the topology remains intact and the SPF will be deferred to the next period.

If new PTSEs have been received, then the topology database is re-computed. This database is used by call control within the OmniSwitch to forward calls.

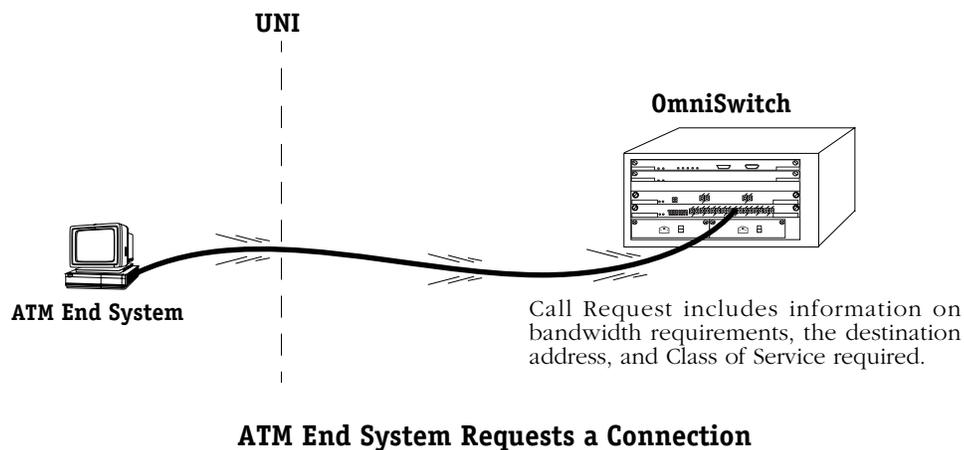
Establishing a Connection

It is easier to understand the features of PNNI in the OmniSwitch by following a simple example. In this example, the steps required for establishing a point-to-point connection using PNNI are illustrated. This example assumes that the connection is a Switched Virtual Circuit (SVC) and that the OmniSwitch nodes involved are using the PNNI routing protocol. It also assumes that the ATM network has initialized properly as explained in *PNNI Network Initialization* on page 46-19.

Step 1. Receive a Call Request

The first step is initiated by the ATM End System (ES) that wants to communicate over the ATM network with another ATM ES. An ATM ES could be a workstation, server, LAN switch, or router. The source ATM ES requests a connection with another ATM ES, the destination. This request will be received by the OmniSwitch node to which the source ATM ES is directly connected. The OmniSwitch may receive this request in the form of a signalling protocol message (as in the case of an SVC), or as a request from the Network Management Software on behalf of the station (as in the case of a soft PVC).

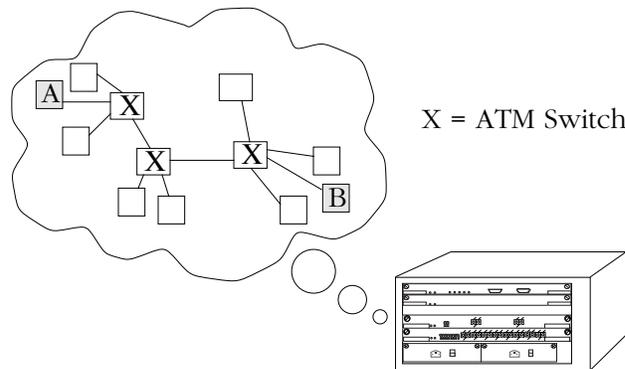
In the case of an SVC, the signalling message will contain information on the requested cell rate, the address of the destination station, a virtual connection identifier (VPI/VCI value) and a requested Class of Service.



Step 2. Locate Called Parties

In the first step, the OmniSwitch PNNI node learned the address of the destination End System. An OmniSwitch using the PNNI protocol continuously updates its internal map of the ATM network. This map—referred to as a “Topology Database”— includes reachability, link status, and node status information. This map is updated through topology update messages called PNNI Topology State Packets (PTSPs), which are received from other PNNI nodes.

In this second step, the OmniSwitch searches its topology database for the location of the destination device within the ATM network. Within this database, the OmniSwitch finds the location of the end device and the ATM switch to which the destination is attached. This information is also referred to as “reachability” information. By looking through its database, the OmniSwitch decides whether or not this device is reachable. The illustration below shows the OmniSwitch node locating the source (A) and the destination (B) in its topology database. If the end device is not reachable, then connection establishment may be terminated at this point.



OmniSwitch Locates the Destination in Topology Database

The topology database contains information on End System and node reachability. This database specifies the nodes where an End System may be reached and the set of paths that lead to that node.

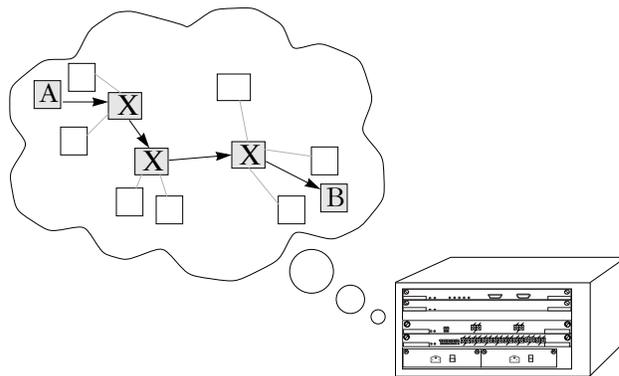
PNNI summarizes reachability information in a node’s topology database. Summarization reduces the amount of information needed to be stored in the database. A switch does not require a database of all end stations, just enough information to uniquely identify the device’s link to a PNNI node. Therefore, each OmniSwitch node can advertise a single prefix (known as a summary address) instead of the entire ATM address of an End System.

Step 3. Path Selection

Once the OmniSwitch knows where the destination system is located (i.e., the ATM address of the node that represents the destination), it computes the path through the ATM network that will meet the bandwidth and Class of Service requirements of the original request. The OmniSwitch uses its topology database to determine which paths are possible based on the dynamic state of the network.

The OmniSwitch knows the node state, link state, and reachability information for the ATM network. From this information it can determine which path is best. It may find a switch that is located within the path but does not support enough bandwidth or a particular Class of Service to sustain the connection requirements of the source device. In such a case, that switch will be eliminated from consideration when constructing the path.

The selected path is identified as a sequence of Node IDs and, optionally, Port IDs along a path from End System A (source) to End System B (destination). This information, referred to as a Designated Transit List (DTL), is added to the original Setup message. The illustration below shows an OmniSwitch node selecting a path through the various nodes in the ATM network to the destination (B).

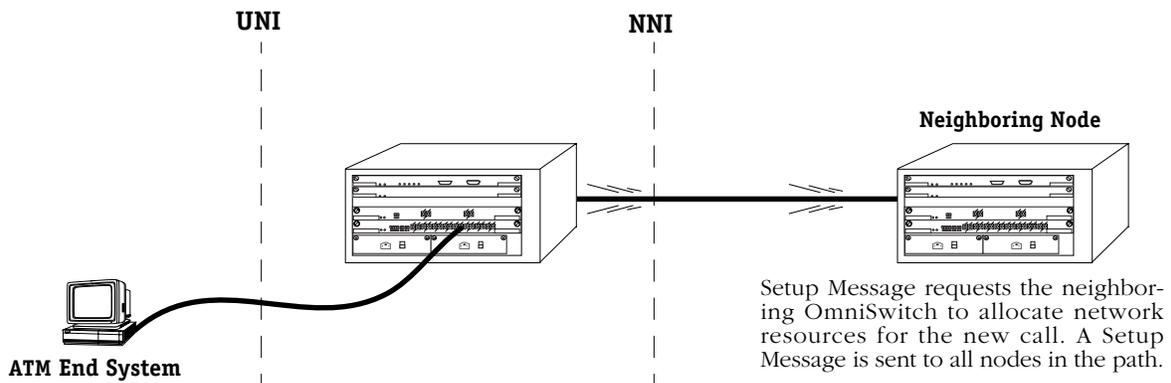


OmniSwitch Selects a Path to the Destination

Step 4. Send Setup Message

The OmniSwitch node now sends a Setup Message along the path selected in the previous step to the first node in the path. The neighboring OmniSwitch (or other ATM switch) will then process the setup request. If this node accepts the request, it forwards the setup message to the next node in the path.

This step will be repeated at each node on the path. However, a node only passes on the request if it accepts the request. The setup message is source routed along the path until all nodes receive the request. Each node in the path is concerned only with the connection to the neighboring node upstream and downstream. The illustration below shows the first OmniSwitch sending the Setup Message to the next node in the path.



OmniSwitch Sends Setup Message to Neighboring Node

Step 5. Process Setup Message

At each hop along the path selected, each ATM switch processes the setup message to determine if it can meet the connection requirements of the request. To process the setup message, a switch uses a specialized part of its functionality referred to as Call Admission Control (CAC). CAC is a set of functionality concerned with determining whether a particular connection request can be met by the available resources in the switch. During this process, CAC looks at its available bandwidth and the Classes of Service it supports. If it determines it can set up the connection, then it assigns a connection identifier (VPI or VPI/VCI) and allocates bandwidth for the connection.

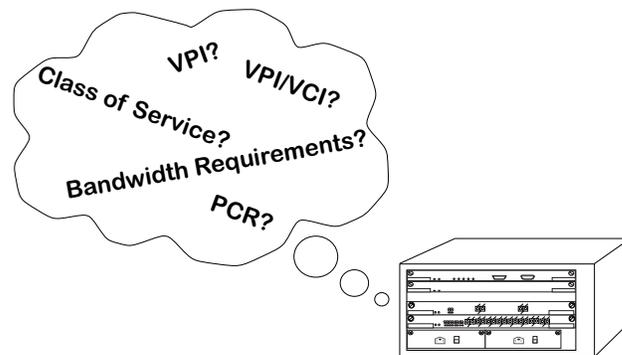
◆ **Note** ◆

The OmniSwitch uses the generic CAC algorithm defined in the ATM Forum PNNI 1.0 specification.

This step is repeated at each switch that receives the setup message. If CAC determines the connection cannot be made, the call will be “cranked back” up to the entry border node in that peer group and *not* to the switch which had originated the setup. It will be cranked back to the switch that originated the setup message only if the call crankback is in the same peer group as that of the originator. An alternate route will be selected for the call.

Crankback is the mechanism for releasing an in-progress connection setup due to a failure, such as a link failure or bandwidth allocation failure. *Alternate routing* is a mechanism that allows the call to be re-established on an alternate path when a setup fails.

Even if other switches earlier along the path determined the connection could be set up, the call still cranks back to the originating switch. The Path Selection computations performed in Step 3 are then repeated with knowledge of the node that could not set up the request.

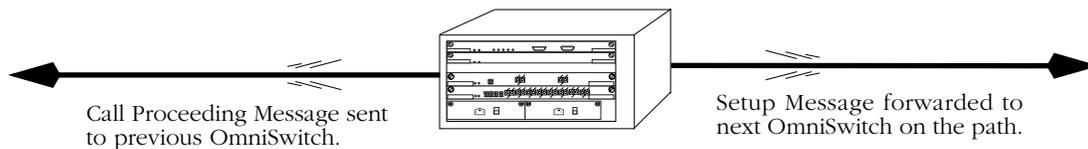


OmniSwitch Using CAC: Can the Connection Be Accepted?

Step 6. Send Call Proceeding Message

After accepting a connection request, each OmniSwitch forwards the setup message to the next hop in the path. This next switch will use its CAC to determine if it can set up the connection as described in Step 5.

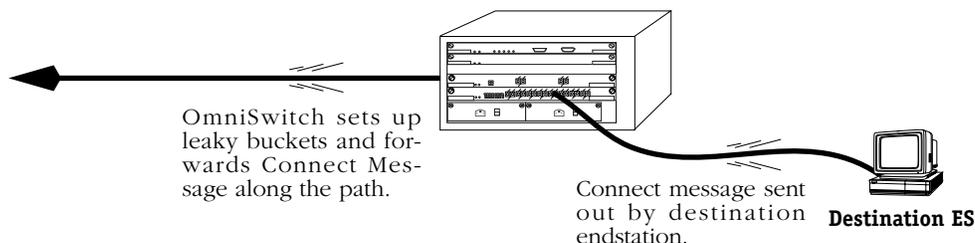
After accepting the connection request, a second message is sent backward along the path. This second message, referred to as a Call Proceeding message, goes back to the node that forwarded the call setup message. At each node along the path, a node knows whether the next node was able to set up the connection. These Call Proceeding messages continue along the ATM switches until the final node in the path forwards the final call setup message to the destination ATM end station.



Messages Forwarded to Neighboring Nodes

Step 7. Send Connect Message

After each node in the path accepts the setup message, the destination ES initiates a Connect message back to the source ES. The node to which the destination ES is attached receives this message and forwards it to the next node in the path leading to the source ES. Upon receipt of the Connect Message, a node establishes a leaky bucket algorithm according to the Class of Service and Traffic Descriptors included in the original call setup message. Leaky buckets are described in Chapter 41, “Managing Cell Switching Modules (CSMs).”



Connect Message Sent Along Path

This process continues until each node in the path receives the Connect message and sets up a leaky bucket. Finally the initial source ES receives the Connect message and prepares to send data. The connection between the source and the destination is now established end-to-end. All nodes have reserved bandwidth, set up leaky buckets, and assigned virtual circuits to support the connection.

Step 8. Data Flow

After all the virtual connections have been set up on each node along the path, the source ES begins sending data over the connection.

The PNNI Menu and Submenus

The PNNI menu contains six submenus that provide command options for configuring PNNI attributes and displaying PNNI configuration parameters and statistics. The main PNNI menu displays as shown below:

Command	ATM PNNI Menu
Pconfig	Enter the PNNI configuration submenu
Proute	Enter the PNNI route management submenu
Pinfo	Enter the PNNI information submenu
Pstats	Enter the PNNI statistics submenu
Padmin	Enter the PNNI administration submenu

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

This chapter describes the **Pconfig**, **Pinfo**, **Pstats**, **Ptest**, and **Padmin** submenus. The **Proute** submenu is described in Chapter 47, “Managing IISP and PNNI Routes.” The following sections provide a brief description of each PNNI submenu.

◆ Important Note ◆

In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. Chapter 8, “The User Interface,” includes documentation on changing from CLI mode to UI mode.

Pconfig

The **Pconfig** submenu contains options for configuring general PNNI parameters, node-level parameters, and port-level parameters. The submenu displays as shown below.

Command	ATM PNNI Configuration Menu
pgcfg	Configure PNNI general parameters
pncfg	Configure PNNI node-specific operation parameters
ppcfg	Configure PNNI port (interface) operating parameters
pndel	Remove a PNNI logical group node

Related Menus:	Pconfig	Proute	Pinfo	Pstats	Padmin
-----------------------	----------------	---------------	--------------	---------------	---------------

Descriptions of **Pconfig** submenu commands begin on page 46-32.

Proute

The **Proute** submenu contains options for configuring and monitoring PNNI static routes. The submenu displays as shown below:

Command	ATM PNNI Route Management Menu
proutea	View the Table of routes from nodes to reachable addresses
prouten	View the Table of routes to other nodes
prpadd	Add a PNNI static route property (type, metrics, TNS)
prpdel	Delete a PNNI static route property
pradd	Add PNNI static route address(es) to a route property
prdel	Delete PNNI static route address(es) from a route property
prp	View PNNI configured route properties
prt	View PNNI configured route prefixes
Related Menus:	
Pconfig	Proute
Pinfo	Pstats
Padmin	

All **Proute** submenu options are described in Chapter 47, “Managing IISP and PNNI Routes.”

Pinfo

The **Pinfo** submenu contains options for displaying PNNI general, node, and port attributes. In addition, various connections statistics are available through these commands. The submenu displays as shown below.

Command	ATM PNNI Information Menu
pginfo	View general PNNI information
pninfo	View node-specific PNNI information
ptinfo	View PNNI timer information
pnbrs	View PNNI neighbor information
ppinfo	View PNNI port information
plink	View PNNI link information
pptse	Dump PTSE database (output may be lengthy)
pdtl	View the PNNI DTL Table
padj	View end-point adjacencies reported by call control to PNNI
psmap	View PNNI scope mapping information
pmap	View the Pnni Map Table
pnpmap	View the Pnni Nodal Map Table
pcalls	View the status of ongoing PNNI calls
Related Menus:	
Pconfig	Proute
Pinfo	Pstats
Padmin	

Descriptions of **Pinfo** submenu commands begin on page 46-53. Many PNNI informational commands provide a “-s” flag option that allows you to summarize displays (see *Summary Form of PNNI Commands* on page 46-31).

◆ **Note** ◆

The **psmap** command will not display unless you are running the multiple-peer group version of PNNI.

Pstats

The **Pstats** submenu contains options for displaying port, error, and PTSE statistics. The submenu displays as shown below.

Command	ATM PNNI Statistics Menu
pgstats	View PNNI port basic statistics
pestats	View PNNI port error statistics
ppstats	View PNNI port ptse statistics

Related Menus:
Pconfig Proute Pinfo Pstats Padmin

Descriptions of **Pstats** submenu commands begin on page 46-85.

Padmin

The **Padmin** submenu contains options for bringing the PNNI protocol entity up and down and for resetting PNNI statistical counters. The submenu displays as shown below.

Command	ATM PNNI Administration Menu
phalt	Halts all PNNI operations - clears all databases
preset	Reset the PNNI interface counters
prestart	Restart the PNNI entity (from a halted state)
pvcfg	View PNNI information in the configuration file
prmcfg	Remove PNNI information from the configuration file
prtst	Route test to verify reachability to an ATM address

Related Menus:
Pconfig Proute Pinfo Pstats Padmin

Descriptions of **Padmin** submenu commands begin on page 46-90.

Summary Form of PNNI Commands

You can use the **-s** option on many PNNI display commands to display a summary form instead of a lengthy list of parameters. For example, to display the summary form of the **pnbrs** command, enter

```
pnbrs -s
```

The following PNNI commands support the summary option:

pnbrs

ppinfo

plink

pptse

pmap

pnmap

pdtl

proutea (described in Chapter 47, “Managing IISP and PNNI Routes”)

prouten (described in Chapter 47, “Managing IISP and PNNI Routes”)

Displaying PNNI Command Help (Multi-Peer Group PNNI Only)

In the multiple-peer group version of PNNI, you can display the syntax for many PNNI commands by entering the command followed by a space, hyphen (-), and the word **help**. For example, to display the syntax for the **pninfo** command, enter:

```
pninfo -help
```

The following screen will be displayed:

```
Usage: pninfo [-s | <node level>]
where -s is for summary mode and
<node level> is between 1 and 104
```

◆ Note ◆

You can abbreviate **-help** as **-h**.

Text displayed within square brackets is optional. A vertical line (|) separates mutually exclusive parameters. And a user-supplied value can be indicated “less-than” sign (<) and a “greater-than” sign (>) or by two more words written without spaces (e.g., **portld**).

You can display syntax help on all PNNI commands *except* for the following:

```
pgcfg
ppcfg
prpadd
prdel
prp
prt
padj
phalt
prestart
pvcfg
prmcfg
prtst
```

Configuring General PNNI Parameters

The **pgcfg** command allows you to configure general PNNI parameters for the local OmniSwitch. It allows you to globally enable PNNI on all CSM ports in the switch, set timers, operational limits, and the topology metrics to use for path selection computations. The values you set here apply to all CSM ports in the switch. Defaults are supplied for all parameters. You can begin configuring these parameters by entering:

pgcfg

at a system prompt. A screen similar to the following displays.

```

Modifying PNNI General Operating Parameters
(Will be defaulted to bracketed values if unspecified)

1) PNNI enabled on all interfaces configured as
   type=PNNI in the "map" and cvpt cmds (t,f) [t]:Unspecified
2) Shortest path first calc timer (seconds) [ 20]:Unspecified
3) Period at which the process to age PTSEs
   in the database is activated (seconds) [ 10]:Unspecified
4) AvCR proportional multiplier (1-99%) [50]:Unspecified
5) AvCR minimum threshold (1-99%) [ 3]:Unspecified
6) CTD proportional multiplier (1-99%) [50]:Unspecified
7) CDV proportional multiplier (1-99%) [25]:Unspecified

8) Configure Operation Limits sub-menu (for performance tuning)
9) Configure Routing Table Operation sub-menu
10) Configure Multi-Peer Group Operation sub-menu

To configure a parameter, type "item = value" (as in 1=t)
To quit out of configuration, type "quit"
To save the configured info, type "save"
-> 1=f
Note that since you've not enabled PNNI on any ports, you must
explicitly enable the ports on which PNNI is to operate by using the
ppcfg command.
-> save
Do you want these parameters to take effect immediately? (y)

```

To alter a parameter, enter the line number for the parameter, followed by an equal sign (=), and then the new value. For example, to change the **PTSE Aging Timer** (line 3) from 10 seconds to 15 seconds, you would enter:

3=15

When you have completed configuring parameters, enter **save**. Your new values will be saved and you will exit this menu. If you want to exit this menu without saving changes, simply enter **quit**.

◆ Note ◆

Option 10, **Configure Multi-Peer Group Operation sub-menu**, will not display unless you are running the multiple-peer group version of PNNI.

Options on line numbers 8, 9, and 10 enter submenus with additional configuration parameters. Simply enter the submenu's line number (8, 9, or 10) and press **<Enter>** to go to that submenu. Descriptions for the parameters under option 8 can be found in *Configuring PNNI Operation Limits* on page 46-35. Descriptions for the parameters under option 9 can be found in *Selecting Metrics Used in Path Computations* on page 46-38. Descriptions for the parameters under option 10 can be found in *Configuring Multi-Peer Group Operation* on page 46-39.

1) PNNI enabled on all interfaces configured as PNNI

Indicate whether you want to enable the PNNI routing protocol for all CSM ports in this OmniSwitch chassis that have been configured as PNNI type ports through the **map** command (see Chapter 41, “Managing Cell Switching Modules,” for information on the **map** command). You can also enable PNNI on a port-by-port basis through the **ppcfg** command. The setting configured through **ppcfg** takes precedence over the global setting you configure here. For example, if you enable PNNI here (by entering a **t**), but you disable PNNI on a specific port (through **ppcfg**), then PNNI will not run on that port. If you disable PNNI here (by entering an **f**), but enable PNNI on a specific port (through **ppcfg**), then PNNI will run on that port.

2) Shortest path first calc timer (seconds)

The time interval, in seconds, between recomputations of routes in the routing tables based on the current contents of the topology database. This timer may range from 1 to 255 seconds. Note that shorter periods increase the sensitivity and reaction time to topology changes, but also consume more switch CPU time in networks where topology changes occur frequently. The default value of 20 is sufficient for most networks of a modest size.

3) Period at which the process to age PTSEs is activated (seconds):

The time, in seconds, before the process to age PTSEs starts. When the aging process begins, PTSEs are aged out of the topology database. If a PTSE's lifetime goes to zero (0), then it will be removed. However, a PTSE may be refreshed by the originating node before this entry ages out. This timer may range from 1 to 255 seconds.

4) AvCR proportional multiplier (1..99%)

The Available Cell Rate (AVCR) Proportional Multiplier expressed as a percentage. Valid values are integers from 1 to 99. This value is used in determining what defines a significant change in the Available Cell Rate, which is a measure of the bandwidth available for each service class. The switch will measure the AVCR at the current time and at a previous time. The percent indicated here is multiplied by the previous AVCR. If the difference between the current AVCR and the previous AVCR is greater than the product of the Proportional Multiplier (i.e., this value) and the previous AVCR, then the change in AVCR will be considered significant by PNNI.

5) AvCR minimum threshold (1..99%)

The Available Cell Rate (AVCR) Minimum Threshold expressed as a percentage. Valid values are integers from 1 to 99. This value is used in computing the lowest level of significant change in the Available Cell Rate, which is the bandwidth available for each service type. The value you indicate here is multiplied by the Maximum Cell Rate to yield the minimum difference (allowed in computations) between the current AVCR and a previously measured AVCR. If the previously measured AVCR multiplied by the AVCR Proportional Multiplier (indicated on line 4 in this menu) is less than the Maximum AVCR multiplied by the value indicated here, then this value will be used in computations to determine upper and lower limits of significance in AVCR change.

6) CTD proportional multiplier (1..99%)

The Cell Transfer Delay (CTD) Proportional Multiplier expressed as a percentage. Valid values are integers from 1 to 99. This value is used in determining what defines a significant change in the Cell Transfer Delay, which is the time it takes cells to transmit across a link within a single peer group. The switch will measure the CTD at the current time and at a previous time. The percent indicated here is multiplied by the previous CTD. If the difference between the current CTD and the previous CTD is greater than the product of the Proportional Multiplier (i.e., this value) and the previous CTD, then the change in CTD will be considered significant by PNNI.

7) CDV proportional multiplier (1..99%)

The Cell Delay Variation (CDV) Proportional Multiplier expressed as a percentage. Valid values are integers from 1 to 99. This value is used in determining what defines a significant change in the Cell Delay Variation, which is a measure of “jitter” or the change in cell spacing over a given link. The switch will measure the CDV at the current time and at a previous time. The percent indicated here is multiplied by the previous CDV. If the difference between the current CDV and the previous CDV is greater than the product of the Proportional Multiplier (i.e., this value) and the previous CDV, then the change in CDV will be considered significant by PNNI.

Configuring PNNI Operation Limits

Option 8 on the main **pgcfg** configuration menu opens a submenu for fine-tuning performance and resource utilization in the local switch. The options on this submenu set limits for various PNNI attributes, such as nodes in the network, Designated Transit Lists (DTLs), and static routes. PNNI uses these values to pre-allocate storage for the related elements. When limits are set too high, memory can be wasted. If limits are set too low, then the database can become overloaded.

◆ Note ◆

If you are unsure of a limit, use the default supplied. If the default clearly does not fit your network configuration, then configure it appropriately.

The submenu displays as follows:

Modifying PNNI General Operating Limit Parameters (Will be defaulted to bracketed values if unspecified)

10) Approximate number of nodes in network	[100]:Unspecified
11) Approximate Max neighbors for this node	[30]:Unspecified
12) Approximate Max PTSEs in net	[1000]:Unspecified
13) Approximate Max Information Groups in PTSEs	[1500]:Unspecified
14) Max reachable addresses in this network	[400]:Unspecified
15) Max transit networks in this network	[50]:Unspecified
16) Max Designated Transit Lists (DTLs)	[200]:Unspecified
17) Max DTL entries	[200]:Unspecified
18) Max outstanding route requests	[500]:Unspecified
19) Max configured static routes	[300]:Unspecified
20) Max configured static route groups	[200]:Unspecified
21) Max point to multipoint endpoints	[500]:Unspecified
22) Max number of Paths	[1000]:Unspecified
23) Max number of retransmissions	[250]:Unspecified
24) Max number of entries in any routing tbl	[2000]:Unspecified

To configure a parameter, type "item = value" (as in 11=100)
 To quit out of configuration, type "quit"
 To save the configured info, type "save"
 To return to General Operating Parameters, type "return"

Operational limit parameters are described on the next two pages. Unless otherwise specified, the values for these limits may range from 1 to 1,000.

10) Max Nodes in Network

The maximum number of nodes that are allowed in this PNNI network.

11) Max neighbors

The maximum number of neighboring node connections for each switch. A good rule of thumb is to never attach more than 30 neighbors without making appropriate adjustments to the hello timers.

12) Max PTSEs

The maximum number of PTSEs that can be held in the topology database of a switch. Up to 65,535 PTSEs may exist in a switch.

13) Max Information Groups in PTSEs

The maximum number of Information Groups this switch will store in its topology state database. The switch will store up to 65,535 Information Groups.

14) Max reachable addresses in this network

The maximum number of ATM End System addresses that will be available to nodes in this PNNI network. This value may range from 1 to 65,535.

15) Max transit networks in this network

A transit network is a route used to tunnel call requests from an ATM End System in one peer group to an ATM End System in another peer group. A transit network differs from a Designated Transit List (DTL) in that it provides a route to links outside the peer group while a DTL provides a route to nodes within the same peer group. This value may range from 1 to 255.

16) Max Designated Transit Lists (DTLs)

The maximum number of Designated Transit Lists (DTLs) that may be set up through the PNNI network. A DTL is a complete source route through a peer group. This value may range from 1 to 65,535.

17) Max DTL entries

The maximum number of entries (hops) that can be used to make up a single DTL. An entire DTL includes all hops that comprise a source route through a peer group. In a single peer group, this value is the maximum path length plus 1. This value may range from 1 to 500.

18) Max outstanding route requests

The maximum number of call setup messages that can be outstanding at one time. Call setup messages are initiated by ATM End Systems. When a call setup is in progress, a call descriptor is held by PNNI until the connection is set up or the setup cranksback. This value may range from 1 to 65,535.

19) Max configured static routes

The maximum number of static routes that can be configured in the PNNI network. A static route is a vector through the network that routes to a particular class of NSAP addresses. This value may range from 1 to 10,200.

20) Max configured static route groups

The maximum number of static route groups allowed. A group of static routes is ordered by route properties. This value limits the amount of space reserved for route properties. This value may range from 1 to 255.

21) Max point to multipoint endpoints

The maximum number of multicast virtual circuits that may be configured within the PNNI network. This number is limited by the type and number of CSM modules installed. CSM-155 modules each support 8,000 multicasts, and CSM-622 modules support 16,000 multicasts.

22) Max number of Paths

The maximum number of paths that may be stored in this switch. A path is a physical connection between two switches.

23) Max number of retransmissions

PTSE requests and PTSEs will be retransmitted this number of times before PNNI declares that the neighboring node is down. This value may range from 1 to 255.

24) Max number of entries in any routing tbl

The maximum number of routing table entries. This value may range from 1 to 65,535.

Selecting Metrics Used in Path Computations

Option 9 on the main **pgcfg** configuration menu opens a submenu for configuring the Routing Table. These submenu options allow you to choose the topology metric on which each Class of Service will be sorted. Each Class of Service can be sorted on Administrative Weight, Cell Transfer Delay (CTD), or Cell Delay Variation (CDV). The submenu displays as follows:

Modifying PNNI Routing Table Configuration

This sub-menu allows a user to configure a PNNI routing table. When the next route calculation executes, a routing table will be generated for the configured quality of service on the metric specified. Note that there may be only one metric per QOS specified. (The default metric in brackets will be used if the value is unspecified.)

Valid metric values are:

Admin Weight: **AW**
Cell Transit Delay: **CTD**
Cell Delay Variation: **CDV**

25) QOS Class CBR sorted on Metric	[AW]:Unspecified
26) QOS Class rt-VBR sorted on Metric	[AW]:Unspecified
27) QOS Class nrt-VBR sorted on Metric	[AW]:Unspecified
28) QOS Class ABR sorted on Metric	[AW]:Unspecified
29) QOS Class UBR sorted on Metric	[AW]:Unspecified

To configure a parameter, type "item = value" (as in 26=AW)

To quit out of configuration, type "quit"

To save the configured info, type "save"

To return to General Operating Parameters, type "return"

25) QOS Class CBR sorted on Metric

The metric on which Constant Bit Rate (CBR) traffic will be sorted during path selection computations. CBR traffic can be sorted by Administrative Weight (AW), Cell Transfer Delay (CTD), or Cell Delay Variation (CDV). The default metric is Administrative Weight.

26) QOS Class VBR-RT sorted on Metric

The metric on which real-time Variable Bit Rate (VBR-RT) traffic will be sorted during path selection computations. VBR-RT traffic can be sorted by Administrative Weight (AW), Cell Transfer Delay (CTD), or Cell Delay Variation (CDV). The default is Administrative Weight.

27) QOS Class VBR-NRT sorted on Metric

The metric on which non-real-time Variable Bit Rate (VBR-NRT) traffic will be sorted during path selection computations. VBR-NRT traffic can be sorted by Administrative Weight (AW), Cell Transfer Delay (CTD), or Cell Delay Variation (CDV). The default is Admin Weight.

28) QOS Class ABR sorted on Metric

The metric on which Available Bit Rate (ABR) traffic will be sorted during path selection computations. ABR traffic can be sorted by Administrative Weight (AW), Cell Transfer Delay (CTD), or Cell Delay Variation (CDV). The default metric is Administrative Weight.

29) QOS Class UBR sorted on Metric

The metric on which Unspecified Bit Rate (UBR) traffic will be sorted during path selection computations. UBR traffic can be sorted by Administrative Weight (AW), Cell Transfer Delay (CTD), or Cell Delay Variation (CDV). The default metric is Administrative Weight.

Configuring Multi-Peer Group Operation

Option 10 on the main **pgcfg** configuration menu opens a submenu for configuring Multi-Peer Group PNNI operation. These submenu options allow you to configure a node for operation as a Logical Group Node (LGN). The submenu displays as follows:

Modifying PNNI Multi-Peer-Group Operating Parameters
(Will be defaulted to bracketed values if unspecified)

31) Interval for initiating SVC-RCC (secs) [1]:Unspecified

The following are for all LGN levels operating within this switch:

32) Max RCC expected to be established [200]:Unspecified

33) Max LGN Hor Links expected to be advertised [100]:Unspecified

34) Max DTL Hops [50]:Unspecified

To configure a parameter, type "item = value" (as in 31=10)

To quit out of configuration, type "quit"

To save the configured info, type "save"

To return to General Operating Parameters, type "return"

:

Multi-peer group (MPG) operation parameters are described below. Options 32, 33, and 34 are used to set Logical Group Node (LGN) parameters for the local OmniSwitch only.

31) Interval for initiating SVC-RCC (secs)

Enter the maximum amount of time (in seconds) to establish a Switched Virtual Circuit (SVC) Routing Channel Connection (RCC). This value can be from 1 to 1800 seconds (the default is 1 second). SVC-RCCs are used to route PNNI management information, such as PNNI Topology State Packets (PTSPs) and Database Summary packets.

32) Max RCC expected to be established

Enter the maximum amount of Routing Channel Connections (RCCs) for this OmniSwitch. This value can be from 1 to 1000 (the default is 200). Switched Virtual Circuit (SVC)-RCCs are used to route PNNI management information, such as PNNI Topology State Packets (PTSPs) and Database Summary packets.

33) Max LGN Hor Links expected to be advertised

Enter the maximum number of horizontal links to Logical Group Nodes (LGNs) to be advertised by this node. This value can be from 1 to 1000 (the default is 100).

34) Max DTL Hops

Enter the maximum number of Designated Transit List (DTL) hops in this node. This value can be from 1 to 1000 (the default is 50).

Configuring Node-Specific Parameters

The **pncfg** command allows you to configure node-level PNNI parameters. It allows you to set the ATM address, PNNI node level, and administrative status of this node. In addition, you can configure several refresh timers for PTSE exchanges and the Hello protocol. The values you set here apply to all CSM ports in the OmniSwitch. Defaults are supplied for all parameters.

The **pncfg** command operates somewhat differently between the single-peer group version of the software and the multiple-peer group version of the software. For descriptions of the multiple-peer group version of the **pncfg** command, see *Configuring Multiple-Peer Group Nodes* on page 46-45. For the single-peer group version of the **pncfg** command, see the section below.

Configuring Single-Peer Group Nodes

You can begin configuring node-specific parameters in the single-peer group version of the software by entering:

```
pncfg
```

at a system prompt. A screen similar to the following displays.

```

      ATM PNNI Node-specific Configuration
      (Will be defaulted to bracketed values if unspecified)

1) ATM address of this node(hex)      :Unspecified
   [3903488001bc9000010178aee00020da78aee000]
2) Node ID (without level and rsvd)   :Unspecified
   [3903488001bc9000010178aee00020da78aee000]
3) Local node level                   [80]:Unspecified
4) Admin status (up,down)             [up]:Unspecified

5) Advertise Addr. summary(t,f)      [t]: Unspecified
6) Summary address for ILMI clients  : Unspecified
   [3903488001bc90000178aee0]

7) Timer configuration sub-menu

      To configure a parameter, type "item = value" (as in 3=100)
      To quit out of configuration, type "quit"
      To save the configured info, type "save"
-> 2=3903488001bc9000010178aeb10020da78aeb100
-> ?
```

To alter a parameter, enter the line number for the parameter, followed by an equal sign (=), and then the value for the parameter. For example, to enter an ATM address for the node, you might enter:

```
1=41000700040011223344556677080a1100000100
```

When you have completed configuring parameters, enter **save**. Your new values will be saved and you will exit this menu. If you want to exit this menu without saving changes, simply enter **quit**.

Line number 7 enters a submenu for configuring PTSE and Hello protocol timers. Simply enter **7** and press **<Enter>** to go to this submenu. Parameters for option 7 can be found in *Configuring PTSE and Hello Timers* on page 46-42.

1) ATM address of this node (hex)

The 20-byte ATM address for this node. Other nodes in the network that need to exchange PNNI protocol packets with this node will direct those packets to this address. The default ATM node address is

3903488001bc90000101xxyzz0020daxxyzz00

where **xxyzz** is the Alcatel-specific OID for the MPM in this chassis. This parameter can only be configured on a lowest-level node.

2) Node ID (without level and rsvd)

The Node ID for this node. The Node ID is a 22-octet identifier for a node within the PNNI network. Do not include the node level or other reserved characters in this specification. Include only the last 20-bytes of the Node ID. This parameter can only be configured on a lowest-level node.

3) Local Node Level

The level within the PNNI hierarchy where this node exists. This attribute is used to determine the default Node ID and the default Peer Group ID for this node. This value may only be set when the node's Admin Status is down. PNNI levels range from 0 to 104. The default node level is 80 in decimal notation. Lower values are higher in the hierarchy than higher values.

In a single peer group network, all nodes in the PNNI network will have the same node level.

4) Admin Status

Indicates the Administrative Status of this node. The default is **Up**, which means that the node can become operationally active and participate in PNNI protocol exchanges. If set to **Down**, then the node will be inactive and not participate in PNNI protocol exchanges.

5) Advertise Addr. summary

Indicate whether you want this node to use summarization when advertising the addresses of attached devices to other PNNI nodes. Using address summarization to advertise internal reachability speeds PNNI database searches. If a node does not support address summarization, then it will advertise the entire local address of its attached devices during PNNI exchanges. This parameter can only be configured on a lowest-level node.

6) Summary address for ILMI clients

Required only if you turn on address summarization in line 5. Enter the summary address that will be used to advertise all devices attached to this node. This parameter can only be configured on a lowest-level node. See *Summary Addresses* on page 46-14 for more information on summary addresses.

Configuring PTSE and Hello Timers

Option 7 on the main **pnconf** configuration menu opens a submenu for configuring PTSE and Hello protocol timers. These submenu options set parameters for how PTSE, Database Summary, and Hello packets are transmitted, re-transmitted, and acknowledged. In the single-peer group version of the software, the submenu displays as shown below:

ATM PNNI Lowest Level Node Timer Configuration
(Unspecified attributes assume the value in [] during operation)

- 8) PTSE timers:
 - a) Refresh interval (self-orig ptses) [1800]:Unspecified
 - b) Lifetime factor (multiples of a) [2]:Unspecified
 - c) Hold down (in seconds) [1]:Unspecified
 - d) Delayed ack timer [1]:Unspecified
- 9) PTSP transmit timer [10]:Unspecified
- 10) Timer to Xmit PTSPs in resp to incoming PTSE requests [1]:Unspecified
- 11) Db summary re-transmit time (if unack'd) [3]:Unspecified
- 12) Hello timers:
 - a) Hello interval (seconds: 1-255) [15]:Unspecified
 - b) Hold down interval (in seconds) [3]:Unspecified
 - c) Inactivity factor (multiples of a) [5]:Unspecified

To configure a parameter, type "item = value" (as in 9a=2000)
To quit out of configuration, type "quit"
To save the configured info, type "save"
To return to Node Config Menu, type "return"

In the multiple-peer group version of the software, the submenu displays as shown below:

ATM PNNI Lowest Level Node Timer Configuration
(Unspecified attributes assume the value in [] during operation)

- 9) PTSE timers:
 - a) Refresh interval (self-orig ptses) [1800]:Unspecified
 - b) Lifetime factor (multiples of a) [2]:Unspecified
 - c) Hold down (in seconds) [1]:Unspecified
 - d) Delayed ack timer [1]:Unspecified
- 10) PTSP transmit timer [10]:Unspecified
- 11) Timer to Xmit PTSPs in resp to incoming PTSE requests [1]:Unspecified
- 12) Db summary re-transmit time (if unack'd) [3]:Unspecified
- 13) Hello timers:
 - a) Hello interval (seconds: 1-255) [15]:Unspecified
 - b) Hold down interval (in seconds) [3]:Unspecified
 - c) Inactivity factor (multiples of a) [5]:Unspecified
- 14) PGL Timers :
 - a) PGL Init Timer [15]:Unspecified
 - b) PGL Override Timer [30]:Unspecified

To configure a parameter, type "item = value" (as in 9a=2000)
To quit out of configuration, type "quit"
To save the configured info, type "save"
To return to Node Config Menu, type "return"

◆ Note ◆

The option number for the PTSE and hello timer configuration submenu and all of its suboptions is one (1) number higher in the multiple-peer group version of PNNI, due to the addition of option 7 (**PGL Priority**), which is described in 7) *PGL Priority* on page 46-46.

8) PTSE Timers

a) Refresh interval

The time, in seconds, before a self-originated PTSE is updated. PTSEs are aged out of the database unless refreshed by the originating node. The lifetime of a PTSE is determined by multiplying the Refresh Interval by the Lifetime Factor (specified in line 9b). The range for this value is 1 to 32,767 seconds. The default value is 1800 seconds.

b) Lifetime factor (multiples of a)

The value for the PTSE lifetime multiplier. The Refresh Interval (specified in line 9a) multiplied by the Lifetime Factor determines the initial lifetime of a PTSE in the topology database. Valid values are integers ranging from 1 to 255. The default value is 2.

c) Holddown (in seconds)

The minimum time, in seconds, before which this node can refresh PTSEs. A node can prevent a PTSE from aging out of the topology database by refreshing it. This Holddown value limits the node from refreshing PTSEs too often and exhausting database space too quickly. The range for this value is from 1 to 255 seconds. The default value is 1 second.

d) Delayed ack timer

When a node receives a PTSE from another node it sends back an Acknowledgment Packet. However, the acknowledgment is not immediate. The amount of time between the receipt of a PTSE and its acknowledgment is the value you enter here. The range is from 1 to 255 seconds.

9) PTSP transmit timer

PTSPs are sent until they are acknowledged by neighboring nodes. This variable is the amount of time, in seconds, between successive transmissions of PTSPs. If a PTSP is acknowledged before the time interval specified here, then a retransmission will not be sent. This value may range from 1 to 255 seconds.

10) Timer to Xmit PTSPs in resp to incoming ptse request

The time interval between the receipt of Database Summary packets and the sending of PTSE Request packets. Database Summary packets contain an index of the PTSEs in a node's topology database. Other nodes use Database Summary packets to request PTSEs. If a node requires a PTSE listed in a Database Summary packet, then it requests that PTSE in the form of a PTSE Request packet. This value may range from 1 to 255 seconds.

11) Db summary re-transmit time

The time, in seconds, before this node will re-transmit a Database Summary packet that has gone unacknowledged by another node. This value may range from 1 to 255 seconds.

12) Hello timers

a) Hello interval

The initial value for the Hello timer in seconds. In the absence of triggered Hellos, this node will send one Hello packet on each of its ports at the interval specified here. The default Hello Interval is 15 seconds. Values can range from 1 to 255 seconds.

b) Hold down interval

The initial value for the Hello hold down timer. This node will use this value to limit the rate at which it sends Hello messages. The default value is 3 seconds. Valid values range from 1 to 255 seconds.

c) Inactivity factor

The number of Hello intervals that may pass without receiving a Hello before the neighboring node is determined to have gone down. The default is 5. Valid values range from 1 to 255.

◆ Note ◆

Option 14 (**PGL Timers**) will not appear unless you have installed the software for multiple-peer group PNNI.

14) PGL Timers

a) PGL Init Timer

The amount of time (in seconds) this node will delay advertising its choice of preferred PGL after having initialized operation and reached the full state with at least one neighbor in the peer group.

b) PGL Override Timer

The amount of time (in seconds) a node will wait for itself to be declared the preferred PGL by unanimous agreement among its peers. In the absence of unanimous agreement, it will abandon the attempt to get unanimous agreement and this will be the amount of time that will pass before this node considers a 2/3 majority as sufficient agreement to declare itself peer group leader.

Configuring Multiple-Peer Group Nodes

You can begin configuring node-specific parameters in the multiple-peer group version of the software by entering:

```
pncfg
```

at a system prompt. A screen similar to the following displays.

```

      ATM PNNI Node-specific Configuration
      (Will be defaulted to bracketed values if unspecified)

1) ATM address of this node(hex)      :Unspecified
   [3903488001bc9000010178aee00020da78aee000]
2) Node ID (without level and rsvd)   :Unspecified
   [3903488001bc9000010178aee00020da78aee000]
3) Local node level                   [80]:Unspecified
4) Admin status (up,down)             [up]:Unspecified

5) Advertise Addr. summary(t,f)      [t]: Unspecified
6) Summary address for ILMI clients   : Unspecified
   [3903488001bc90000178aee0]

7) PGL Priority                       [50]:Unspecified
8) Timer configuration sub-menu

      To configure a parameter, type "item = value" (as in 3=100)
      To quit out of configuration, type "quit"
      To save the configured info, type "save"
-> 2=3903488001bc9000010178aeb10020da78aeb100
-> ?

```

To alter a parameter, enter the line number for the parameter, followed by an equal sign (=), and then the value for the parameter. For example, to enter an ATM address for the node, you might enter:

```
1=41000700040011223344556677080a1100000100
```

When you have completed configuring parameters, enter **save**. Your new values will be saved and you will exit this menu. If you want to exit this menu without saving changes, simply enter **quit**.

See *Configuring Single-Peer Group Nodes* on page 46-40 for descriptions of Options 1 (**ATM address of this node**) through 6 (**Summary address for ILMI clients**). Line number 7 (**PGL Priority**) is described in *7) PGL Priority* on page 46-46. Line number 8 enters a submenu for configuring PTSE and Hello protocol timers. Simply enter **8** and press **<Enter>** to go to this submenu. Parameters for option 8 can be found in *Configuring PTSE and Hello Timers* on page 46-42.

◆ Note ◆

The option numbers for the timer configuration submenu and all of its suboptions are one (1) number higher in the multiple-peer group version of PNNI, due to the addition of option 7 (**PGL Priority**), which is described on the following page.

In addition, Peer Group Leader (PGL) nodes have some additional parameters, which are described in *Configuring Peer Group Leader Nodes* on page 46-46. And see *Configuring the Peer Group Leader Election Process on All Node Levels* on page 46-48 for configuration steps for the PGL election process on all node levels.

7) PGL Priority

The Peer Group Leader (PGL) priority for this node. You can use this parameter to configure which node will become the primary leader, secondary backup leader, etc. in a peer group. Lower values have lower priority than higher values. The PGL node will commence Logical Group Node (LGN) operation. You can enter a value from 0 to 205.

Any node within a peer group can be the PGL. A border node may or may not be the PGL.

◆ Note ◆

The PGL of any level must be the PGL of all descendent (child) levels.

Configuring Peer Group Leader Nodes

There are additional parameters in the **pncfg** command when you configure a Peer Group Leader of a Logical Group Node. On these nodes, a screen similar to the following will be displayed when you execute the **pncfg** command.

ATM PNNI Lowest Level Node-specific Configuration (Will be defaulted to bracketed values if unspecified)

- 1) ATM address of this node(hex) :Unspecified
[3903488001bc9000010178aee00020da78aee000]
- 2) Node ID (without level and rsvd) :Unspecified
[3903488001bc9000010178aee00020da78aee000]
- 3) Local node level [80]:Unspecified
- 4) Admin status (up,down) [up]:Unspecified

- 5) Advertise Addr. summary(t,f) [t]: Unspecified
- 6) Summary address for ILMI clients : Unspecified
[3903488001bc90000178aee0]

- 7) PGL Priority [50]: Unspecified
- 8) Complex Representation(t,f) [f]: f
- 9) Timer configuration sub-menu

To configure a parameter, type "item = value" (as in 3=100)
To quit out of configuration, type "quit"
To save the configured info, type "save"
-> 2=3903488001bc9000010178aeb10020da78aeb100
-> ?

These additional parameters are described below.

◆ Note ◆

The option numbers in the Timer configuration submenu (*see following page*) and all of its suboptions are one (1) number higher, due to the addition of option 8 (**Complex Representation**), described below.

8) Complex Representation(t,f)

The complex node representation is the process of representing a child peer group by a logical node in its parent peer group. Set this parameter to **t** (true) to activate complex node representation. If you set this parameter to **f** (the default), then simple node representation will be implemented where the nodal state parameter PTSEs from this node will not be used in route computations. See *Complex Representation* on page 46-10 for more information.

9) Timer configuration sub-menu

When you enter the timer configuration (now Option 9) on a Peer Group Leader of a Logical Group Node, a screen similar to the following will be displayed:

ATM PNNI Lowest Level Node Timer Configuration
(Unspecified attributes assume the value in [] during operation)

- 10) PTSE timers:
 - a) Refresh interval (self-orig ptses) [1800]:Unspecified
 - b) Lifetime factor (multiples of a) [2]:Unspecified
 - c) Hold down (in seconds) [1]:Unspecified
 - d) Delayed ack timer [1]:Unspecified
- 11) PTSP transmit timer [10]:Unspecified
- 12) Timer to Xmit PTSPs in resp to incoming PTSE requests [1]:Unspecified
- 13) Db summary re-transmit time (if unack'd) [3]:Unspecified
- 14) Hello timers:
 - a) Hello interval (seconds: 1-255) [15]:Unspecified
 - b) Hold down interval (in seconds) [3]:Unspecified
 - c) Inactivity factor (multiples of a) [5]:Unspecified
- 15) LGN Specific Timers:
 - a) SVCC calling interval timer [35]:35
 - b) SVCC called interval timer [50]:50
 - c) Horizontal link inactive timer [75]:75

To configure a parameter, type "item = value" (as in 9a=2000)
 To quit out of configuration, type "quit"
 To save the configured info, type "save"
 To return to Node Config Menu, type "return"

For descriptions of Option 10 (**PTSE timers**) through Option 14 (**Hello Timers**), see *Configuring PTSE and Hello Timers* on page 46-42. Option 15 (**LGN Specific Timers**) is described below.

15) LGN Specific Timers

a) SVCC calling interval timer

The Switched Virtual Circuit Channel Connection (SVCC) interval timer for this node in seconds. An SVCC is a routing control channel between logical group nodes. This parameter sets the maximum amount time that a calling LGN should wait before restarting the process of establishing an SVCC-based Routing Control Channel (RCC). Values can range from 1 to 65535 seconds. (The default is 35 seconds.)

b) SVCC called interval timer

Enter the Switched Virtual Circuit Channel Connection (SVCC) interval timer for this node. An SVCC is a routing control channel between logical group nodes. This parameter sets the maximum amount time that a called LGN should wait for an SVCC-based Routing Control Channel (RCC) to be established. Values range from 1 to 65535 seconds. (The default is 50 seconds.)

c) Horizontal link inactive timer

The horizontal link inactive timer for this node in seconds. This parameter determines the interval a node should wait to re-establish a horizontal link with a neighboring peer group after no Hello packets have been received from that neighboring node. data between neighboring peer groups. Valid values range from 1 to 65535 seconds. (The default is 75 seconds.)

Configuring the Peer Group Leader Election Process on All Node Levels

Follow the steps below to configure the Peer Group Leader (PGL) election process on all node levels in multiple-peer group networks.

1. Enter:

pncfg

at the system prompt.

2. Enter **3=** followed by the node level. For example, to set the node level to 88, enter:

3=88

at the **pncfg** prompt.

3. Enter any other parameters. (See *Configuring Multiple-Peer Group Nodes* on page 46-45 for the **pncfg** options.) When you are finished, enter:

save

at the **pncfg** prompt to save your settings.

4. You must now configure this node to participate in the PGL election process for its own node level. To do this, enter **pncfg** followed by the node level of this node minus an integer greater than or equal to 1. For example, to allow a node at level 88 to participate in the PGL election for node level 88, you can enter:

pncfg 80

at the system prompt. (The number 8 was used here because it will configure node level differences corresponding to octets.)

5. Enter any other parameters. When you are finished, enter:

save

at the **pncfg** prompt to save your settings.

6. You must now configure this node to participate in the PGL election process for all higher-level (lower-numbered) nodes. To do this, enter **pncfg** followed by the node level minus an integer greater than or equal to 1 for each level. For example, to allow a node at level 88 to participate in the PGL election for node levels 80 and 72, follow the steps below.
 - a. Enter:
pncfg 72
at the system prompt.
 - b. Enter any other parameters. When you are finished, enter:
save
at the **pncfg** prompt to save your settings
 - c. Enter:
pncfg 64
at the system prompt.
 - d. Enter any other parameters. When you are finished, enter:
save
at the **pncfg** prompt to save your settings.

Configuring Port Parameters

The **ppcfg** command allows you to configure port-level PNNI parameters. It allows you to enable PNNI on a port and configure metrics for each ATM traffic type supported on the port. (Before PNNI can be enabled on a port, the port must be configured as a PNNI type port through the **map** command, which is described in Chapter 41, "Managing Cell Switching Modules.") You can begin configuring PNNI port parameters by entering

```
ppcfg <slot>/<port>
```

at a system prompt. For example, if you wanted to configure PNNI for port 1 on the CSM module in slot 5, then you would enter:

```
ppcfg 5/1
```

You could also configure multiple ports at one time by specifying a port list after the slot number. For example, you could configure ports 1 and 2 on the CSM module in slot 5 by specifying:

```
ppcfg 5/1-2
```

Virtual Path Tunnels. To configure PNNI parameters for a specific virtual path tunnel, you need to include the instance number of the virtual tunnel in the **ppcfg** command. (Physical level parameters for virtual tunnels are configured through the **cvpt** command, which is described in Chapter 42, "Advanced CSM Management.") The **ppcfg** format for virtual path tunnels is as follows:

```
ppcfg <slot>/<port>/<virtual tunnel instance>
```

where **<virtual tunnel instance>** is a unique value assigned to each virtual tunnel on a CSM module port. You can find a specific virtual tunnel instance through the **lvpt** command. If you wanted to configure PNNI parameters for the second virtual tunnel instance on third port on the CSM module in slot 4, you would specify:

```
ppcfg 4/3/2
```

The following is a sample display for the **ppcfg** command.

```

      Modifying PNNI/AAL Operating/Advertisement Parameters for slot 5 port 1:
1) PNNI enabled on this port (t,f)      [t]:Unspecified
2) VPI                                  [0]:Unspecified
3) VCI                                  [18]:Unspecified

      Admin Weight   Cell Transfer Delay   Cell Delay Variance
      (a)[5040]      (b)                (c)
      (Disable a class by assigning an admin weight to 0)
4) CBR               Disabled
5) rt-VBR            Disabled
6) nrt-VBR           Disabled
7) ABR               Disabled
8) UBR               Disabled

To set a value, type "item=value" (as in 1=y);
To cancel this and move on to the next port, type "next";
To quit out of configuration, type "quit";
To save this port information and move on to the next port, type "save".
-> 1=t
-> save
Do you want these parameters to take effect immediately? (y)
Done.
```

1) PNNI enabled on this port

Indicates whether PNNI is enabled on this port. If PNNI is enabled on all ports through the **pgcfg** command, then this value will already be set to **Yes** (enabled). This value overrides the value set through **pgcfg**. If PNNI is enabled on all ports, you can disable it on this port by setting this value to **No**. If this field is set to **No**, then all other parameters on this screen will not display.

In release 4.1 and later, you should not disable ILMI since ILMI will be running across all ATM links unless it has been explicitly disabled. In releases prior to 4.1, you should disable ILMI—through the **map** command—on a PNNI port.

2) VPI

The default Virtual Path Identifier (VPI) that will be used to transmit PNNI routing messages. This VPI will not be available for data connections. This Virtual Path is also referred to as the Routing Control Channel (RCC). If you are configuring a virtual tunnel, then you will need to specify this VPI value through the **cvpt** command, not in this field. Values may range from 0 to 255. The default is 0.

3) VCI

The default Virtual Channel Identifier (VCI) that will be used to transmit PNNI routing messages within each Virtual Path. This VCI will not be available for data connections. This Virtual Channel is also referred to as the Routing Control Channel (RCC). Values may range from 1 to 65,536. The default is 18.

4-8) Metrics

You can configure three metrics for each class of ATM traffic. These configurable metrics are Administrative Weight, Cell Transfer Delay (CTD), and Cell Delay Variation (CDV).

To configure these metrics, first enter the number for the Class of Service, then the letter corresponding to the metric you want to configure, an equal sign (=), and finally the value for the metric. For example, if you wanted to assign an Administrative Weight of **3200** to the CBR traffic class, then you would enter:

4a=3200

The three configurable metrics are described below. PNNI also uses a number of topology attributes for connections, but these attributes are not user-configurable; PNNI reads topology attributes directly from the switch fabric. See *Metrics and Attributes* on page 46-16 for further information.

a) Admin Wt

You enable a class of traffic by assigning an Administrative Weight to it. The Administrative Weight indicates the preference of a given link relative to other links. Lower values have a higher priority than higher values.

b) Cell Transfer Delay

The time it takes for cells to transmit across a link within a single peer group.

c) Cell Delay Var

Also referred to as “jitter,” this metric is the change that occurs in cell spacing from the time cells leave one node and arrive at another node.

◆ Note ◆

The Maximum Transmission Unit (MTU) is set to a constant 8192 bytes and cannot be altered.

Viewing General PNNI Information

The `pginfo` command displays several current configuration values as well as statistics on connections. When you enter

```
pginfo
```

a screen similar to the following displays:

```

                        ATM PNNI General Information

Nodes in this switch:      1      Neighbors detected:      5
PNNI highest version supported: 1      Lowest version:          1
Node routing database size: 7      Address database size:   10
PTSEs in database:        24     RCCS in database:        5

Times SPF executed:       5

Pt to Pt calls in progress: 13     Pt to MultiPt calls in prog: 11
Conns cranked back to this sys: 0     Conns cranked from border:  0
DTL stacks in use:        24     DTL Stacks Free:          176
Total DTL stacks originated: 453    Total DTL borders originated: 0
Alt DTLs originated:      0      Alt border DTLs originated: 0

Route failures:           13     Border failures:          0
Route unreachable errs:   0      Border unreachable errs:   0
PNNI AAL Discards:        0

Max Concurrent Pt-Mpt Calls 500

```

Nodes in this switch. The number of instances of the PNNI protocol within this OmniSwitch. In a single peer group network, only one instance of PNNI, or node, can exist in a single OmniSwitch.

Neighbors detected. The number of neighboring nodes attached to this node. Neighbor nodes are physically connected to this node via a CSM port.

PNNI highest version supported. The highest version of the PNNI protocol that the software in this OmniSwitch is capable of executing. The current release supports PNNI version 1.0.

Lowest version. The lowest version of the PNNI protocol that the software in this OmniSwitch is capable of executing.

Node routing database size. The current number of valid pre-calculated PNNI routes to nodes.

Address database size. The current number of valid PNNI routes from nodes in this PNNI routing domain to exterior ATM addresses and transit networks.

PTSEs in database. The total number of PNNI Topology State Elements (PTSEs) in this node's topology database. PTSEs and the topology database are discussed in *PNNI Network Initialization* on page 46-19 and *Establishing a Connection* on page 46-22.

RCCS in database. The number of Routing Control Channels (RCCs) currently in the database. RCCs are used to route PNNI management information, such as PNNI Topology State Packets (PTSPs) and Database Summary packets.

Times SPF executed. The number of times the Shortest Path First (SPF) algorithm has been executed to compute paths for call connections.

Pt to Pt calls in progress. The number of point-to-point calls that are being set up right now. Once a call has been set up it will not be included in this count.

Pt to Multi-Pt calls in prog. The number of point-to-multipoint calls that are being set up right now. Once a call has been set up it will not be included in this count.

Conns cranked back to this sys. The total number of connection setup messages, including DTL stacks originated by this node, that have cranked back to this node at all levels of the PNNI hierarchy. Connection setups will crankback when one node along the pre-computed path is not able to set up the connection due to bandwidth, Quality of Service, or other considerations.

Conns cranked from border. The total number of connection setup messages, including DTLs by this node as an entry border node, that have cranked back to this node at all levels of the PNNI hierarchy. This value does not include crankbacks for which this node was not the crankback destination. It includes only those crankbacks that were directed to this node. In a single peer group network, this value will be 0.

DTL stacks in use. The number of Designated Transit Lists (DTLs) that are in use right now to set up point-to-point and point-to-multipoint PNNI calls. If no calls are being set up, then this field will read zero (0).

DTL Stacks Free. The number of Designated Transit List (DTLs) that are available to set up PNNI calls. This value does not indicate how many DTLs are in use; it indicates the number of DTLs in the PNNI database that may be put to use for settings up calls.

Total DTL stacks originated. The total number of DTL stacks that this OmniSwitch has originated and placed into signalling messages. This value includes the initial DTL stacks computed by this node as well as any alternate DTL routes (second, third choice, etc.) computed in response to crankbacks.

Total DTL borders originated. The number of partial DTL stacks that this OmniSwitch has added into signalling messages as an entry border node. This includes the initial partial DTL stacks computed by this system as well as any alternate route (second, third choice, etc.) partial DTL stacks computed by this node in response to crankbacks. In a single peer group network, this value will be 0.

Alt DTLs originated. The total number of alternate DTL stacks that this node has computed and placed into signalling messages as the DTL Originator.

Alt Border DTLs originated. The total number of alternate partial DTL stacks that this node has computed and placed into signalling messages as an entry border node. In a single peer group network, this value will be 0.

Route failures. The number of times this node failed to compute a viable DTL as the originator of a call. This value further indicates the number of times a call was cleared from this node due to originator routing failure.

Border failures. The number of times this node failed to compute a viable partial DTL stack as an entry border node for a call. This value indicates the number of times a call was either cleared or cranked back from this node due to border routing failure. In a single peer group network, this value will be 0.

Route unreachable errs. The total number of times this node failed to compute a viable DTL stack as the DTL originator because the destination was unreachable (i.e., those calls that are cleared due to an unreachable transit network or destination).

Border unreachable errs. The number of times this node failed to compute a viable partial DTL stack as an entry border node because the target of the path calculation was unreachable (i.e., those calls that are cleared are cranked back due to an unreachable transit network or destination). In a single peer group network, this value will be 0.

PNNI AAL Discards. An indicator of congestion-related problems. This value should always be zero (0).

Max Concurrent Pt-Mpt Calls. The maximum number of point-to-multipoint calls that this switch can support.

If this is not a lowest-level node (i.e., it is an LGN), then the Node ID is as follows: the first octet equals the node level within the PNNI hierarchy, the next 14 octets equal the Peer Group ID for the Peer Group Leader (PGL) node connected to this LGN, the next six octets equal the End System Identifier (ESI) of the physical switch implementing this LGN functionality, and the last octet equals zero.

◆ Note ◆

In a single peer group network, the Node ID is computed using the lowest-level node convention.

ATM address of this Node. This node's ATM address. Remote systems must direct packets or calls to this address to exchange PNNI protocol packets with this node.

Node level. The level within the PNNI hierarchy where this node exists. This value may range from 0 to 104 with higher values indicating nodes lower in the PNNI hierarchy. This level is used to determine the default node ID and the default peer group ID for this node. The default node level is 80 decimal. In single peer group operation, all nodes will be at the same level.

Peer group ID. The peer group identifier of the peer group to which this node will become a member. The default value of this ID is as follows: the first octet is the level within the PNNI hierarchy where nodes in this peer group are located and the next 13 octets are the prefix for the ATM End System Address of the node.

PNNI node index. The value assigned to this node to identify itself to SNMP management software.

Administrative status. Indicates the Administrative Status of this node. **ENABLED** means that the node is allowed to become operationally active and participate in PNNI protocol exchanges. **DISABLED** means the node will be inactive and not participate in PNNI protocol exchanges.

Operational status. Indicates whether this node is active (**UP**) or whether it has become non-operational (**DOWN**). When **DOWN**, all state information is cleared from the node and the node is not communicating with any of its neighbor nodes.

Lowest level node. Indicates whether this node acts as a lowest-level node or whether it is a Logical Group Node (LGN) that becomes active when one of the other nodes in this peer group becomes a Peer Group Leader (PGL). A value of **False** indicates nodes that are capable of becoming Logical Group Nodes. In a single peer group network, all nodes will be lowest-level nodes and this value will be **True**.

Restricted transit. Indicates whether this node is restricted from supporting Switched Virtual Circuits (SVCs) transversing this node. **False** means this node can support ATM data links transversing this node for another destination. **True** means this node will be restricted from setting up SVCs unless overridden by another PNNI parameter.

Complex representation. Specifies whether this node uses complex node representation. **True** indicates complex representation is used. **False** indicates that simple node representation is used.

Restricted branching. Indicates whether the originating node is able to support additional multicast virtual circuit branches. **False** means that the node can support additional multicast branches. **True** means that additional branches are not supported because the maximum number of multicast virtual circuits on all modules in the node has been reached. The maximum number of multicast virtual circuits supported by a CSM-155 module is 8000, and the maximum supported by a CSM-622 module is 16,000.

Address summarization. Indicates whether this node uses summarization when advertising the addresses of attached devices to other PNNI nodes. Using address summarization to advertise internal reachability speeds PNNI database searches.

Summary address. The summary address that will be used to advertise all devices attached to this node. The summary address is the only address advertised, reducing the PNNI database size and the amount of information exchanged in PTSEs. This address prefix is also used by ILMI when registering clients.

◆ **Note** ◆

The following fields only apply to the multiple-peer group version of PNNI.

PGL Priority. The leadership priority value advertised by the local node. In the election process to determine the PGL (see *Peer Group Leader (PGL) Election Algorithm* on page 46-9 for more information), lower values have higher priority than higher values. The message **PGL Increment is a constant 50** refers to the condition when a node is elected PGL, it will increment its PGL priority by 50 to prevent hung elections.

You can set this value with the **pncfg** command, which is described in *Configuring Node-Specific Parameters* on page 46-40.

PGL State. Indicates if this node is a lowest-level node, a Peer Group Leader (PGL) node, or a potential PGL node. The possible PGL states are described below:

starting. This node has begun participation in the election of a PGL.

awaiting. This node has sent Hello messages on at least one link but no peer has been found.

awaitingFull. A least one neighboring peer has been found but the database synchronization process has been completed yet.

initialDelay. Database synchronization has been completed with at least one neighboring peer.

calculating. This node is calculating its new choice for peer group leader.

awaitUnamity. This node has chosen itself as PGL. It will check to see if all other nodes in the peer group have also elected it as PGL. This node will wait for a unanimous decision by all the nodes in the peer group or after a set period of time before declaring itself as the PGL.

NORMAL OPERATION: I'M PGL. This node is the PGL. It will continue to examine PTSEs to determine if other nodes in the peer group have a higher PGL priority.

NORMAL OPERATION: I'M NOT PGL. This node is not the PGL. It will continue to examine PTSEs to determine which node has the highest priority to be PGL.

hungElection. This node has chosen itself as PGL but it has failed to be elected PGL by at least 2/3 of the nodes in the peer group. This situation will be resolved by the node changing its preferred PGL or other nodes will accept it as the PGL.

awaitReElection. This node has lost its connection to the current PGL. A new election process will be started.

Preferred PGL. The ATM address of the node that this local believes should be or should become the preferred Peer Group Leader (PGL). If a PGL has not been chosen, then this field will display all zeroes.

Parent Node Id. When the local node is the Peer Group Leader (PGL), then this field will display the node ID of the parent Logical Group Node (LGN). If the local node is not the PGL of its peer group, then this field will display all zeroes.

Parent ATM Addr. When the local node is the Peer Group Leader (PGL), then this field will display the ATM address of the parent Logical Group Node (LGN). If the local node is not the PGL of its peer group, then this field will display all zeroes.

Parent PG Id. When the local node is the Peer Group Leader (PGL), then this field will display the local node's parent peer group ID. If the local node is not the PGL of its peer group, then this field will display all zeroes.

Parent PGL Node ID. When the local node is the Peer Group Leader (PGL), then this field will display the ID of the node elected as PGL in the parent peer group. If the local node is not the PGL of its peer group, then this field will display all zeroes.

Viewing Timer Information

The **ptinfo** command displays current configuration values for PTSE and Hello timers. These values are configured through the **pgcfg** and **pncfg** commands. For the single-peer group version of PNNI, enter

```
ptinfo
```

at the system prompt. For the multiple-peer group version of PNNI, the syntax for this command is as follows:

```
ptinfo [ <node level>]
```

The **<node level>** option allows you to display the current configuration for a specific node. If you do not use this option, then the **ptinfo** command will display the lowest level node. For example, when you enter

```
ptinfo
```

a display similar to the following displays:

```

                PNNI Timer Information
      (All time values are seconds unless otherwise specified)

PNNI node index:                1

PTSE refresh interval:          1800
PTSE lifetime factor:           2 (refresh intervals)
PTSE hold down interval:        1
PTSE delayed acknowledgement timer: 1

PTSP transmit timer:            10
PTSE request re-transmit timer: 1
PTSE aging timer:               10
Database summary re-transmit interval: 3

Hello interval:                 15
Hello hold down interval:        3
Hello inactivity factor:         5 (hello intervals)

Link AvCR proportional multiplier: 50%
Link AvCR minimum threshold:     3%
Link CTD proportional multiplier: 50%
Link CDV proportional multiplier: 25%
```

PNNI node index. A value used by SNMP to identify this node in the PNNI network.

PTSE refresh interval. The time, in seconds, before a self-originated PTSE is updated. PTSEs are aged out of the database unless refreshed by the originating node. The lifetime of a PTSE is determined by multiplying the Refresh Interval by the Lifetime Factor. The range for this value is 1 to 32,767 seconds. The default value is 1800 seconds.

PTSE lifetime factor. The value for the PTSE lifetime multiplier expressed as a percentage. Valid values are integers ranging from 1 to 255. This value helps determine the initial lifetime of a PTSE. The Lifetime Factor multiplied by the PTSE Refresh Interval is the initial lifetime of a PTSE. The default value is 2.

PTSE hold down interval. The minimum time, in seconds, before which this node can refresh PTSEs. A node can prevent a PTSE from aging out of the topology database by refreshing it. This holddown value limits the node from refreshing PTSEs too often and exhausting database space too quickly.

PTSE delayed acknowledgement timer. When a node receives a PTSE from another node it sends back an Acknowledgment packet. However, this acknowledgment is not immediate. This value is the amount of time between the receipt of a PTSE and its acknowledgment.

PTSP transmit timer. PTSPs are sent until they are acknowledged by neighboring nodes. This variable is the amount of time, in seconds, between successive transmissions of PTSPs. If a PTSP is acknowledged before this time interval, then a retransmission will not be sent.

PTSE request re-transmit timer. The time interval between the receipt of Database Summaries and the sending of PTSE Request packets. Database Summary packets contain an index of the PTSEs in a node's topology database. Other nodes use Database Summary packets to request PTSEs. If a node requires a PTSE listed in a Database Summary packet, then it will request that PTSE in the form of a PTSE Request packet.

PTSE aging timer. The time, in seconds, before a given PTSE entry in the topology database is aged out of the database. The PTSE may be refreshed by the originating node before this entry ages out. The timer may range from 1 to 255 seconds.

Database summary re-transmit interval. The time, in seconds, before this node will re-transmit a Database Summary packet that has gone unacknowledged by another node.

Hello interval. The value for the Hello timer in seconds. In the absence of triggered Hellos, this node will send one Hello packet on each of its ports at the interval specified here. Values can range from 1 to 255 seconds.

Hello hold down interval. The value for the Hello hold down timer. This node will use this value to limit the rate at which it sends Hello messages. Valid values range from 1 to 255 seconds.

Hello inactivity factor. The number of Hello intervals that may pass without receiving a Hello before the neighboring node is determined to have gone down. Valid values range from 1 to 255.

Link AVCR proportional multiplier. This variable is described in *Configuring General PNNI Parameters* on page 46-32.

Link AVCR minimum threshold. This variable is described in *Configuring General PNNI Parameters* on page 46-32.

Link CTD proportional multiplier. This variable is described in *Configuring General PNNI Parameters* on page 46-32.

Link CDV proportional multiplier. This variable is described in *Configuring General PNNI Parameters* on page 46-32.

Viewing PNNI Neighbor Information

The **pnbrs** command displays information on neighbor nodes connected to this OmniSwitch. It includes Node IDs of the neighboring nodes as well as statistics on PTSE communication between this node and its neighbors. For the single-peer group version of PNNI, the syntax for this command is as follows:

```
pnbrs [-s]
```

For the multiple-peer group version of PNNI, the syntax for this command is as follows:

```
pnbrs [-s] [<node level>]
```

The **-s** option provides a summary version of the **pnbrs** command (see *Summary Form of pnbrs* on page 46-63). The **<node level>** option allows you to display the current configuration for a specific node. If you do not use this option, then the **pnbrs** command will display the lowest level node. For example, when you enter

```
pnbrs
```

a screen similar to the following displays:

```

                                PNNI Port Neighbor Information
Neighbor: 50a03903488001bc900001010230e00020da0230e000  Nbr State: FULL
          PTSP  PTSE ACKS PTSE REQs  DB Sums  Port Count: 1
Rcvd/Xmtd  Rcvd/Xmtd  Rcvd/Xmtd  Rcvd/Xmtd  Local Ports To This Neighbor
-----
                2/          5/          1/          2/          5/2
                5           2           1           5
Neighbor: 50a03903488001bc9000010175ee100020da75ee1000  Nbr State: FULL
          PTSP  PTSE ACKS PTSE REQs  DB Sums  Port Count: 1
Rcvd/Xmtd  Rcvd/Xmtd  Rcvd/Xmtd  Rcvd/Xmtd  Local Ports To This Neighbor
-----
                2/          3/          1/          2/          5/1
                4           2           1           5

```

Neighbor. The Node ID of the neighboring peer node. This command displays a separate Node ID and a separate listing for each neighbor of this node.

Nbr State. The state of the neighboring node's Peer State Machine. The neighboring Peer State Machine manages exchanges of Hello and topology state packets. In addition, it describes the state of database synchronization and flooding ongoing with the neighboring peer. Possible states are as follows:

DOWN	No active links to the neighboring peer node.
NEGOTIATING	The first step in setting up a link between two neighbor nodes. The master node is determined during this step.
EXCHANGING	The node describes its topology database to its neighboring peer in the form of Database Summary packets.
LOADING	All Database Summary packets have been exchanged and all required PTSEs have been requested, but not all PTSEs have been received.
FULL	All PTSEs have been received from the neighboring peer node. Links to this node can now be advertised to other nodes via PTSEs.

PTSP Rcvd/Xmtd. The number of PNNI Topology State Packets (PTSPs) received from and transmitted to the neighboring peer node. PTSPs received are listed on the first line and PTSPs transmitted are listed on the bottom line.

PTSE Ack Rcvd/Xmtd. The number of PNNI Topology State Element (PTSE) Acknowledgment packets received from and transmitted to the neighboring peer node. Received PTSE Acknowledgments are listed on the first line and transmitted PTSE Acknowledgments are listed on the bottom line.

PTSE REQ Rcvd/Xmtd. The number of PTSE Request packets received from and transmitted to the neighboring peer node. Received PTSE Requests are listed on the first line and transmitted PTSE Acknowledgments are listed on the bottom line.

DB Sum Recvd/Xmtd. The number of Database Summary packets received from and transmitted to the neighboring peer node. Received Database Summaries are listed on the first line and transmitted Database Summaries are listed on the bottom line.

Port Count. The number of ports on this node that connect to the neighboring peer node. If the neighboring peer only communicates via an SVCC-based RCC, then the value of this variable will be zero. Otherwise it is set to the total number of ports connected to the neighboring peer that are in the Hello state, 2-WayInside. The ports included in this count are listed under the **Local Ports To This Neighbor** column.

Local Ports To This Neighbor. The local ports (i.e., ports on this OmniSwitch) connected to the neighboring peer node that are in the Hello state, 2-WayInside. In this Hello state, bi-directional communication between the two nodes has been achieved. The nodes are in the same peer group. Database summary packets, PTSE Request packets, PTSPs, and PTSE Acknowledgment packet can be transmitted over this link. If this node is an LGN, then this field will display **Over SVC/RCC** in this field.

Summary Form of pnbrs

The **pnbrs** command also has a summary option that allows you to view less information on each neighbor node. Simply enter the command

```
pnbrs -s
```

to obtain a display similar to the following:

PNNI Port Neighbor Information

```
3903488001bc9000010178aee00020da78aee000 NEGOTIATING 3/1 3/5 3/6 3/3
```

This display is a condensed form of the full **pnbrs** display. It shows the Node ID for each neighbor, the current state of the neighbor, and the local port connected to that neighbor. Full definitions of each of these pieces of information can be found in the above explanations.

Viewing Port Information

The **ppinfo** command displays information on all CSM ports (about which PNNI is aware) in this OmniSwitch. Information includes the port type, the port's current Hello State, and the Administrative Weight of the attached link. When you enter

ppinfo

a screen similar to the following displays:

PNNI Port Information								
PNNI SI/Prt PortId	VPI//VCI Type	VP Cap	Neighbor State	Advertised Max CR/ Avail CR	Admin Weight			
5/ 2 (257)	0/18 OC3	n	RCC Unavail	350000	CBR:5040 rt-VBR:5040	ABR:5040	UBR:5040 nrt-VBR:5040	
7/ 1 (384)	0/18 OC3	n	LOADING	350000	CBR:5040 rt-VBR:5040	ABR:5040	UBR:5040 nrt-VBR:5040	

PNNI SI/Prt PortId. The slot and port for this CSM port. The first number is the slot number for the CSM module and the second number (after the slash) is the port number on the CSM module. The number in parentheses is the internal identification for this port.

Vpi/Vci. The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) for the Routing Control Channel (RCC) defined here. The VPI is listed first, followed by a slash (/), and then the VCI.

The port type is listed under the VPI/VCI. This information indicates whether this is an OC-3c/STM-1c port connection (155 Mbps) or an OC-12c/STM-4c (622 Mbps) port connection. If this entry is describing the internal port on an FCSM module or an ATM uplink port on an ASM module, then this column will read **ASM**.

VpCap. Indicates whether this port advertises to other nodes that it supports the establishment of Virtual Paths. **Y** means the port advertises that Virtual Paths can be established on this physical link. **N** means that this port does not advertise that it is capable of setting up Virtual Paths.

Neighbor state. Indicates the state of the neighboring node. Possible states are as follows:

DOWN	No active links to the neighboring peer.
NEGOTIATING	The first step in setting up a link between two neighbors.
EXCHANGING	The node describes its topology database to its neighboring peer in the form of Database Summary packets.
LOADING	All Database Summary packets have been exchanged and all required PTSEs have been requested, but not all PTSEs have been received.
FULL	All PTSEs have been received from the neighboring peer. Links to the neighboring peer can now be advertised to other nodes via PTSEs.
RCC Unavail	The Routing Control Channel is not available on his link. The link may not be supported by PNNI.
Border Node	The neighboring node is a border node.

Advertised Max CR/Avail CR. The first line is the maximum cell rate (in cells per second) for each QoS on this port. This value is determined by hardware. The second line is the currently available bandwidth for each QoS; this value may be less than the maximum cell rate due to usage on the port. The maximum cell rate, in cells per second, for each CSM port type is as follows:

- OC-3 ports 350,000
- OC-12 ports 1,400,000
- ATM 25 Mbps ports 50,000

AdminWt. The Administrative Weight assigned to each Class of Service on this port. Administrative Weight is assigned through the **ppcfg** command.

Summary Form of ppinfo

The **ppinfo** command also has a summary option that allows you to view less information on each PNNI port. Simply enter the command

```
ppinfo -s
```

to obtain a display similar to the following:

PNNI Port Information Summary

SI/Port [/Inst]	Phys Port	State	SI/Port [/Inst]	Phys Port	State
3/ 1	(128)	FULL	3/ 3	(144)	FULL
3/ 5	(160)	FULL	3/ 6	(168)	FULL
3/ 2/1	(701)	RCC UNAVAIL			

This display is a condensed form of the full **ppinfo** display. It shows physical port information and the state of the neighbor currently attached to the local port. Full definitions of each of these pieces of information can be found in the above explanations.

Viewing Link Information

The **plink** command contains information on the logical links attached to this OmniSwitch and the relationship with the neighbor nodes on the other end of the links. For the single-peer group version of PNNI, the syntax for this command is as follows:

```
plink [-s]
```

For the multiple-peer group version of PNNI, the syntax for this command is as follows:

```
plink [-s] [ <node level>]
```

The **-s** option provides a summary version of the **plink** command (see *Summary Form of plink* on page 46-68). The **<node level>** option allows you to display the current configuration for a specific node. If you do not use this option, then the **plink** command will display the lowest level node. For example, when you enter

```
plink
```

a screen similar to the following displays:

PNNI Link Table					
Lcl/Rmt PortId	S/P/I IfIndex	State/ Version	Remote Node Id	Hellos Xmtd/Recvd	Link Type
128/ 128	3/1 30100	2 WAY INSIDE 1	3903488001bc90000101 7a1bd00020da7a1bd000	1295/ 1287	Lowest Level Horizontal
144/ 144	3/3 30300	2 WAY INSIDE 1	3903488001bc90000101 7a1bd00020da7a1bd000	1295/ 1286	Lowest Level Horizontal
160/ 160	3/5 30500	2 WAY INSIDE 1	3903488001bc90000101 7a1bd00020da7a1bd000	1295/ 1286	Lowest Level Horizontal

Lcl/Rmt PortId. The first line in each row of this column is the PNNI Port Identifier of the local port on this link as selected by the local node. This value is relevant to the local switch only. Different ATM switches may use different formulas to derive this value.

The second line in each row of this column is the Port Identifier at the remote end of this link as assigned by the remote node. If the Link Type is **Outside Uplink**, then this ID is assigned by the lowest-level neighbor node to identify the outside link. If the Remote Port ID is unknown or the link type is **Uplink**, then this value is set to zero.

S/P/I If Index. The first line in each row of this column is the CSM slot and port for link. The second line is the IfIndex for this interface. For horizontal and outside links between the lowest-level nodes and for links of an unknown type, the IfIndex identifies the physical interface to which this logical link corresponds. For all other links, this value is zero.

State. Indicates the state of the Hello protocol exchange over this link. Possible values are as follows:

DOWN	No PNNI Routing packets sent or received over the link.
ATTEMPTING	Attempts were made to contact the neighboring node with Hello messages, but no valid Hellos have been received from the neighbor.
1 WAY INSIDE	A Hello has been received from the neighboring node. Both nodes are members of the same peer group, but the node and port identifiers from the neighbor are set to zero.

2 WAY INSIDE	Bi-directional communication between the two nodes on this link has been achieved. The nodes are in the same peer group. Database summary packets, PTSE Request packets, PTSPs, and PTSE Acknowledgment packets can be transmitted over this link.
1 WAY OUTSIDE	A Hello has been received from the neighboring node. The nodes are members of different peer groups. The node and port identifiers from the neighbor are set to zero. This node will now search for a common peer group that contains both nodes.
2 WAY OUTSIDE	A Hello has been received from the neighboring node. The nodes are members of different peer groups. Valid node and port identifiers have been received, but a common peer group between the two nodes has not been identified. This node will now search for a common peer group that contains both nodes.
COMMON_OUTSIDE	Bi-directional communication between the two nodes on this link has been achieved. This link can now be advertised through PTSEs.

Version. Indicates the version of the PNNI Routing protocol used to exchange information over this link. If communication with the neighbor node has not yet been established, then this value is set to **Unknown**. The version of PNNI supported in this release is 1.0.

Remote Node Id. Indicates the Node ID of the remote (neighboring) node on the other end of the link. If the Link Type is **Outside Uplink**, then this is the Node ID of the lowest-level neighbor node on the other end of the outside link. If the remote node ID is unknown or if the Link Type is **Uplink**, then this variable is set to all zeros.

Hellos: Transmitted and Received. For horizontal links between lowest-level nodes, these values indicate the number of Hello packets transmitted or received over this link.

Type. The type of link described in this display. The following types are possible:

Unknown	Unknown type of link.
Lowest Level Horizontal	Lowest-level node, horizontal link.
Lowest Level Outside	Lowest-level node connected via an outside link.
Hor link to LGN	Horizontal link to a Logical Group Node. (Not supported in a single peer group network).
Uplink	Uplink to a Logical Group Node in another peer group. (Not supported in a single peer group network.)
Outside uplink	An outside link that is also an uplink. (Not supported in a single peer group network.)

Summary Form of plink

The **plink** command also has a summary option that allows you to view less information on the logical links connected to this node. Simply enter the command

plink -s

to obtain a display similar to the following:

PNNI Link Table			
Lcl PortId	Rmt PortId	State	Link Type
=====	=====	=====	=====
128	128	2 WAY INSIDE	Lowest Level and Horizontal
136	136	2 WAY INSIDE	Lowest Level and Horizontal

This display is a condensed form of the full plink display. It shows the local port ID, the remote port ID, the state of the Hello protocol exchange over this link, and the type of link. Full definitions of each of these pieces of information can be found in the above explanations.

Viewing the PTSE Database

The **pptse** command displays the kind of information contained in a node's topology database. A separate entry is provided for each PNNI Topology State Element (PTSE) in the database. Output from this command can become lengthy depending on the complexity of the network. The number of PTSEs is dependent on the number of nodes in the network as well as the number of End Systems, routes, and topology metrics.

This command also has a verbose mode that displays a hexadecimal dump of the topology database contents. This hex dump displays actual database entries as they reside in the topology database. Examples of the standard and verbose mode output from this command are given below.

Standard Output

For the single-peer group version of PNNI, the syntax for this command is as follows:

```
pptse [-s | -v]
```

For the multiple-peer group version of PNNI, the syntax for this command is as follows:

```
pptse [-s | -v] [ <node level>]
```

The **-s** option provides a summary version of the **pptse** command (see *Standard Output* on page 46-69) and the **-v** option provides a verbose option (see *Verbose Mode Output* on page 46-70). The **<node level>** option allows you to display the current configuration for a specific node. If you do not use this option, then the **pptse** command will display the lowest level node. For example, when you enter

```
pptse
```

a screen similar to the following displays:

```

                                PNNI PTSE Database Summary
Node ID:50a03903488001bc900001010230e00020da0230e000   PTSE:  1
Checksum: 1a81   Remaining lifetime: 3129 seconds       Seq #:  1
Information Group Carried: Nodal IG
=====
Node ID:50a03903488001bc900001010230e00020da0230e000   PTSE:  3
Checksum: 58da   Remaining lifetime: 3519 seconds       Seq #:  1
Information Group Carried: Horizontal Links IG
=====
Node ID:50a03903488001bc9000010175ee100020da75ee1000   PTSE:  1
Checksum: 5408   Remaining lifetime: 2888 seconds       Seq #:  1
Information Group Carried: Nodal IG
=====
Node ID:50a03903488001bc9000010175ee100020da75ee1000   PTSE:  2
Checksum: 5a49   Remaining lifetime: 3168 seconds       Seq #:  1
Information Group Carried: Horizontal Links IG
=====
Node ID:50a03903488001bc90000101761c900020da761c9000   PTSE :  1
Checksum: 53ab   Remaining lifetime: 3490 seconds       Seq #:  1
Information Group Carried: Nodal IG
=====
Node ID:50a03903488001bc90000101761c900020da761c9000   PTSE :  2
Checksum: d8db   Remaining lifetime: 3520 seconds       Seq #:  1
Information Group Carried: Horizontal Links IG
=====

```

Node ID. The Node Identifier of the node that originated the PTSE.

PTSE. The PTSE Identifier assigned to this PTSE by the node that originated the PTSE.

Checksum. The value of the PTSE checksum as it appears in the local topology database.

Remaining lifetime. The remaining lifetime, in seconds, for this PTSE in the local node's topology database.

Seq #. The sequence number for this PTSE as it appears in this node's local topology database. This value differs from the PTSE ID as it is defined by the recipient of the PTSE (i.e., this node). The PTSE ID is assigned by the sender of the PTSE (i.e., the originating neighbor node).

INFORMATION GROUPS CARRIED. The type of information contained in this PTSE.

Verbose Mode Output

You can obtain the actual contents for each PTSE in the topology database through the **pptse** verbose mode. Note that output can become quite lengthy.

When you enter

```
pptse -v
```

a screen similar to the following displays:

PNNI PTSE Database Summary

```
Node ID:50a03903488001bc900001010230e00020da0230e000 PTSE: 1
```

```
Checksum: 1a81 Remaining lifetime: 3019 seconds Seq #: 1
```

```
Information Group Carried: Nodal IG
```

```
PTSE contents:
```

```
0000: 00 02 00 70 01 01 01 00 60 a0 39 03 48 80 01 bc
0010: 90 00 01 01 72 b1 b0 00 20 da 72 b1 b0 00 50 39
0020: 03 48 80 01 bc 90 00 01 01 01 00 00 00 40 00 44
0030: 00 61 00 00 00 00 01 00 00 00 01 1a 81 0b cb
0040: 00 61 00 50 39 03 48 80 01bc 90 00 01 00 01 00
0050: 01 00 20 da 72 b1 b0 00 00 00 00 00 00 00 00 00
0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
=====
Node ID:50a03903488001bc900001010230e00020da0230e000 PTSE: 3
```

```
Checksum: 58da Remaining lifetime: 3409 seconds Seq #: 1
```

```
Information Group Carried: Horizontal Links IG
```

```
PTSE contents:
```

```
0000: 00 02 00 c0 01 01 01 00 50 a0 39 03 48 80 01bc
0010: 90 00 01 00 01 00 01 00 20 da 72 b1 b0 00 50 39
0020: 03 48 80 01 bc 90 00 01 01 01 00 00 00 40 00 94
0030: 01 20 00 00 00 00 03 00 00 00 01 58 da 0d 51
0040: 01 20 00 80 80 00 50 a0 39 03 48 80 01bc 90 00
0050: 01 01 01 00 01 00 20 da 76 1c 90 00 00 00 01 80
0060: 00 00 00 c0 00 00 00 01 00 80 00 2c 18 00 00 00
0070: 00 00 13 b0 00 05 57 30 00 04 93 e0 00 00 00 0a
0080: 00 00 00 02 00 08 00 00 00 a0 00 0c 00 00 00 64
0090: 00 00 00 02 00 80 00 2c e0 01 00 00 00 00 13 b0
00a0: 00 05 57 30 00 04 93 e0 00 00 00 0a 00 00 00 02
00b0: 00 08 00 00 00 a0 00 0c 00 00 00 64 00 00 00 02
```

A separate listing is provided for each PTSE. The top portion of each listing is the same information provided through the non-verbose **pptse** command. The additional information is a hexadecimal dump of the actual PTSE data.

Verbose Information on a Single PTSE

You can also obtain the verbose mode output for a single PTSE. This display may be useful when you require detailed PTSE information, but not for every PTSE in the PNNI database. To request detailed information for a PTSE, you will need to know its Node ID and PTSE ID. You can get these two pieces of information via the standard **pptse** output. After obtaining the Node ID and PTSE ID, enter your **pptse** command as follows:

```
pptse -v <22-byte Node ID> -p <PTSE ID>
```

The following is an example of a command line specification:

```
pptse -v 50a03903488001bc900001010230e00020da0230e000 -p 3
```

This command line would display the same output as second PTSE in the sample verbose mode output shown above.

Summary Mode Output

You can also obtain a summary display of all PTSEs associated with a given Node ID through the **pptse** summary mode. When you enter

pptse -s

a screen similar to the following displays:

```

                                PNNI PTSE Summary Table
                                (PTSE lifetime is displayed in seconds)

Node Id: 50a03903488001bc900001016cdb200020da6cdb2000
PG ID:   503903488001bc90000101000000
  PTSE:   1 (seq 512): Nodal IG                2868
  PTSE:   2 (seq 513): IReach ATM addresses IG  2868
  PTSE:   3 (seq 512): HLink                   2918
  PTSE:   4 (seq 512): HLink                   2918
  PTSE:   5 (seq 510): HLink                   1688
Node Id: 50a03903488001bc900001017def000020da7def0000
PG ID:   503903488001bc90000101000000
  PTSE:   1 (seq 557): Nodal IG                3459
  PTSE:   2 (seq 558): IReach ATM addresses IG  3459
  PTSE:   5 (seq 480): HLink                   3529
  PTSE:   6 (seq 479): HLink                   3529
Node Id: 50a03903488001bc900001017f6bc00020da7f6bc000
PG ID:   503903488001bc90000101000000
  PTSE:   1 (seq 668): Nodal IG                2820
  PTSE:   2 (seq 669): IReach ATM addresses IG  2820
  PTSE:   9 (seq 574): HLink                   2830
  PTSE:  10 (seq 574): HLink                   2830
  PTSE:  11 (seq 574): HLink                   2830
Node Id: 50a03903488001bc900001018519000020da85190000 (MYSELF)
PG ID:   503903488001bc90000101000000
  PTSE:   1 (seq 557): Nodal IG                3468
  PTSE:   2 (seq 558): IReach ATM addresses IG  3468
  PTSE:   3 (seq 557): HLink                   3518
  PTSE:   4 (seq 557): HLink                   3518
  PTSE:   5 (seq 557): HLink                   3518
  PTSE:   6 (seq 555): HLink                   2608
Node Id: 50a03903488001bc900001018519b00020da8519b000
PG ID:   503903488001bc90000101000000
  PTSE:   1 (seq 514): Nodal IG                3539
  PTSE:   2 (seq 515): IReach ATM addresses IG  3539
  PTSE:   5 (seq 37): HLink                    3549
  PTSE:   7 (seq 37): HLink                    3549
Node Id: 50a03903488001bc900001019238700020da23870000
PG ID:   503903488001bc90000101000000
  PTSE:   1 (seq 557): Nodal IG                3459
  PTSE:   2 (seq 558): IReach ATM addresses IG  3459
  PTSE:   3 (seq 557): HLink                   3519

```

This summary display groups PTSEs with their associated Node IDs. Each PTSE entry shows the number of the PTSE on that node, the sequence number for the PTSE, the information groups in the PTSE, and then the remaining lifetime (in seconds) for the PTSE. See *Standard Output* on page 46-69 for a more complete description of each of these values.

Viewing End-Point Adjacencies

The **padj** command displays adjacencies to this node. An adjacency is an End System or other ATM destination that is attached to a CSM port on this OmniSwitch node. Adjacencies are learned via ILMI. An adjacency differs from a neighbor in that a neighbor is an active participant in PNNI exchanges and is normally another node or switch.

When you enter

```
padj
```

a screen similar to the following displays:

PNNI Adjacency Table

```
Client: 4700790000000000000000000000a03e00000100   Advertised: TRUE
Learnt: TUE JAN 20 11:44:59 1998                   Slot/Port/Inst: 3/8 (port 184)
```

The following adjacencies are summarized by this node's summary address (which is 3903488001bc900001017a1bd0):

Native Address	PNNI Port	Learned at Time
3903488001bc900001017a1bd000041347561000	3/8 (184)	TUE JAN 20 11:44:59

Client. The 20-octet End System ATM address for the adjacency described by this entry.

Learnt. The date and time at which this adjacency was learned by this node. Node adjacencies are normally learned through ILMI.

Advertised. Since adjacencies are learned via ILMI, they can be learned at any time, including when PNNI is not operational in the OmniSwitch. If PNNI is not operational or if it has not been updated with this adjacency information, then this information is not advertised by PNNI throughout the network. In other words, information on this adjacency is not being passed via PTSEs to other nodes and this field would be False (**F**). If PNNI is operational and information on this adjacency is being passed to other nodes, then this field will be True (**T**).

Also, note that adjacencies are advertised on internally reachable destinations in PTSE IREACH frames.

Slot/Port/Inst. The CSM slot and port to which this adjacency is attached. The slot number is listed first, followed by a slash (/), and then the port number on the CSM module.

Some adjacencies may use address summarization to advertise their status. Those addresses that use summarization are listed with the following column descriptions:

Native Address. The full non-summarized 20-octet ATM address used to describe this adjacency.

PNNI Port. The physical slot and port number and the internal port number for this adjacency.

Learned at Time. The date and time at which the PNNI database learned about this adjacency.

Configuring PNNI Scope Mapping Parameters

The **psmap** command is used to view and configure how the UNI/ILMI scope is mapped to the PNNI scope. UNI 4.0/ILMI 4.0 clients have a scope associated with an address. During ILMI address registration, ILMI will pass this scope along with an address to PNNI. In order to determine the scope of address advertisement, PNNI needs to map this ILMI scope to a PNNI scope. The default UNI/ILMI scope value is 15 (global) when ILMI scope is absent.

◆ **Note** ◆

You must install the software for multiple group operation to use this command.

For example, say an operational PNNI ATM network has three (3) levels (scope): 96, 80, 72. When ILMI registers address A.1.1 with scope 1 (which maps to PNNI scope 96), PNNI will only advertise this address in the PNNI level 96 network. When ILMI registers address A.1.2 with scope 6 (which maps to PNNI scope 72), then PNNI will advertise this address in level 72 (which is higher in the in the PNNI hierarchy than level 96), this address will known by more nodes.

To use the **psmap** command, enter

```
psmap
```

at the system prompt. A screen similar to the following will be displayed.

PNNI Scope Mapping Table

Scope Name	UNI/ILMI Scope	PNNI Scope/Level
1) LocalNetwork	1	96
2) LocalNetworkPlusOne	2	96
3) LocalNetworkPlusTwo	3	96
4) SiteMinusOne	4	80
5) IntraSite	5	80
6) SitePlusOne	6	72
7) OrganizationMinusOne	7	72
8) IntraOrganization	8	64
9) OrganizationPlusOne	9	64
10) CommunityMinusOne	10	64
11) IntraCommunity	11	48
12) CommunityPlusOne	12	48
13) Regional	13	32
14) InterRegional	14	32
15) Global	15	0

To configure a parameter, type "item = value" (as in 1=96)
 To quit out of configuration, type "quit"
 To save the configured info, type "save"

:

The PNNI mapping parameters listed by the **psmap** command are displayed in ascending order by hierarchy level. Each parameter is identified under the headings **Scope Name**, **UNI/ILMI Scope**, and **PNNI Scope/Level**. The **Scope Name** is a text description of the scope. The **UNI/ILMI Scope** is the UNI 4.0/ILMI 4.0 organizational scope. The lowest level is 1 and the highest level is 15. And the **PNNI Scope/Level** is the configurable PNNI routing level.

Higher values in the PNNI routing level indicate lower levels in the PNNI hierarchy. A logical node will only advertise its reachability to an organizational level that is greater than or equal to the node ID. Therefore, setting the PNNI routing level of an organizational level lower than the node's ID will prevent the node's address from being advertised at that level. Setting this value to 0 will prevent the node from advertising its reachability to this level.

All parameters are set to default values listed in ATM Forum PNNI Specification Version 1.0. To alter a parameter, enter the line number for the parameter, followed by an equal sign (=), and then the value for the parameter. For example, to change **Regional** from 32 to 48, enter:

```
13=48
```

at the prompt.

You can redisplay the parameters by entering a question mark (?). When you have completed configuring parameters, enter **save**. Your new values will be saved and you will exit this menu. If you want to exit this menu without saving changes, simply enter **quit**. If you have made any changes, then the following prompt will be displayed.

```
Do you want these changes to take effect immediately? (y)
```

Press **<Return>** to implement your changes immediately or press **n** to implement your changes at the next reboot.

The PNNI scope mapping parameters displayed by the **psmap** command are described below.

1) LocalNetwork

This level corresponds to the concept of a physical network. The default value is 96.

2) LocalNetworkPlusOne

This level corresponds to the concept of an ATM subnet that does *not* use inter-building or wide-area links. This level could consist of a peer group and its neighboring peer group, for example. The default value is 96.

3) LocalNetworkPlusTwo

This level corresponds to the concept of an ATM subnet that does *not* use inter-building or wide-area links. This level could consist of two or more peer groups, for example. The default value is 96.

4) SiteMinusOne

This level corresponds to the concept of an ATM subnet that does *not* use inter-building or wide-area links. This level could consist of the majority of peer groups in a building, for example. The default value is 80.

5) IntraSite

This level identifies the inclusive routing hierarchy of nodes that are not geographically separated. You can use this parameter to confine ATM traffic to a local location and thereby avoid using inter-building and wide-area links. The default value is 80.

6) SitePlusOne

This level identifies ATM networks that may use inter-building and wide-area links. This level could consist of ATM networks in two different buildings, for example. The default value is 72.

7) OrganizationMinusOne

This level identifies ATM networks that may use inter-building and wide-area links. This level could consist of ATM networks in several different buildings, for example. The default value is 72.

8) IntraOrganization

This level identifies the inclusive routing of an autonomous organization, which is defined as the organization that has administrative authority of the network. This level may use inter-building and wide-area links. The default value is 64.

9) OrganizationPlusOne

This level identifies the union of at least two autonomous organizations. The default value is 64.

10) CommunityMinusOne

This level identifies the union of two or more autonomous organizations. The default value is 64.

11) IntraCommunity

This level identifies a collection of autonomous organization that are organized by a provider or organizational partnership. The default value is 48.

12) CommunityPlusOne

This level identifies a collection of autonomous organization that are organized by a provider or organizational partnership. The default value is 48.

13) Regional

This level identifies a collection of autonomous organization that are organized by a provider or organizational partnership. The default value is 32.

14) InterRegional

This level identifies a collection of autonomous organization that are organized by a provider or organizational partnership. The default value is 48.

15) Global

This level represents all autonomous organizations That form a connected private ATM network. The default value is 0.

Viewing the PNNI Map Table

The **pmap** command displays the PNNI map table, which contains information on all links and nodes in the PNNI hierarchy from the perspective of a local node. For the single-peer group version of PNNI, the syntax for this command is as follows:

```
pmap [-s]
```

For the multiple-peer group version of PNNI, the syntax for this command is as follows:

```
pmap [-s] [ <node level>]
```

The **-s** option provides a summary version of the **pmap** command (see *Summary Form of pmap* on page 46-78). The **<node level>** option allows you to display the current configuration for a specific node. If you do not use this option, then the **pmap** command will display the lowest level node. For example, when you enter

```
pmap
```

a screen similar to the following displays:

PNNI Map Table

```

1) Orig Node Id: 50a03903488001bc900001010230e00020da0230e000
   Remote Node Id: 50a03903488001bc90000101761c900020da761c9000
   PGID: 50 3903488001bc90000101000000
   Orig Port ID: 192 Remote Port ID: 384
   Map entry type: Horizontal Link Derived Aggr Token: 1
   PTSE-Id: 3 VP Capability: Enabled

```

Map table entries are numbered with a node index number in the leftmost column. This index identifies each connection. A single node may have multiple entries for multiple connections.

Orig Node Id. The node identifier of the node originating the PTSE. If the **Map entry type** is **Node**, then this value is also set to zero.

Remote Node Id. For horizontal links, this value is the node identifier of the node at the other end of the link from the node originating the PTSE. If the link is unknown, then PNNI sets this value to all zeros. If the **Map entry type** is **Node**, then this value is also set to zero.

PGID. The peer group ID of the originating node.

Orig Port ID. The Port Identifier assigned to this port by its node. The first number is the CSM slot number and the second number (after the slash) is the port number on the module.

Remote Port Id. For horizontal links, this value is the Port Identifier of the port at the remote end of this link. If the remote port is unknown, then PNNI sets this value to zero. For Nodes, this value is the Port Identifier of the remote port connected to the originating port. This value is only relevant to the local switch as ATM switches calculate this value differently.

Map entry type. The type of PNNI entity described in this entry. The PNNI type will either be a Horizontal Link (**HORIZ LINK**) or a Node (**NODE**).

Derived Aggr Token. The aggregation token for this port on the remote node. This variable is configured through the **ppcfg** command. The aggregation token allows links from the same switch to be advertised separately and contain independent topology metrics. If two links contain different aggregation tokens, then they will be viewed as distinct links by the peer group. If two links have the same aggregation token value, then they will be viewed as the same link by the peer group.

PTSE-Id. The PTSE Identifier for the PTSE sent by the originating node that contains the information group(s) describing the PNNI entity. Each PNNI entity (node or link) or aspect of a PNNI entity (such as a node's peer group) is completely described by a single PTSE.

Viewing the PNNI Map Table

VP Capability. Indicates whether this port advertises to other nodes that it supports the establishment of Virtual Path Connections (VPCs). **Enabled** means the port advertises that Virtual Paths can be established on this physical link. **Disabled** means that this port will not advertise that it is capable of setting up Virtual Paths.

Summary Form of pmap

You can also obtain a summary output of the **pmap** command that organizes all map table information into two tables. When you enter

```
pmap -s
```

A screen similar to the following displays:

```

                                PNNI Map Summary
                                Within Peer Group: 50 3903488001bc90000101000000

Node Index                      Node ID
-----
 1      50a03903488001bc900001016cdb200020da6cdb2000
 2      50a03903488001bc900001017defc00020da7defc000
 3      50a03903488001bc900001017f6bc00020da7f6bc000
 4      50a03903488001bc900001018519000020da85190000 (MYSELF)
 5      50a03903488001bc900001018519b00020da8519b000
 6      50a03903488001bc900001019238700020da23870000

Orig Node Index  Orig Port Id  Link Type  Rem Port Id  Rem Node Index
-----
 1      (192) <== HLINK ==> (192) 2
 1      (200) <== HLINK ==> (416) 3
 1      (208) <== HLINK ==> 4/2 (200) 4
 1      (216) <== HLINK ==> 4/4 (216) 4
 2      (200) <== HLINK ==> 7/5 (416) 4
 3      (464) <== HLINK ==> 8/3 (464) 4
 3      (200) <== HLINK ==> 4/3 (208) 5
 4      7/8 (440) <== HLINK ==> (200) 5
 5      (216) == HLINK ==> (200) 6 (Unusable)*

```

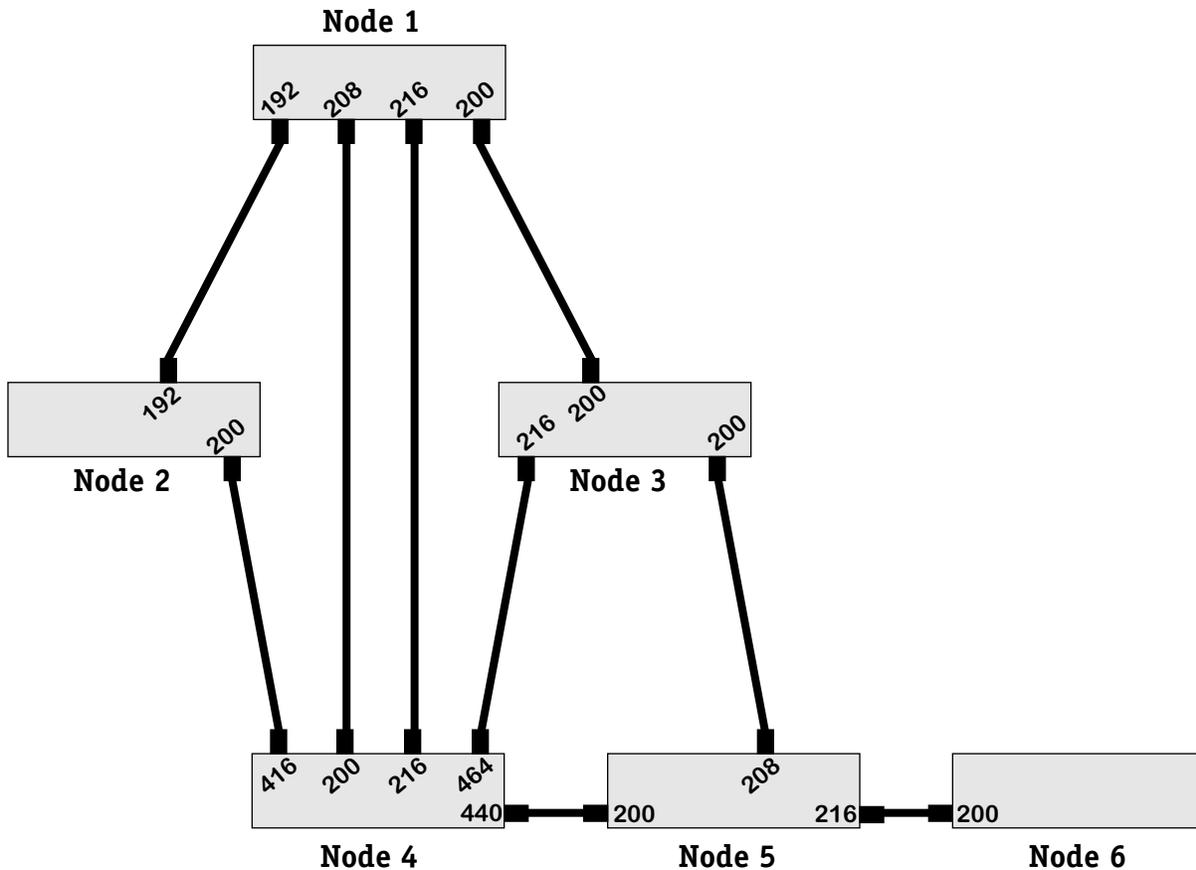
* - Unusable links may be so noted if their PTSE is being re-originated due to lifetime expiration.

The first table lists all the node indexes in the PNNI map table along with their associated Node IDs. The second table lists attributes of each node index. Descriptions of these variables can be found in the section for the standard **pmap** output. Note that one of the links is considered “unusable” because PNNI cannot forward on links that are not bi-directional.

A network diagram of this display is shown on the following page.

Network Diagram of pmap Summary Display

As an illustration, the summary **pmap** display on page 46-78 is generated from a network that is configured as follows. The port numbers shown on each node correspond to internal PNNI port numbers.



Network Configuration Used for pmap Display

In the **pmap** UI display, each connection is represented by a pair of port ids: **Orig Port Id** and **Rem Port Id**. Each port id also has a corresponding node index. If you compare the above diagram with the **pmap** summary display, you will find each port-to-port connection in the display.

The one variant connection is the one listed last in the **pmap** display. This link is listed as **Unusable** in the display. The **pmap** display provides a clue as to why this connection is not usable.

Note that under the **Link Type** column, the arrow points in only one direction—from port 216 to port 200. All other connections in the table show the arrow pointing in both directions, which is symbolic of a bi-directional traffic flow. In the unusable link, traffic can flow from Node 5 (port 216) to Node 6 (port 200), but it cannot flow from Node 6 back to Node 5. When a link is not bi-directional, PNNI deems it unusable.

Viewing the PNNI Nodal Map Table

The **pnmap** command displays information learned by the local node from nodal information PTSEs. For the single-peer group version of PNNI, the syntax for this command is as follows:

```
pnmap [-s]
```

For the multiple-peer group version of PNNI, the syntax for this command is as follows:

```
pnmap [-s] [<node level>]
```

The **-s** option provides a summary version of the **pnmap** command (see *Summary Form of pnmap* on page 46-82). The **<node level>** option allows you to display the current configuration for a specific node. If you do not use this option, then the **pnmap** command will display the lowest level node. For example, when you enter

```
pnmap
```

a screen similar to the following displays:

```

                                PNNI Nodal Map Table

1) Node ID:                      50a03903488001bc900001020000080020da00000800 *
   Peer Group Id:                 50 3903488001bc90000102000000
   ATM Address:                   3903488001bc900001020000080020da00000800
   Restr. Transit:                False           Restr Branching:      False
   Complex Rep:                  False           DB Overloaded:        False
   Is Peer Grp Leader:           False           Leadership Priority:   100

   Preferred PGL:                50a03903488001bc900001020000080020da00000800
   Parent Node Id:                0000000000000000000000000000000000000000
   Parent ATM Addr:              0000000000000000000000000000000000000000
   Parent PG Id:                 00 00000000000000000000000000000000
   Parent PGL Node ID:           0000000000000000000000000000000000000000

```

◆ Note ◆

The last set of parameters (**Preferred PGL** through **Parent PGL Node ID**) will not display unless you have installed the software for multiple-peer group PNNI.

Node ID. The node identifier for the node described in this entry.

Peer Group Id. The peer group of the originating node.

ATM Address. The ATM End System (ES) address of the originating node.

Restr. Transit. Indicates whether this node is restricted from supporting Switched Virtual Circuits (SVCs) transiting this node. **False** means the port can support ATM transit data links. **True** means the port will be restricted from setting up SVCs unless overridden by another PNNI parameter; only SVCs originating and terminating at this node are supported.

Restr Branching. Indicates whether the originating node is able to support additional multicast virtual circuit branches. **False** means that the node can support additional multicast branches. **True** means that additional branches are not supported because the maximum number of multicast virtual circuits on all modules in the node has been reached. The maximum number of multicast virtual circuits supported by a CSM-155 module is 8000, and the maximum supported by a CSM-622 module is 16,000.

Complex Rep. Indicates whether the originating nodes use complex node representation. **True** indicates complex representation is used. **False** indicates that simple node representation is used.

DB Overloaded. Indicates whether the originating node is currently operating in topology database overload state. If the node is in overload state, then you may want to increase PNNI operating limits through the **pgcfg** command (described in *Configuring General PNNI Parameters* on page 46-32).

Is Peer Grp Leader. Indicates whether the originating node claims to be peer group leader of its peer group.

Leadership Priority. The leadership priority advertised by the originating node.

◆ **Note** ◆

The following fields only apply to nodes in multiple peer groups.

Preferred PGL. The ATM address of the node that this local believes should be or should become the preferred Peer Group Leader (PGL). If a PGL has not been chosen, then this field will display all zeroes.

Parent Node Id. When the local node is the Peer Group Leader (PGL), then this field will display the node ID of the parent Logical Group Node (LGN). If the local node is not the PGL of its peer group, then this field will display all zeroes.

Parent ATM Addr. When the local node is the Peer Group Leader (PGL), then this field will display the ATM address of the parent Logical Group Node (LGN). If the local node is not the PGL of its peer group, then this field will display all zeroes.

Parent PG Id. When the local node is the Peer Group Leader (PGL), then this field will display the local node's parent peer group ID. If the local node is not the PGL of its peer group, then this field will display all zeroes.

Parent PGL Node ID. When the local node is the Peer Group Leader (PGL), then this field will display the ID of the node elected as PGL in the parent peer group. If the local node is not the PGL of its peer group, then this field will display all zeroes.

Summary Form of pnmmap

The **pnmmap** command also has a summary option that allows you to view less information on each node. Simply enter the command

```
pnmmap -s
```

to obtain a display similar to the following:

PNNI Nodal Map Summary Table

- 1) Node ID: 50a03903488001bc90000101784e500020da784e5000**
- 2) Node ID: 50a03903488001bc9000010178aee00020da78aee000**
- 3) Node ID: 50a03903488001bc900001017a1bd00020da7a1bd000 (MYSELF)**
- 4) Node ID: 50a03903488001bc900001017f6e900020da7f6e9000**

This display is a condensed form of the full **pnmmap** display. It simply lists the Node IDs for nodes currently included in the PNNI topology database for this network.

Viewing Current PNNI Calls

The **pcalls** command displays the current in-progress PNNI calls. The number of current calls is listed in the **pginfo** command. The **pcalls** command provides more detail on each of these calls. The table includes current Point-to-Point and Point-to-Multipoint calls. The table for each call type is the same.

◆ Note ◆

PNNI calls are opened and closed continuously. Therefore, the calls listed in **pcalls** output are probably complete by the time you view information in this display.

The following is an example of the **pcalls** output. Note that only information for Point-to-Multipoint calls is displayed in this sample. If there were Point-to-Point calls present, then information on those calls would display before the Point-to-Multipoint table.

The Point-to-Point Call Table is empty.

PNNI Point-to-Multipoint Call Table

CallRef	Call Id	Dtl	CallRef	Call Id	Dtl
=====	=====	=====	=====	=====	=====
4b200010	00000001	1	4b200010	00000002	1
4b201870	00000004	1	4b201c80	00000005	1
4b202ab8	00000007	1	4b202cc0	00000008	1
4b2030d0	0000000a	1	4b2034e0	0000000b	1
4b203f08	0000000c	1	4b204318	0000000d	1
4b200010	0000000e	1	4b200010	0000000f	1
4b200010	00000012	1	4b209458	00000014	1

CallRef. An internal reference to this call used by the PNNI protocol. This number is useful when using a network analyzer to view call activity.

Call Id. An internal reference to this call used by signaling software. The value is similar to the **CallRef** variable except it is used by signaling software rather than PNNI to identify this call.

Dtl. The Designated Transit List (DTL) or correct path associated with this call.

Viewing Current DTLs

The **pdtl** command allows you to view a list of all current Designated Transit Lists (DTLs) in the PNNI database. The list will be limited to 200 DTL entries. The following is a sample of the output shown from the **pdtl** command.

PNNI Designated Transit List Table

(Note that RefCount 0 DTLs are free DTL entries.)

DTL Index	Ref Count	Hop Count	DTL (Node ID + Port ID)
1	0	0	<No DTL>
2	4	3	50a03903488001bc9000010178aee00020da:78aee000 208 50a03903488001bc900001010230e00020da:0230e000 209 50a03903488001bc900001016542fg0020da:6542fg00 210
3	5	3	50a03903488001bc9000010178aee00020da:78aee000 208 50a03903488001bc900001010230e00020da:0230e000 209 50a03903488001bc900001010967df0020da:0967df00 201
4	1	2	50a03903488001bc9000010178aee00020da:78aee000 208 50a03903488001bc900001016542fg0020da:6542fg00 210
6		2	50a03903488001bc900001010230e00020da:0230e000 209 50a03903488001bc900001016542fg0020da:6542fg00 210
7	10	2	50a03903488001bc9000010178aee00020da:78aee000 208 50a03903488001bc900001016542fg0020da:6542fg00 210
8	20	2	50a03903488001bc9000010178aee00020da:78aee000 208 50a03903488001bc9000010178yu650020da:78yu6500 249
9	15	4	50a03903488001bc9000010178aee00020da:78aee000 208 50a03903488001bc900001010230e00020da:0230e000 209 50a03903488001bc9000010178yu650020da:78yu6500 249 50a03903488001bc90000101135jh40020da:135jh400 235
10	6	3	50a03903488001bc9000010178aee00020da:78aee000 208 50a03903488001bc9000010178yu650020da:78yu6500 249 50a03903488001bc90000101135jh40020da:135jh400 235

DTL Index. The internal reference number used by PNNI to identify this Designated Transit List.

Ref Count. The number of calls that have used this DTL to as a path to reach their destination.

Hop Count. The number of hops, or PNNI nodes, on this DTL. This value will be zero (0) until the DTL is actually used by a call. Therefore, if the **Ref Count** column displays a positive number, then the number of hops on this DTL should be listed in this column.

DTL (Node ID + Port ID). A description of the hops, or nodes, that comprise this DTL. Each DTL is described as a number of node and port IDs. Each row describes one node/port in the DTL. The number of node/port pairs should correspond to the number of hops listed in the **Hop Count** column.

Summary Form of pdtl

You can also obtain a summary output of the **pdtl** command that displays the number of DTLs and the number of DTLs that are currently being used. When you enter

```
pdtl -s
```

A screen similar to the following displays:

```
From a total of 200 DTLs, 5 are currently used.
```

Viewing Basic Port Statistics

The **pgstats** command displays statistics for the number of Hello, PTSE, and Database Summary packets sent and received on each CSM port in the OmniSwitch. For the single-peer group version of PNNI, enter

```
pgstats
```

at the system prompt. For the multiple-peer group version of PNNI, the syntax for this command is as follows:

```
pgstats [ <node level>]
```

The **<node level>** option allows you to display the current configuration for a specific node. If you do not use this option, then the **pgstats** command will display the lowest level node. For example, when you enter

```
pgstats
```

a screen similar to the following displays:

PNNI Port Basic Statistical Information

Neighbor	Intf	Hellos Xmtd/Rcvd	PTSPs Xmtd/Rcvd	Dbase Sum Pdus Xmtd/Rcvd
3903488001bc90000101 75ee100020da75ee1000	5/ 2	7 6	7 4	2 3
3903488001bc90000101 72b1b00020da72b1b000	7/ 1	7 6	3 1	5 3

Neighbor. The node identifier of the neighboring peer node.

Intf. The CSM slot and port for which these statistics are compiled. The slot is listed first, followed by a slash (/), and then the port number.

Hello Xmtd/Rcvd. The number of Hello packets transmitted (top value) or received (bottom value) over his link. For links other than those between lowest-level nodes in this peer group, this value will be zero.

PTSPs Xmtd/Rcvd. The number of PTSPs transmitted/retransmitted to (top value) or received from (bottom value) the neighboring peer node. Topology database information in the form of PNNI Topology State Elements (PTSEs) is encoded in PTSPs.

DBase Sum Pdus Xmtd/Rcvd. The number of Database Summary packets transmitted/retransmitted to (top value) or received from (bottom value) the neighboring peer. Database Summary packets contain identifiers of the PTSE data available from the neighboring node's topology database, but these summary packets do not contain the actual PTSE data. To obtain PTSE data, a node issues a PTSE Request packet after receiving a Database Summary packet.

Viewing Port Error Statistics

The **pestats** command displays statistics for the number of errors (i.e., PDU errors and cell discards) sent and received on each CSM port in the OmniSwitch. For the single-peer group version of PNNI, enter

```
pestats
```

at the system prompt. For the multiple-peer group version of PNNI, the syntax for this command is as follows:

```
pestats [ <node level>]
```

The **<node level>** option allows you to display the current configuration for a specific node. If you do not use this option, then the **pestats** command will display the lowest level node. For example, when you enter

```
pestats
```

a screen similar to the following displays:

PNNI Port Error Statistical Information						
Neighbor	Intf	Errors		Discards		
		Incoming	Outgoing	Incoming	Outgoing	
3903488001bc90000101 75ee100020da75ee1000	5/ 2	0	0	0	0	
3903488001bc90000101 72b1b00020da72b1b000	7/ 1	0	0	0	0	

Neighbor. The ATM address for the node on which error statistics are provided.

Intf. The CSM Slot and Port for which error statistics are provided. The slot is listed first, followed by a slash (/), and then the port number.

Errors Incoming. The number of PNNI Protocol Data Unit (PDU) errors that have been received on this port. This figure includes only malformed frames from remote destinations (i.e., outside this peer group). These errors will not occur between neighboring nodes in the same peer group; errors between such nodes will be resolved by the Hello protocol. For example, if there are errors in Hello messages between two nodes in the same peer group, then the link with the neighboring node will simply not be set up and no PDUs will be exchanged.

Errors Outgoing. The number of PNNI Protocol Data Unit (PDU) errors that have been transmitted on this port. These errors occur when the OmniSwitch software driver fails to transmit a frame successfully.

Discards Incoming. The number of PNNI Protocol Data Units (PDUs) that have been discarded on the receive side of this port. Received frames are discarded if they are corrupt, received on a user-disabled CSM port, or received on a port where the Hello state has gone Down.

Discards Outgoing. The number of PNNI Protocol Data Units (PDUs) that have been discarded on the transmit side of this port. Transmit frames are discarded when the OmniSwitch software driver fails to transmit a frame successfully.

Viewing Port PTSE Statistics

The **ppstats** command displays statistics on the number of PTSE requests and acknowledgments sent and received on each CSM port in the OmniSwitch. For the single-peer group version of PNNI, enter

```
ppstats
```

at the system prompt. For the multiple-peer group version of PNNI, the syntax for this command is as follows:

```
ppstats [<node level>]
```

The **<node level>** option allows you to display the current configuration for a specific node. If you do not use this option, then the **ppstats** command will display the lowest level node. For example, when you enter

```
ppstats
```

a screen similar to the following displays:

PNNI Port PTSE Statistical Information						
Neighbor	Intf	PTSE Request		PTSE Acknowledgements		
		Xmtd	Rcvd	Xmtd	Rcvd	
3903488001bc90000101 75ee100020da75ee1000	5/ 2	1	0	2	6	
3903488001bc90000101 72b1b00020da72b1b000	7/ 1	0	1	1	2	

Neighbor. The node identifier for the neighboring peer node.

Intf. The CSM slot and port for which these statistics are compiled. The slot is listed first, followed by a slash (/), and then the port number.

PTSE Request Xmtd. The number of PTSE Request frames transmitted via this CSM port to neighboring peer nodes. PTSE Requests are sent by this node in response to Database Summary packets from neighboring nodes. When this node finds a PTSE for which it requires more information, it sends a PTSE Request to obtain the actual PTSE data referred to in the Database Summary packet.

PTSE Request Rcvd. The number of PTSE Request frames received on this CSM port from neighboring peer nodes. PTSE Requests are sent by neighboring nodes in response to Database Summary packets from this node. When a neighboring node finds a PTSE for which it requires more information it sends a PTSE Request to obtain the actual PTSE data referred to in the Database Summary packet.

PTSE Acknowledgement Xmtd. The number of PTSE Acknowledgment frames transmitted via this CSM port to neighboring peer nodes. PTSE Acknowledgments are sent in response to received PTSEs. When this node receives a PTSE it requested through a PTSE Request packet, it acknowledges this receipt via a PTSE Acknowledgment packet.

PTSE Acknowledgement Rcvd. The number of PTSE Acknowledgement frames received on this CSM port from neighboring peer nodes. PTSE Acknowledgments are sent in response to PTSE Requests. When a node receives a PTSE it requested through a PTSE Request packet, it acknowledges this receipt via a PTSE Acknowledgment packet.

Halting PNNI Operations

The **phalt** command disables the PNNI protocol entity currently running in this OmniSwitch. This command clears out the topology database and all port and node configuration data on this switch. Using **phalt** could result in a loss of network connectivity for this node and could affect databases of PNNI nodes in the same peer group. (The **phalt** command, however, does not unload the PNNI module from system memory.) This command should only be used during off-peak network periods. The **phalt** command must be used before using the **prestart** command (described in *Restarting PNNI* on page 46-89).

For the single-peer group version of PNNI, enter

```
phalt
```

at the system prompt. For the multiple-peer group version of PNNI, the syntax for this command is as follows:

```
phalt [ <node level>]
```

The **<node level>** option allows you to halt PNNI operation at the level indicated. If you do not use this option, then the **phalt** command will halt all PNNI operation in an OmniSwitch at every level. For example, to halt the PNNI protocol at every level, enter

```
phalt
```

The following warning message and confirmation prompt will display:

```
Shutting down the PNNI Operation currently executing in this node could  
cause temporary ATM network routing problems such as network partitioning.  
Which, in turn, could result in a loss of connectivity. Also, remote ATM  
PNNI nodes may experience temporal disinformation as they expire this  
node's PTSEs and neighbor information.
```

```
This typically will not result in a loss of ongoing connections through  
this switch. It will prevent new connections from temporarily being routed  
through this node however. Also, ongoing connections which crankback will be  
discarded, causing them to timeout at the originator.
```

```
Are you absolutely sure you wish to do this? (n) y
```

If you want to continue with the PNNI halt, enter a **Y**. Otherwise, press **<Enter>** and the command will be exited. If you enter **Y**, the following status messages will display as the PNNI entity is brought down:

```
Disabling all available PNNI ports...      OK  
Removing all end systems directly attached... OK  
Removing all statically configured routes... OK  
Unbinding with Upper Call Control...      OK  
Unconfiguring this PNNI Node's basic info... OK  
Freeing buffers...                          OK  
Unconfiguring Dynamic Routing Tables...    OK  
Generating Final Mgmt Event...            OK  
Done.
```

Restarting PNNI

The PNNI protocol entity on this OmniSwitch can be restarted after you halt it via the **phalt** command. The **prestart** command brings the PNNI protocol back up after a halt. Database and configuration information will be set to system defaults upon this restart.

For the single-peer group version of PNNI, enter

```
prestart
```

at the system prompt. For the multiple-peer group version of PNNI, the syntax for this command is as follows:

```
prestart [ <node level>]
```

The **<node level>** option allows you to restart PNNI operation at the level indicated. If you do not use this option, then the **prestart** command will restart all PNNI operation in an OmniSwitch at every level. For example, to restart the PNNI protocol entity, enter:

```
prestart
```

Status messages will display, updating you on the current status of the restart:

```
Generating Mgmt Event...           OK  
Configuring Dynamic Routing Tables... OK  
Configuring this PNNI Node's basic info... OK  
Configuring Call Control service...  OK  
Inserting all end systems directly attached... OK  
Inserting all statically configured routes... OK  
Enabling all available PNNI ports...  OK  
Done.
```

Note that you cannot restart PNNI before disabling it through the **phalt** command. If you do not use the **phalt** command before **prestart**, the following message will display:

```
You must first shut down pnni using phalt
```

Resetting PNNI Statistics Counters

The **preset** command resets all PNNI port statistical counters for this OmniSwitch or for selected PNNI ports. It affects the results of commands on the **Pstats** submenu (**pgstats**, **pestats**, and **ppstats**).

For the single-peer group version of PNNI, the syntax for this command is as follows:

```
preset all | <slot/port>[/<instance>] | <slot/port-list>[/<instance>]
```

For the multiple peer group version of PNNI, the syntax for this command is as follows:

```
preset [ <node level>] all | [ <node level>]<slot/port>[/<instance>] | [ <node level>]  
<slot/port-list>[/<instance>]
```

The **<node level>** option allows you to reset PNNI statistics counters related to a specific node level. The **[/<instance>]** option allows you to specify a specific virtual path tunnel. To reset statistics counters for all PNNI ports in this OmniSwitch, for example, enter the following:

```
preset all
```

the following message will display:

```
PNNI statistics for all interface's have been cleared.
```

To reset statistics for a specific CSM port, enter the **preset** command followed by the slot and port number for the port. For example to reset counters for port 1 on the CSM module in slot 3, enter:

```
preset 3/1
```

You can also enter multiple port numbers to reset several ports on a single CSM module. For example, to reset counters for ports 1 through 4 on the CSM module in slot 3, you would enter:

```
preset 3/1-4
```

The following message would display in response to this command:

```
3/1-4 cleared.
```

In addition, you can also reset the PNNI port statistics counters for a specific virtual path tunnel on a single port or on a range of ports on a CSM module. For example, to reset the PNNI port statistics counter for virtual path tunnel 1 on CSM port 3 in slot 3, enter:

```
preset 3/3/1
```

at the prompt.

Viewing PNNI Configuration Information

The **pvcfg** command displays the type of PNNI information that has been user-configured. This information may have been configured through UI commands or through SNMP-based network management software. You can configure general PNNI parameters, node-specific parameters, and PNNI port-specific parameters. In addition, you can configure IISP route and route property information.

You can see the types of PNNI information that have been configured by entering **pvcfg**. A screen similar to the following displays:

```

pgcfg info
pncfg info
ppcfg 4/4 info
Route property info - property 1
Route instance 0 info for property 1

```

This display shows that general PNNI parameters (**pgcfg info**), node-specific parameters (**pncfg info**), and PNNI port parameters for port 4 on the CSM module in slot 4 (**ppcfg 4/4 info**) has been configured. In addition, a route property template has been set up (**Route property info - property 1**) and one route has been configured using the route property template (**Route instance 0 info for property 1**).

Removing PNNI Configuration Information

When you configure PNNI through UI commands or via SNMP-based network management software, configuration data is stored in the **mpm.cnf** file. The PNNI-specific information in this file may be removed by using the **prmcfg** command. Using **prmcfg** does affect any other non-PNNI information in the **mpm.cnf** file.

The syntax for this command is as follows:

```
prmcfg [-i]
```

The **-i** option will cause the **prmcfg** command to run “interactively.” In other words, you will be prompted before any configuration information is removed.

To remove PNNI configuration information (without prompts), enter

```
prmcfg
```

at a system prompt. PNNI unconfigures any static PNNI information. Run-time PNNI configuration information is not affected. However, when you reset the switch, the factory default configurations for all PNNI parameters will be restored. If you set a port to the PNNI type through the **map** command, then that port will remain a PNNI port after using **prmcfg** and rebooting.

Verifying Routes

Since each PNNI node learns the topology for the whole network, each node has the ability to reach all known destinations. The **prtst** command helps to verify PNNI reachability to a destination. When you issue the command, the system displays how PNNI will attempt to route a call through the network to a destination ATM address you specify.

To verify a route, enter **prtst** followed by the ATM address for which you want to check the route. For example, to check the route to ATM address **4222334455667788990011223344556677889900**, you would enter the following:

```
prtst 4222334455667788990011223344556677889900
```

The system displays a screen showing the Node ID and ports used to reach the address.

**PNNI created the following Designated Transit List to setup this connection:
(Note that the first node in the DTL is displayed first, while the last node is displayed last. For reference, if the downstream switch is an OmniSwitch, its OC3 slot/port is displayed after the logical port id conveyed in the DTL)**

Logical Node ID	Logical Port	XCell Slot/Port
60a0 3903488001bc900001178aee010020da:78aee000	208	(4/3)
current->60a0 3903488001bc900001178db3010020da:78db3000	232	(4/6)

The “current” node is the local OmniSwitch and the other node is the one where the specified ATM address is attached. If the ATM address is not known or if it is attached to the local switch, then a message will be returned informing of the unknown or local address.

Operating PNNI with Redundant MPMs

If you have an OmniSwitch with redundant MPMs, PNNI node configuration parameters can be lost during failover. For example, if you do not specify the switch's node ID, it will change if the primary MPM goes down and the secondary MPM becomes primary. To prevent the switch's PNNI node parameters from changing after a failover, perform the steps described in the subsection below.

As an option, you can verify that the node information is consistent on both MPMs by performing the steps described in *Verifying PNNI Node Information on Redundant MPMs* on page 46-94.

Configuring Node Information on Redundant MPMs

Perform the steps below to configure the same node information on both MPMs.

1. Enter

```
pncfg
```

at the system prompt. (See *Configuring Node-Specific Parameters* on page 46-40 for more information on the **pncfg** command.)

2. Enter **1=** followed by the ATM address of the switch (to change it from **Unspecified**). For example, if the ATM address is **3903488001bc9000010178aee00020da78aee000**, enter

```
1=3903488001bc9000010178aee00020da78aee000
```

at the prompt.

3. Enter **2=** followed by the node ID of the switch (to change it from **Unspecified**). For example, if the node ID is **3903488001bc9000010178aee00020da78aee000**, enter

```
2=3903488001bc9000010178aee00020da78aee000
```

at the prompt.

4. Enter **3=** followed by the node level of the switch (to change it from **Unspecified**). For example, if the node ID is **80** (decimal), enter

```
3=80
```

at the prompt.

5. Enter **6=** followed by the summary address for ILMI clients (to change it from **Unspecified**). For example, if the summary address is **3903488001bc90000178aee0**, enter

```
6=3903488001bc90000178aee0
```

at the prompt.

6. If you have the single-peer group version of the software, proceed to Step 7. If you have the multiple-peer group version of the software, enter **7=** followed by the Peer Group Leader (PGL) priority of the node (to change it from **Unspecified**). For example, if the PGL priority is **50** (decimal), enter

7=50

at the prompt.

7. Enter

save

at the prompt to save your settings. The following prompt will display.

Do you want these changes to take effect immediately? (y)

8. Press **<Enter>** to have your changes take effect immediately.

save

at the prompt to save your settings.

9. Enter

configsync

at the system prompt to synchronize the configuration file on both MPMs. (See Chapter 10, “Configuring Management Processor Modules,” for more information on the **configsync** command.) Messages similar to the following will be displayed.

**Syncing Config file
Config files are currently synchronized.**

Verifying PNNI Node Information on Redundant MPMs

To verify that the PNNI node configurations are the same on both MPMs, perform the following steps.

1. Enter

pncfg

at the system prompt. (See *Configuring Node-Specific Parameters* on page 46-40 for more information on the **pncfg** command.)

2. Copy the ATM address, node ID, node level, and summary address for ILMI displayed in fields 1, 2, 3, and 6, respectively. If you have the multiple-peer group version of the software, copy the PGL priority displayed in field 7.

3. Enter

quit

at the prompt to exit the command.

4. Enter

renounce

at the prompt to make the secondary MPM the primary one. (See Chapter 10, “Configuring Management Processor Modules,” for more information on the **renounce** command.)

5. Log into the new primary MPM.

6. Enter

pncfg

at the system prompt.

7. Compare the data displayed in fields 1, 2, 3, and 6 (and field 7 if you have the multiple-peer group version of PNNI) with the data you copied in Step 2. If the data are not consistent, perform the steps described in *Configuring Node Information on Redundant MPMs* on page 46-93.

FCSM I PNNI Frame Size Guidelines

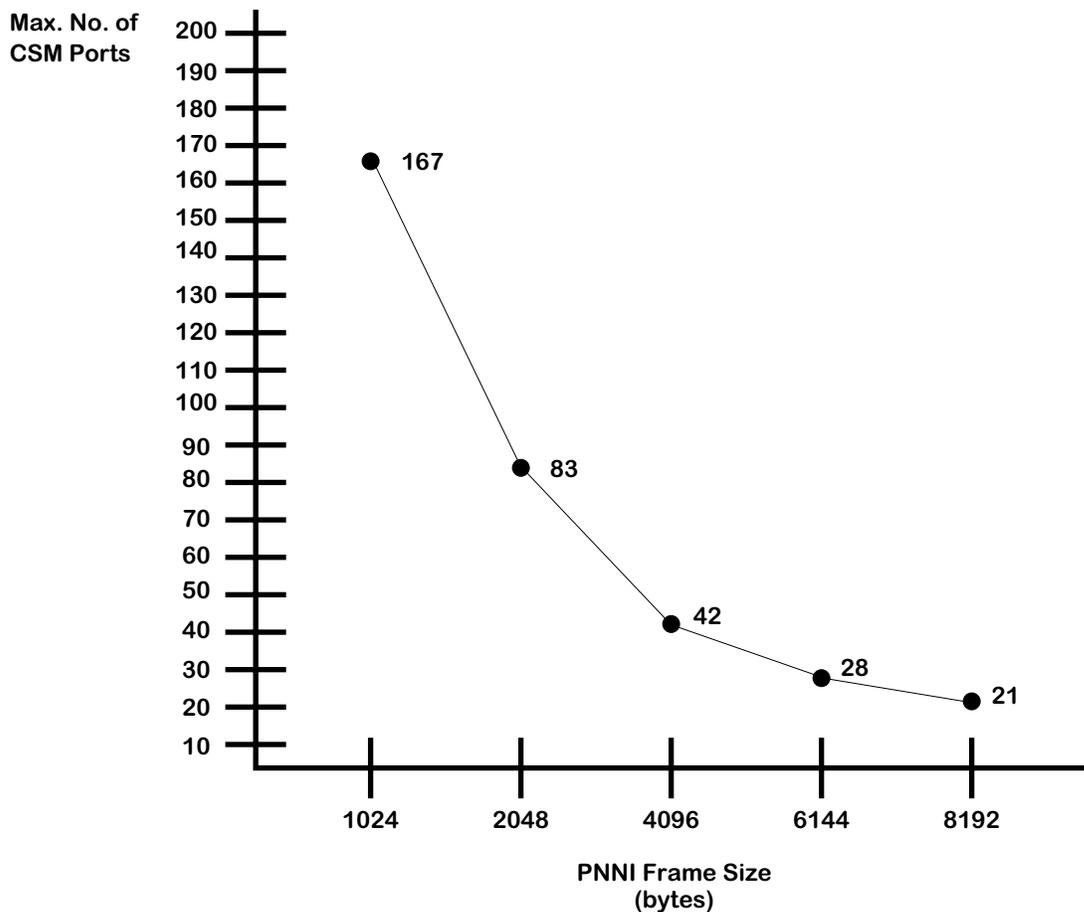
PNNI packet (frame) sizes vary from 16 to 8192 bytes, depending on what type of information is being sent between PNNI nodes. For example, hello packets are approximately 100 bytes long. However, database summaries and PNNI Topology State Elements (PTSEs) exchanged between switches can run from 64 to 8192 bytes long.

As frame sizes increase, the total number of CSM ports you can have decreases on OmniSwitches with an FCSM I. In all-Alcatel network, this is not a problem since Alcatel switches do not generate frames greater than 2048 bytes. However, in multi-vendor networks, frames can be as large as 8192 bytes.

◆ **Note** ◆

This restriction only applies to OmniSwitches with an FCSM I; it does not apply to the FCSM II or MPM-C.

The figure below shows the relationship between PNNI frame size and the maximum number of CSM ports you can have an OmniSwitch with an FCSM I. For example, if you need to support PNNI frames up to 8192 bytes, the total number of CSM ports that you can have in the chassis is limited to 21 CSM ports.



PNNI Frame Size vs. Maximum Number of CSM Ports

You can configure the maximum frame size on the FCSM I with the **map** command, which is described in Chapter 33, “Managing ATM Access Modules.” (You configure the frame size on the ASM side of the FCSM I and not the CSM side.) For example, if the FCSM I is in slot 2, you would enter

```
map 2/2
```

at the system prompt.

When you configure the frame size, you should follow these two guidelines;

- Small-to-medium networks (i.e., up to 20 PNNI nodes): 2048 to 6144 bytes
- Large networks (i.e., more than 20 nodes): 8192 bytes

In addition, the maximum number of PNNI neighbors per PNNI node should be less than, or equal to, 30 neighbors. More than 30 neighbors will trigger higher CPU utilization on the MPM, unless the hello timers are re-configured using the **pnCFG** command with higher values. (See *Configuring Node-Specific Parameters* on page 46-40 for more information on the **pnCFG** command.)

47 Managing IISP and PNNI Routes

PNNI is a dynamic routing protocol that is capable of establishing switched virtual connections based on ATM End System requests. It is also capable of managing connections that use pre-configured static routes. You configure static routes through options on the PNNI Route Management submenu. Static routes are used by the Interim Inter-Switch Signalling Protocol (IISP), which is an ATM static routing protocol.

This Route Management submenu allows you to add and delete static routes. Static routes are useful in directing calls to ATM ports that do not participate in PNNI exchanges or are outside the PNNI peer group.

◆ Important Note ◆

In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. Chapter 8, “The User Interface,” includes documentation on changing from CLI mode to UI mode.

Setting Up Static Routes

Setting up static routes requires two steps:

1. Configure a route property, or template, that describes route characteristics, such as Quality of Service and metrics. This step requires using the **prpadd** command. Instructions for this step start on page 47-3.
2. Add route addresses to one of the pre-configured route properties. All addresses added to a route property will use the characteristics configured for that property. This step requires using the **pradd** command. Before adding a static route address, you must first configure a route property. Instructions for this step start on page 47-9.

In addition, if you want a CSM port to support IISP for static routes, then you must configure the port to be an IISP port in the **map** command. The **map** command is described in Chapter 41, “Managing CSM Modules (CSMs).” There are two types of IISP ports—user side and network side. Be sure you configure your IISP port according to its function.

The PNNI/IISP Route Management Menu

The PNNI/IISP Route Management menu is a submenu of the PNNI menu. It contains commands for viewing learned routes and for configuring and viewing static routes. It displays as follows:

Command	ATM PNNI Route Management Menu
proutea	View the Table of routes from nodes to reachable addresses
prouten	View the Table of routes to other nodes
prpadd	Add a PNNI static route property (type, metrics, TNS)
prpdel	Delete a PNNI static route property
pradd	Add PNNI static route address(es) to a route property
prdel	Delete PNNI static route address(es) from a route property
prp	View PNNI configured route properties
prt	View PNNI configured route prefixes
Related Menus:	
Pconfig	Proute Pinfo Pstats Padmin

The first two commands on this menu (**proutea** and **prouten**) provide information on dynamically learned routes in the network. The remaining commands (i.e., those listed after **prouten**) allow you to configure, delete, or view static route properties and addresses.

Configuring a PNNI/IISP Static Route Property

The **prpadd** command allows you to configure a PNNI/IISP static route property for a given CSM port. Note that a route property may be set up without assigning any actual route addresses. (Static route addresses are assigned to route properties through the **pradd** command. See *Adding a PNNI/IISP Static Route Address* on page 47-9).

Follow the steps below to set up a static route property.

1. Enter **prpadd** followed by the slot and port number of the CSM where this property will be valid. For example, to set up a static route property on port 2 of the CSM module in slot 3, you would enter the following:

```
prpadd 2/3
```

Virtual Path Tunnels. To configure a static route property for a specific virtual path tunnel, you need to include the instance number of the virtual tunnel in the **prpadd** command. (Physical level parameters for virtual tunnels are configured through the **cvpt** command, which is described in Chapter 42, "Advanced CSM Management.") The **prpadd** format for virtual path tunnels is as follows:

```
prpadd <slot>/<port>/<virtual tunnel instance>
```

where **<virtual tunnel instance>** is a unique value assigned to each virtual tunnel on a CSM module port. You can find a specific virtual tunnel instance through the **lvpt** command. If you wanted to configure a static route property for the second virtual tunnel instance on first port on the CSM module in slot 5, you would specify:

```
prpadd 5/1/2
```

After you enter the command line, a display similar to the following displays:

Route Property Configuration for Slot 5 Port 1

```

1) Internal or exterior (i or e)      [i]: Unspecified
2) Scope (1-104)                    [80]: Unspecified
3) VP Capable (t or f)              [t]: Unspecified
4) VPI                               : Unspecified
5) E.164 Address                     : Unspecified

```

6) Topology State Parameter Configuration Menu

7) Associated Transit Network Configuration Menu

To configure a parameter, type "item = value" (as in 1=i)

To quit out of configuration, type "quit"

To save the configured info, type "save"

->

2. To alter a parameter, enter the line number for the parameter, followed by an equal sign (=), and then the new value for the parameter. For example, to change the **Scope** (line 2) from level 80 to 96, you would enter:

```
2=96
```

Options on line numbers 6 and 7 enter submenus with additional configuration parameters. Simply enter the submenu's line number (6 or 7) and press **<Enter>** to go to that submenu. Descriptions for the parameters under option 6 can be found in *Configuring QoS and Metrics for Inbound and Outbound Routes* on page 47-5. Descriptions for parameters under option 7 can be found in *Configuring the Associated Transit Network* on page 47-6.

1) Internal or exterior (i or e)

The type of reachability (internal or exterior) from the advertising node to the end address prefix. Internal means this route property is within this PNNI routing domain, or peer group; specify an **i** here for an internal route property. Exterior means this route property is outside this routing domain, or peer group; specify an **e** for an exterior route property.

2) Scope (1-104)

The PNNI scope (i.e., level within the PNNI hierarchy) where addresses configured on this route property will be advertised. Values may range from 0 to 104, with higher values indicating addresses that are lower in the PNNI hierarchy.

3) VP Capable [t or f]

Indicates whether to advertise to reachable address prefixes that the establishment of Virtual Paths is supported. **True** means Virtual Path capability will be advertised for static routes set up using this property. **False** means Virtual Path capability will not be advertised for static routes set up using this property.

4) VPI

The Virtual Path Identifier (VPI) to use for static route addresses set up using this property. Note that the VPI value you select must be within the range of VPIs established for this CSM port through the **map** command. The range of VPIs available on a CSM port is configured through the **Max VPI Bits** variable in the **map** command; see Chapter 41 for more information.

5) E.164 Address

The E.164 address associated with this route property. E.164 addresses are typically required for routes traversing public carrier networks. In contrast to default OmniSwitch PNNI Node addresses, which have a prefix of 39, E.164 addresses use a prefix of 45.

Note

The OmniSwitch is not a public ATM switch. The E.164 capability allows the OmniSwitch to act as a gateway between a private network and a public ATM switched network.

3. When you have completed configuring parameters, enter **save**. Your new values will be saved and you will exit this menu. If you want to exit this menu without saving changes, simply enter **quit**.

Configuring QoS and Metrics for Inbound and Outbound Routes

Option 6 on the **prpadd** main menu enters a submenu of command options for configuring topology metrics for each Class of Service inbound or outbound on this route. If you enter a **6** at the main **prpadd** screen, the following displays:

Topology State Parameter Configuration for PNNI Port 136 (on 3/2)

		Internal Inbound Metrics		
		Admin Weight	Cell Transfer Delay	Cell Delay Variation
		(a) [0]	(b) [0]	(c) [0]
		=====	=====	=====
1) CBR		Unspecified		
2) Rt-VBR		Unspecified		
3) Nrt-VBR		Unspecified		
4) ABR		Unspecified		
5) UBR		Unspecified		
		Internal Outbound Metrics		
		Admin Weight	Cell Transfer Delay	Cell Delay Variation
		(a) [0]	(b) [0]	(c) [0]
		=====	=====	=====
6) CBR		Unspecified		
7) Rt-VBR		Unspecified		
8) Nrt-VBR		Unspecified		
9) ABR		Unspecified		
10) UBR		Unspecified		

To configure a parameter, type "item = value" (as in 1a=5040)

To quit out of configuration, type "quit"

To save the configured info, type "save"

To return to the route property parameters menu, type "return"

->

You configure topology metrics for a given Class of Service by entering the number for the traffic class type, the letter of the topology metric you want to change (**a**, **b**, or **c**), an equal sign (=), and then the value for the topology metric. For example, if you wanted to set the administrative weight for inbound Available Cell rate (ABR) traffic to 1000, you would enter:

4a=1000

a) Admin Weight

The cumulative administrative weight calculated for the forward (inbound) or backward (outbound) direction on this route. If this metric is not used, its value should be set to 0xFFFFFFFF.

b) Cell Transfer Delay

The cumulative Cell Transfer Delay (in microseconds) for the forward (Inbound) or backward (Outbound) direction of the route. This value is the average time it takes for cells to transmit from any incoming port to the outgoing port in the switch for a particular Class of Service. If this parameter is not used, its value will be set to 0xFFFFFFFF.

c) Cell Delay Variation

The cumulative Cell Delay Variation (in microseconds) for the forward (In) or backward (Outbound) direction of the route. Also referred to as "jitter," this metric is the change that occurs in cell spacing from the time cells leave one node and arrive at another node. If this parameter is not used, its value will be set to 0xFFFFFFFF.

Configuring the Associated Transit Network

Option 7 on the **prpadd** main menu enters a submenu of command options for configuring transit networks associated with this route property. The transit network is a network data must travel through before reaching the destination at the end of the route. The transit network is outside a node's peer group. Transit networks are used to tunnel call requests from an ATM End System in one peer group to an ATM End System in another peer group.

Follow these steps to set up transit networks for a static route property:

1. Enter a **7** at the first screen of **prpadd** options.
2. A screen similar to the following displays:

Transit Network Configuration for Routes on PNNI Port 136 (on 3/2)

1) Number of Associated Transit Networks [0-5]: Unspecified

Enter a **1** followed by an equal sign and then the number of transit networks you want to setup. Press **<Enter>**. You may configure up to five transit networks.

3. A screen similar to the following displays:

Type(a)	Plan(b)	Id(c)
2) 0	0	=====
3) 0	0	=====
4) 0	0	=====

Where Type is 0-7 Plan is 0-15 and ID is less than 20 characters
(all according to ATM Forum Specification Section 5.14.7)

To configure a parameter, type "item = value" (as in 1=2)
To abort out of configuration, type "quit"
To return to the route property parameters menu, type "return"
To save the configured info, type "save"

->

This sample shows three transit networks numbered from 2 through 4.

4. Enter parameters for the first transit network. Start each specification with a **2**, followed by the letter of the parameter (a, b, or c), an equal sign (=), and the value of the parameter. For example, to enter a **Type** of **1**, a **Plan** of **1**, and an **Id** of **Northern Telecom -42**, you would enter:

-> **2a=1, 2b=1, 2c=public_1**

Each of the three transit network parameters are described below.

Type. The type of transit network. The type, which is a 3-bit field in the Reachable Address Information Group (RAIG), may be a national network or other type. The network administrator should consult with the ATM service provider for the correct value to enter here.

Plan. The network identification plan for this transit network. This value, which is a 4-bit field in the Reachable Address Information Group (RAIG), may be an identification code for the particular carrier. The network administrator should consult with the ATM service provider for the correct value to enter here.

Id. A textual identifier for this transit network. Enter a description that identifies the the type and carrier for this transit network.

- 5. Repeat Step 4 for the remaining transit networks. The second transit network specifications should start with a 3, the third transit network starts with a 4, and so on.

The following screen shows an example of what the final transit network specifications might look like:

Transit Network Configuration for Routes on Slot 3 Port 2:

1) Number of Associated Transit Networks [0-5]:3

	Type(a)	Plan(b)	Id(c)
	=====	=====	=====
2)	1	1	public_1
3)	2	14	3900102030405060708
4)	1	5	public_2

Where Type is 0-7 Plan is 0-15 and ID is less than 20 characters
(all according to ATM Forum Specification Section 5.14.7)

To configure a parameter, type "item = value" (as in 1=2)
To abort out of configuration, type "quit"
To return to the route property parameters menu, type "return"
To save the configured info, type "save"
->

Deleting a PNNI/IISP Static Route Property

You can delete a PNNI/IISP static route property that has been previously configured. The **prpdel** command allows you to delete one or more static route properties on a CSM port or ports that you specify.

The command first displays the static routes for the port(s) and then prompts you to enter the routes that you want to delete. The syntax for this command is as follows:

prpdel <slot>/<ports>

For example, to delete static routes on port 2 of the CSM module in slot 3, you would enter:

prpdel 3/2

Virtual Path Tunnels. To delete a static route property for a specific virtual path tunnel, you need to include the instance number of the virtual tunnel in the **prpdel** command. (Physical level parameters for virtual tunnels are configured through the **cvpt** command, which is described in Chapter 42.) The **prpdel** format for virtual path tunnels is as follows:

prpdel <slot>/<port>/<virtual tunnel instance>

where **<virtual tunnel instance>** is a unique value assigned to each virtual tunnel on a CSM module port. You can find a specific virtual tunnel instance through the **lvpt** command. If you wanted to delete a static route property for the second virtual tunnel instance on first port on the CSM module in slot 5, you would specify:

prpdel 5/1/2

A screen similar to the following displays:

Deleting static PNNI route properties for Slot 3 Port 2:

Currently there are 3 route configurations for this port as follows:

Rt	Slot/ Port	Int/ Ext	Scope	Metrics		# Route Prefixes
1	3/2	Int	104	CBR In: configured	Out:configured	2
				RT In: configured	Out:configured	
				NRT In:	Out:	
				ABR In: configured	Out:configured	
				UBR In: configured	Out:configured	
2	3/2	Int	104	CBR In: configured	Out:	2
				RT In:	Out:configured	
				NRT In:	Out:	
				ABR In:	Out:	
				UBR In:	Out:	
3	3/2	Ext	92	CBR In:	Out:	2
				RT In: configured	Out:	
				NRT In:	Out:	
				ABR In:	Out:	
				UBR In:	Out:	

Which property do you wish to delete? (Note that all metric, route prefix and tns info will be deleted as well) (1-3):

Enter the route property number(s) that you want to delete at the prompt at the bottom of the screen. The route numbers are listed in the leftmost column of the table. Once you delete a route, all associated metrics, addresses, and transit network information will be cleared from the database.

Adding a PNNI/IISP Static Route Address

The **pradd** command allows you to add PNNI/IISP route address prefixes to previously configured static route properties. Note that you must set up a static route property through the **prpadd** command first before you can add addresses.

Follow the steps below to add one or more static route address(es).

1. Enter **pradd** followed by the slot and port number where you want to set up the static route address(es). For example, to set up an address for a static route on port 2 of the CSM module in slot 3, you would enter the following:

```
pradd 3/2
```

If there are no static route properties set up for this CSM port, then the following message displays:

```
There are no route properties on this interface. Before you can add route
addresses, first add the property to this interface via the Prpadd command.
```

Virtual Path Tunnels. To add a static route address for a specific virtual path tunnel, you need to include the instance number of the virtual tunnel in the **pradd** command. (Physical level parameters for virtual tunnels are configured through the **cvpt** command, which is described in Chapter 42.) The **pradd** format for virtual path tunnels is as follows:

```
pradd <slot>/<port>/<virtual tunnel instance>
```

where **<virtual tunnel instance>** is a unique value assigned to each virtual tunnel on a CSM module port. You can find a specific virtual tunnel instance through the **lvpt** command. If you wanted to add a static route address for the second virtual tunnel instance on first port on the CSM module in slot 5, you would specify:

```
pradd 5/1/2
```

If static route properties were previously set up for this port (using the **prpadd** command), a display similar to the following appears:

Currently there are 3 route configurations for this port as follows:

Rt	Slot/ Port	Int/ Ext	Scope	Admin Weight Metrics		# Route Prefixes	
==	=====	=====	=====	=====	=====	=====	
1	5/1	Int	104	CBR	In:5000	Out:0	0
				rtVBR	In:0	Out:2000	
				nrtVBR	In:0	Out:0	
				ABR	In:0	Out:0	
				UBR	In:0	Out:0	

Do you wish to add to this property? (y)

2. Enter a **y** at this prompt to begin adding route addresses. If more than one route property exists, you will be prompted to enter the route number for which you want to add addresses. Route numbers are listed in the left-most column of the table.
3. The following prompt displays:

```
1) Number of routes (0-20) : Unspecified
To configure a parameter, type "item = value" (as in 1=2)
To abort out of configuration, type "quit"
To return to the route property parameters menu, type "return"
->
```

Adding a PNNI/IISP Static Route Address

Enter the number of addresses you to configure for this static route property by entering a **1**, an equal sign (=) and the number of addresses to add. Up to 20 route prefixes may be added to a route property.

- After you specify the number of route prefixes, the menu updates to reflect the number of routes you requested to set up, as follows:

Route Address Configuration for Routes on Slot 3 Port 2:

```
1) Number of routes (0-20)           : 2
      Address Prefix (a)              Prefix bit-length (b)
=====
2)                                     0
3)                                     0
```

To configure a parameter, type "item = value" (as in 1=2)
To quit out of configuration, type "quit"
To save the configuration, type "save"

Enter parameters for the first address. Start each specification with a **2**, followed by the letter of the parameter (**a** or **b**), an equal sign (=), and the value of the parameter. For example, to enter an address prefix of **1** and an Length of **75**, you would enter:

-> **2a=4700040006345623000047000400063456230000, 2b=75**

Be sure to separate each parameter specification by a comma (.). Each of the static route address parameters is described below.

Address Prefix. The ATM End System address prefix. This prefix is an ATM address of up to 19 octets. The default address prefix length is set to the number of characters entered here multiplied by 4. For example, if you enter **49**, then the default prefix length is **8** (4 x 2 characters=8).

Prefix Length. The prefix length to be applied to the ATM End System address prefix. This value may range from 0 to 152; it specifies the prefix bit length. This field allows you to change the default prefix length derived from the address prefix entered in column **a**. The **prt** command uses this length when displaying address prefixes.

◆ Note ◆

A prefix with a length of zero (0) specifies a default route for all unmatched addresses.

- Repeat Step 4 for other addresses you want to add. The second address specification should start with a **3**, the third address starts with a **4**, and so on. The following screen shows an example of what the final address specifications might look like:

Route Address Configuration for Routes on Slot 3 Port 2:

```
1) Number of routes (0-20)           : 2
      Address Prefix (a)              Prefix bit-length (b)
=====
2) 4700040006345623000047000400063456230000 75
3) 470005                                     22
```

To configure a parameter, type "item = value" (as in 1=2)
To quit out of configuration, type "quit"
To save the configuration, type "save"

->

Deleting a PNNI/IISP Static Route Address

The **prdel** command allows you to delete one or more PNNI/IISP static route addresses on a CSM port or ports. The command first displays the static routes for the port(s) and then prompts you to enter the routes containing addresses that you want to delete. The syntax for this command is as follows:

prdel <slot>/<ports>

For example, to delete static route addresses on port 2 of the CSM module in slot 3, you would enter:

prdel 3/2

You can also enter the command without a CSM port to obtain a listing of static routes for all CSM ports in the OmniSwitch.

Virtual Path Tunnels. To delete a static route address for a specific virtual path tunnel, you need to include the instance number of the virtual tunnel in the **prdel** command. (Physical level parameters for virtual tunnels are configured through the **cvpt** command, which is described in Chapter 42.) The **prdel** format for virtual path tunnels is as follows:

prdel <slot>/<port>/<virtual tunnel instance>

where **<virtual tunnel instance>** is a unique value assigned to each virtual tunnel on a CSM module port. You can find a specific virtual tunnel instance through the **lvpt** command. To delete a static route address for the second virtual tunnel instance on first port on the CSM module in slot 5, specify:

prdel 5/1/2

Follow these steps to delete a static route address:

1. Enter the **prdel** command followed by a CSM slot number, a slash, and a CSM module port number. If no static route properties have been set up on this port, then a message similar to the following displays:

There are no route properties on this interface.

If there are static route properties on this port, then a list of routes displays, as follows:

Currently there are 3 route configurations for this port as follows:

Rt	Slot/ Port	Int/ Ext	Scope	Metrics	# Route Prefixes	
1	3/2	Int	80	CBR In: configured RT In: configured NRT In: ABR In: configured UBR In: configured	Out:configured Out:configured Out: Out:configured Out:configured	2
2	3/2	Int	80	CBR In: configured RT In: NRT In: ABR In: UBR In:	Out: Out:configured Out: Out: Out:	2
3	3/2	Ext	80	CBR In: RT In: configured NRT In: ABR In: UBR In:	Out: Out: Out: Out: Out:	2

From which route property do you wish to delete reachable addresses? (1-3): 1

Deleting a PNNI/IISP Static Route Address

2. Enter the number for the static route property containing the addresses you want to delete. Route property numbers are in the left-most column of the table. If there are no addresses assigned to the static route property you enter, then the following message displays:

There are no reachable addresses configured for this route property.

If there are associated addresses, then a listing of addresses follows:

The following reachable addresses exist:

	Address Prefix (a)	Prefix bit-length (b)
	=====	=====
2)	4700040006345623000047000400063456230000	152
3)	470005	22

Delete which prefixes? (return when done)

->

3. Enter the address number that you want to delete. Address numbers are in the leftmost column of the table. Repeat entering address numbers until you have deleted all those addresses that you want to delete. When you have finished deleting addresses, simply press **<Return>** without entering an address line number.

If you remove all addresses associated with a given static route property, the following message displays:

Since you've removed all prefixes, do you wish to remove this property and its associated metrics and TNS configurations as well? (y,n):

4. Enter a **Y** if you want to delete the entire static route property. You are not required to delete the route property, since you can add other addresses to it later. Enter an **N** if you do not want to delete the route property.

Viewing PNNI/IISP Static Route Properties

The **prp** command displays currently configured PNNI/IISP static route properties in this switch. These route properties, or templates, were configured through the **prpadd** command. The syntax for this command is as follows:

```
prp <slot>/<ports>
```

For example, if you wanted to view the current static route properties configured on port 2 of the CSM module in slot 3, you would enter:

```
prp 3/2
```

In addition, you can view the route properties for a specific virtual path tunnel on a CSM port. Simply enter the virtual tunnel instance after the slot and port. For example, to view the current static route properties configured for virtual tunnel instance 1 on port 2 of the CSM module in slot 3, you would enter:

```
prp 3/2/1
```

You could also view route properties for the entire switch by entering the command with no slot and port parameters:

```
prp
```

After you enter the command, the number of currently configured route properties displays, followed by information on these route properties. The following display shows a sample of the output from the **prp** command:

Currently there is 1 route configurations as follows:

Rt	Slot/ Port	Int/ Ext	Scope	Admin Weight Metrics			TNS in use	# Route Prefixes
==	=====	=====	=====	=====	=====	=====	=====	=====
1	5/1	Int	80	CBR	In:5000	Out:0	Y	0
				rtVBR	In:0	Out:2000		
				nrtVBR	In:0	Out:0		
				ABR	In:0	Out:0		
				UBR	In:0	Out:0		

Rt. The route index number uses to identify this property in the table.

Slot/Port. The CSM slot and port on which this route property was configured.

Int/Ext. Indicates whether this route is and interior route (i.e., within the same peer group) or an exterior route (i.e., outside the peer group).

Scope. The level within the PNNI hierarchy where this route property is configured.

Admin Weight Metrics. Indicates whether metrics have been configured for a given Class of Service. Service classes are listed with the current status of Incoming and Outgoing traffic. If metrics have been configured, then the field next to the class name will read **configured**. If no metrics are configured for a service class, then the field next to the service class name will be blank.

TNS in use. Indicates whether associated transit networks were set up for this route property.

Route Prefixes. The number of route addresses configured for this property through **Pradd**.

Viewing PNNI/IISP Static Route Prefixes

The **prt** command displays currently configured PNNI/IISP address prefixes for this switch. These address prefixes were configured through the **pradd** command. The syntax for this command is as follows:

```
prt <slot>/<ports>
```

For example, if you wanted to view the current static route addresses configured on port 2 of the CSM module in slot 3, you would enter:

```
prt 3/2
```

In addition, you can view the static route addresses for a specific virtual path tunnel on a CSM port. Simply enter the virtual tunnel instance after the slot and port. For example, to view the current static route addresses configured for virtual tunnel instance 1 on port 2 of the CSM module in slot 3, you would enter:

```
prt 3/2/1
```

You could also view static route addresses for the entire switch by entering the command with no slot and port parameters:

```
prt
```

After you enter the command, the number of currently configured route addresses are displayed. The following display shows a sample of the output from the **prp** command:

ATM PNNI Configured Route Prefixes

Prefix Len	Address Prefix	Slot Port	Internal/ Exterior	Scope
0	-- Default Route --	3/3	Ext	20
20	47001	3/3	Int	104
20	47002	3/3	Int	104
20	47003	3/3	Int	104
80	47000400081e2f400005	3/3	Int	104

Prefix Len. The number of octets included in the address prefix.

Address Prefix. The address prefix configured for the static route.

Slot/Port. The CSM slot and port where this address was configured.

Internal/Exterior. Indicates where this address is in the same peer group as this node (**Int**) or whether it is outside this peer group (**Ext**).

Scope. Indicates the scope, or level within the PNNI hierarchy, for this address.

Viewing Learned PNNI/IISP Routes to Reachable Addresses

The **proutea** command displays all PNNI/IISP routes learned by this node to reachable ATM End System addresses in the peer group. This table indicates which ES addresses PNNI believes are reachable from this node. When you enter **Proutea** a screen similar to the following displays:

PNNI Route Table From Nodes To Reachable Addresses

```

Addr Prefix: 3903488001bc9000010178aee00020da78aee0(len=152) Type:Internal
Advrtsed by: 50a03903488001bc9000010178aee00020da78aee000 port:0 (MYSELF)
Learned via: Local Scope: 80 VP Capable:FALSE PTSE:1
on: TUE FEB 10 15:14:38 1998
=====
Addr Prefix: 3903488001bc9000010178aee0(len=104) Type:Internal
Advrtsed by: 50a03903488001bc9000010178aee00020da78aee000 port:1 (MYSELF)
Learned via: Local Scope: 80 VP Capable:FALSE PTSE:2
on: TUE FEB 10 15:14:38 1998
=====
Addr Prefix: 3903488001bc900001017a1bd00020da7a1bd0(len=152) Type:Internal
Advrtsed by: 50a03903488001bc900001017a1bd00020da7a1bd000 port:0
Learned via: PNNI Scope: 80 VP Capable:FALSE PTSE:1
on: THU FEB 12 16:43:21 1998
=====
Addr Prefix: 3903488001bc900001017a1bd0(len=104) Type:Internal
Advrtsed by: 50a03903488001bc900001017a1bd00020da7a1bd000 port:1
Learned via: PNNI Scope: 80 VP Capable:FALSE PTSE:2
on: THU FEB 12 16:43:21 1998

```

Addr Prefix. The value of the ATM End System address prefix.

len. The prefix length to be applied to the ATM End System address prefix.

Type. The type of reachability from the advertising node to the address prefix. This value will be **Internal** (within the same peer group) or **Exterior** (uplink or border link to another peer group). A value of **Reject** refers to an address prefix which if matched indicates that the message should be discarded as unreachable. This value is used in some protocols as a means of correctly aggregating routes.

Advrtsed by. The node ID of a node advertising reachability to the address prefix. If the local node index is zero, then the advertising node ID must be set to all zeros.

port. The port identifier used by the advertising node to reach the given address prefix.

Learned via. The routing mechanism through which the connectivity from the advertising node to the reachable address prefix was learned. A value of **Local** means the the reachable address prefix was learned through ILMI. **Mgmt** means the reachable address was configured statically through SNMP or the User Interface. **PNNI** means the address was learned through the PNNI routing protocol.

Learned on. Indicates the time and date when the connectivity from the advertising node to the reachable address prefix became known to the local node.

Scope. The PNNI scope of advertisement (i.e., level within the PNNI hierarchy) from the advertising node to the address prefix.

VP Capable. Indicates whether the establishment VPCs from the advertising node to the reachable address prefix is advertised.

PTSE. The identifier for the PTSE that describes the reachable address. For reachable addresses learned by means other than PNNI, this attribute is set to zero.

Summary Output for proutea

You can also obtain summary output for the **proutea** command that displays just address information. By using the **-s** flag with **proutea** as follows:

```
proutea -s
```

you obtain output similar to the following:

PNNI Route Table From Nodes To Reachable Addresses (Summary)

Address Prefix	Advertised by Node (on port)
3903488001bc900001017a1bd00020da7a1bd0	50a03903488001bc900001017a1bd00020da7a1bd000 (0) (MYSELF)
3903488001bc900001017a1bd0	50a03903488001bc900001017a1bd00020da7a1bd000 (1) (MYSELF)
47007900000000000000000000000000a03e000001	50a03903488001bc900001017a1bd00020da7a1bd000 (248) (MYSELF)

Each **Address Prefix/Advertised by Node** pair is organized as a two-line step. The **Address Prefix** is on the first line, and is left justified. The **Advertised by Node** variable is on the second line, and is indented such that it is right justified within the table.

Viewing PNNI/IISP Learned Routes to Other Nodes

The **prouten** command displays all known PNNI/IISP routes between this node and other nodes. This table indicates which nodes PNNI believes are reachable from this node. Only nodes within the same peer group are listed.

When you enter **prouten** a screen similar to the following displays:

PNNI Table Of Routes To Other PNNI Nodes

Node: 50a03903488001bc900001017a1bd00020da7a1bd000							Class: UBR
Learned via: PNNI on: THU FEB 12 16:43:21 1998							
Admin Wt	Max CR	Avail CR	Cell TD	Cell DV	CLR(CLP=0)	CLR(CLP=0+1)	
In/Out	In/Out	In/Out	In/Out	In/Out	In/Out	In/Out	
5040	350000	350000	10	2	8	8	
5040	350000	350000	10	2	8	8	
=====							
Node: 50a03903488001bc900001017a1bd00020da7a1bd000							Class: CBR
Learned via: PNNI on: THU FEB 12 16:43:21 1998							
Admin Wt	Max CR	Avail CR	Cell TD	Cell DV	CLR(CLP=0)	CLR(CLP=0+1)	
In/Out	In/Out	In/Out	In/Out	In/Out	In/Out	In/Out	
5040	350000	350000	10	2	8	8	
5040	350000	350000	10	2	8	8	
=====							
Node: 50a03903488001bc900001017a1bd00020da7a1bd000							Class: VBR-Rt
Learned via: PNNI on: THU FEB 12 16:43:21 1998							
Admin Wt	Max CR	Avail CR	Cell TD	Cell DV	CLR(CLP=0)	CLR(CLP=0+1)	
In/Out	In/Out	In/Out	In/Out	In/Out	In/Out	In/Out	
5040	350000	350000	10	2	8	8	
5040	350000	350000	10	2	8	8	
=====							
Node: 50a03903488001bc900001017a1bd00020da7a1bd000							Class: VBR-Nrt
Learned via: PNNI on: THU FEB 12 16:43:21 1998							
Admin Wt	Max CR	Avail CR	Cell TD	Cell DV	CLR(CLP=0)	CLR(CLP=0+1)	
In/Out	In/Out	In/Out	In/Out	In/Out	In/Out	In/Out	
5040	350000	350000	10	2	8	8	
5040	350000	350000	10	2	8	8	
=====							
Node: 50a03903488001bc900001017a1bd00020da7a1bd000							Class: ABR
Learned via: PNNI on: THU FEB 12 16:43:21 1998							
Admin Wt	Max CR	Avail CR	Cell TD	Cell DV	CLR(CLP=0)	CLR(CLP=0+1)	
In/Out	In/Out	In/Out	In/Out	In/Out	In/Out	In/Out	
5040	350000	350000	10	2	8	8	
5040	350000	350000	10	2	8	8	

Node. The node ID of the destination node to which this route proceeds and where the Designated Transit List (DTL) stack for this route terminates.

Class. The service category with which this forwarding table entry is associated. The values will be CBR, rtVBR, nrtVBR, ABR, or UBR.

Learned via. The routing mechanism through which the connectivity from the advertising node to the reachable address prefix was learned. A value of **Local** means the the reachable address prefix was learned through ILMI. **Mgmt** means the reachable address was configured statically through SNMP or the User Interface. **PNNI** means the address was learned through the PNNI routing protocol. The time and date at which this route was last updated or otherwise determined to be correct is also reported.

Traffic Metrics and Attributes

Admin Wt. The cumulative administrative weight calculated for the forward (In) or backward (Out) direction on this route. If this metric is not used, its value should be set to 0xFFFFFFFF.

Max CR. The maximum possible cell rate (in cells per second) for the forward (In) or backward (Out) direction of this route. If this parameter is not used, its value will be set to 0xFFFFFFFF.

Avail CR. The Available Cell Rate (in cells per second) for the forward (In) or backward (Out) direction of the route. The Available Cell Rate is the amount of bandwidth available on this route; this value is dynamic, and changes depending on usage of the link. If this parameter is not used, its value will be set to 0xFFFFFFFF.

Cell TD. The cumulative Cell Transfer Delay (in microseconds) for the forward (In) or backward (Out) direction of the route. This value is the average time it takes for cells to transmit from any incoming port to the outgoing port in the switch for a particular Class of Service. If this parameter is not used, its value will be set to 0xFFFFFFFF.

Cell DV. The cumulative Cell Delay Variation (in microseconds) for the forward (In) or backward (Out) direction of the route. Also referred to as “jitter,” this metric is the change that occurs in cell spacing from the time cells leave one node and arrive at another node. If this parameter is not used, its value will be set to 0xFFFFFFFF.

CLR(CLP=0). The cumulative Cell Loss Ratio for CLP=0 traffic for the forward (In) or backward (Out) direction of the route. This value is the ratio of the number of lost CLP=0 cells to the total number of CLP=0 cells transmitted across a link. If this parameter is not used, its value will be set to 0xFFFFFFFF.

CLR(CLP=0+1). The cumulative Cell Loss Ratio for CLP=0+1 traffic for the forward (In) or backward (Out) direction of the route. This value is the ratio of the number of lost CLP=0+1 cells to the total number of CLP=0+1 cells transmitted across a link. If this parameter is not used, its value will be set to 0xFFFFFFFF.

Summary Output for prouten

You can also obtain a summary display of information in the **prouten** command. The display shows just the Node Id, the Class of Service on that node, and the Administrative Weight assigned to that Class of Service.

When you enter the **prouten** command using the **-s** flag as follows:

prouten -s

you can obtain a table similar to the following:

**PNNI Table Of Routes To Other PNNI Nodes
(Summary)**

Node Id	Class	Admin Weight	
		In	Out
50a03903488001bc900001017a1bd00020da7a1bd000	UBR	0	0 (MYSELF)
50a03903488001bc900001017a1bd00020da7a1bd000	CBR	0	0 (MYSELF)
50a03903488001bc900001017a1bd00020da7a1bd000	VBR-Rt	0	0 (MYSELF)
50a03903488001bc900001017a1bd00020da7a1bd000	VBR-Nrt	0	0 (MYSELF)
50a03903488001bc900001017a1bd00020da7a1bd000	ABR	0	0 (MYSELF)

48 Managing WAN Switching Modules

Introduction

The WAN Switching Modules (WSMs on the OmniSwitch and WSXs on the Omni Switch/Router) are a family of modules that enable the creation of WANs by providing connectivity between geographically-distanced LANs. These modules support a variety of protocols, including Frame Relay, synchronous Point to Point Protocol (PPP), and Integrated Services Digital Network (ISDN).

◆ Note ◆

All WSM software features discussed in this chapter also apply to the Omni Switch/Router WSX.

WSMs extend the power and flexibility of LAN switching over greater geographic distances using either a Frame Relay network, ISDN network or leased line connection, such as T1. In a Frame Relay network configuration, WSMs provide a cost-effective link that is capable of supporting multiple virtual circuits. In a leased line configuration, WSMs provide dedicated bandwidth to a single remote site. In an ISDN line configuration, the WSM supports both inbound and outbound call circuits for interconnection to remote WAN Switching Modules or other devices that support standard PPP over ISDN. In addition, an ISDN configuration supports bandwidth on demand and backup of failed lines.

The family of WSM and WSX modules provides either 2, 4, or 8 ports, which provide a range of access rates from 9.6 kbps to 2 Mbps. Management, data handling, compression, and multi-protocol encapsulation are compatible with the current Frame Relay and PPP standards.

VLAN architectures are preserved and consistent on both sides of a WAN link. WSMs support Alcatel Frame Relay trunking. As a result, VLAN groups on one side of a Frame Relay link are compatible with those on the other side. In addition, the WSM/WSX is capable of both Frame Relay and PPP transparent bridging, and IP and IPX routing.

VLAN architectures are preserved and consistent on both sides of a WAN link. The WSM supports standard RFC 1490 multiprotocol over Frame Relay and synchronous PPP for bridging and routing interoperability with numerous other WAN networking devices. In addition, the WSM supports Alcatel Frame Relay trunking, so multiple VLAN groups on one side of a Frame Relay link can be transported across the WAN.

Type of Service (ToS)

The Type of Service (ToS) settings allow you to prioritize voice data and voice signaling data. Since voice data is time critical, and requires steady throughput, it should be given higher priority than other forms of data. This can be done by assigning a priority value for the Voice Data and Voice Signaling Data fields.

There are two methods of specifying the ToS priority: IP Precedence and Differentiated Services Code Point (DSCP). Both of these methods use a binary value to indicate priority. IP Precedence uses three bits, and DSCP uses six bits; therefore the values for IP Precedence range from 0 to 7, and the values for DSCP range from 0 to 63. The higher the number, the higher the priority of the traffic. IP Precedence uses the most significant (upper) 3 bits, and DSCP uses the most significant (upper) 6 bits.

◆ Important Note ◆

The ToS setting is a feature of Quality of Service (QoS). It was set into the UI to make Voice over IP (VoIP) modules compatible with an Omni Switch/Router that does not have QoS installed. If the QoS image is installed (**qos.img**) on the switch, the UI ToS commands do not function. They are overridden by standard QoS functionality.

Currently, the defaults set for voice data and signaling data are the setting recommended by both Alcatel and Cisco. The default values for switches use hexadecimal forms of IP Precedence; the default value for voice data is 5 decimal, and the default value for signaling is 3 decimal.

Below is a table that shows the relation of IP Precedence levels and DSCP levels.

Relation of IP Precedence, DSCP, and Level of Priority

Priority Level	IP Precedence Value (Decimal)	DSCP Value Range (Decimal)
Routine	0	0 - 7
Priority	1	8 - 15
Immediate	2	16 - 23
Flash	3	24 - 31 (AF31)
Flash-Override	4	32 - 39
Critical	5	40 - 47 (EF)
Internet	6	48 - 55
Network	7	56 - 63

If you feel that changing the default values is imperative to the working of the network, the following table is provided to give the hexadecimal values for various settings:

Hexadecimal Settings

IP Precedence Value	Hexadecimal Value	DSCP Value	Hexadecimal Value
0	0	0	0
1	20	10 (AF11)	28
2	40	18 (AF21)	48
3*	60	26 (AF31)*	68
4**	80	34 (AF41)**	88
5***	a0	46 (EF)***	b8
6	c0	54	d8
7	e0	62	f8

*Default settings for signalling data.

**Cisco suggested default settings for video data.

***Default settings for voice data.

A bit mask is also set with the UI in hexadecimal form. The mask is used during the lookup phase of ToS and screens out the insignificant bits. For IP precedence, the mask should be set to **e0** (this is the default value). For DSCP, the mask is **fc**.

◆ Important Note ◆

These values are set to work with the Alcatel VoIP modules. DO NOT attempt to change them unless you are an advanced user with detailed knowledge of Alcatel products and how they interact.

Supported Physical Interfaces

The WSM and WSX family of products support numerous physical interface (port) types. The port types available with the WSM and WSX family are:

Universal Serial Port

The Universal Serial Port (USP) provides connectivity to legacy synchronous serial port devices. With the addition of an adapter cable, it supports RS-232, RS-449, RS-530, V.35 and X.21 Data Terminal Equipment (DTE) and Data Carrier Equipment (DCE) interfaces at speeds up to 2.048 Mbps. USPs support access via Frame Relay or synchronous PPP. The WSM/WSX automatically detects the cable type connected and will configure the correct physical interface to use.

ISDN Basic Rate Interface Port

The ISDN Basic Rate Interface (BRI) port supports either a U or S/T interface (jumper selectable) for interfacing to public or private ISDN networks. Synchronous PPP is supported on the two bearer (B) channels. Multiple ISDN switch protocol variations are supported on the delta (D) channel (used for signaling). Each B channel runs at 64 kbps, and the D channel runs at 16 kbps.

Fractional T1 Port

The fractional T1 port connects directly to North American and Japanese circuit switch digital data public or private networks without requiring an external Digital Service Unit/Channel Service Unit (DSU/CSU). The port provides an integral DSU/CSU function with both short-haul (i.e., short distance) and long-haul (i.e., long distance) capabilities. The port allows the user to configure a range of time slots from 1 to 24 time slots used to allow for full T1 (all 24 time slots used) or a fractional T1 (less than 24 time slots) service. The fractional T1 port can support access via Frame Relay or synchronous PPP.

◆ Note ◆

For public digital networks, check with your service provider. They may allow only connections that use a configured short-haul interface via a network-provided Channel Service Unit (CSU).

Fractional E1 Port

The fractional E1 port connects directly to ITU-T standard circuit switch digital data public or private networks without requiring an external DSU/CSU. The port provides an integral DSU/CSU function with both short-haul (i.e., short distance) and long-haul (i.e., long distance) capabilities. The port allows you to configure for full E1 (all 30 or 31 time slots used) or fractional E1 (1-29 time slots) service. The fractional E1 port supports access via either Frame Relay or synchronous PPP.

◆ Note ◆

For public digital networks, check with your service provider. They may allow only connections that use a configured short-haul interface via a network-provided Channel Service Unit (CSU).

Supported Protocols

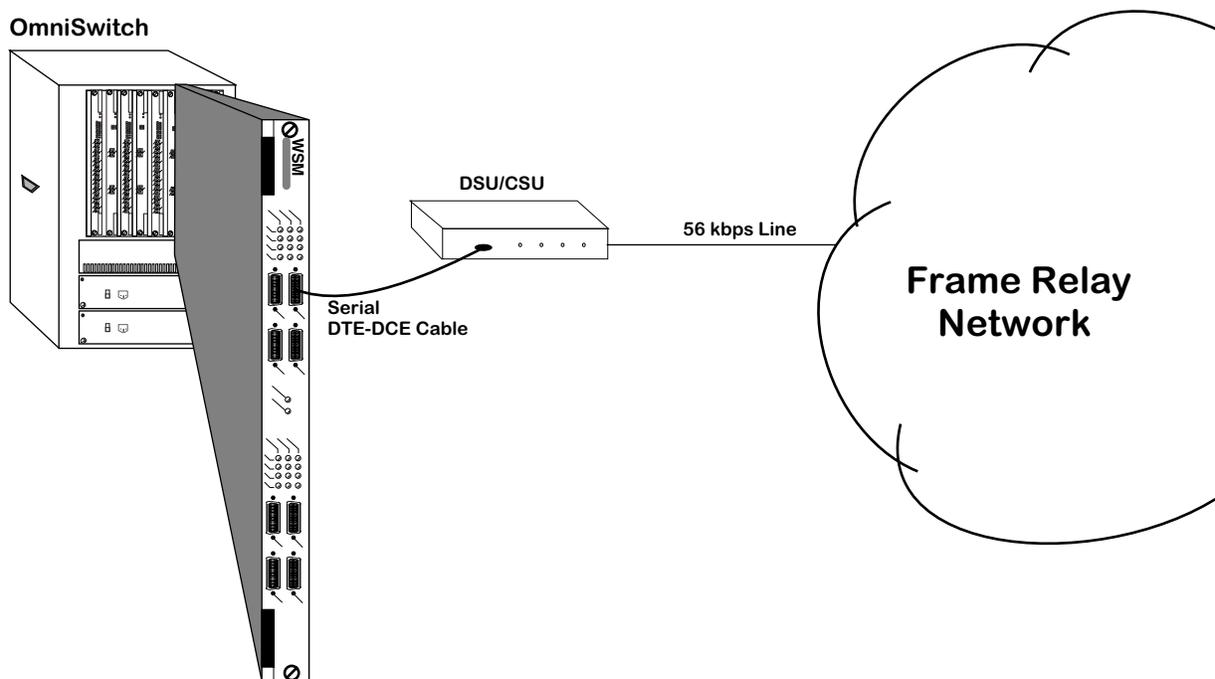
The WAN switching modules support both Frame Relay and synchronous Point-To-Point Protocol (PPP). For ISDN signalling protocols, the modules support D-channel signalling (see Chapter 52, “Managing ISDN Ports.” For more details on implementing these protocols, see Chapter 49, “Managing Frame Relay,” and chapter 50, “Point-to-Point Protocol.”

Application Examples

This section provides several examples of the types of WAN networking possible using WAN switching modules.

Frame Relay WSM/WSX Using Serial Ports

In a typical configuration, the WSM/WSX occupies either a slot in a switch chassis or a submodule in an OmniAccess 512. Because it is compatible with OmniSwitch any-to-any switching and VLAN architecture, you can switch other topologies in the LAN to Frame Relay or PPP. The WSM/WSX connects to a DSU/CSU or T1 multiplexer through a serial cable. The following diagram shows a typical WSM/WSX setup using a 56 kbps Frame Relay line (up to 2 Mbps access rates are supported).



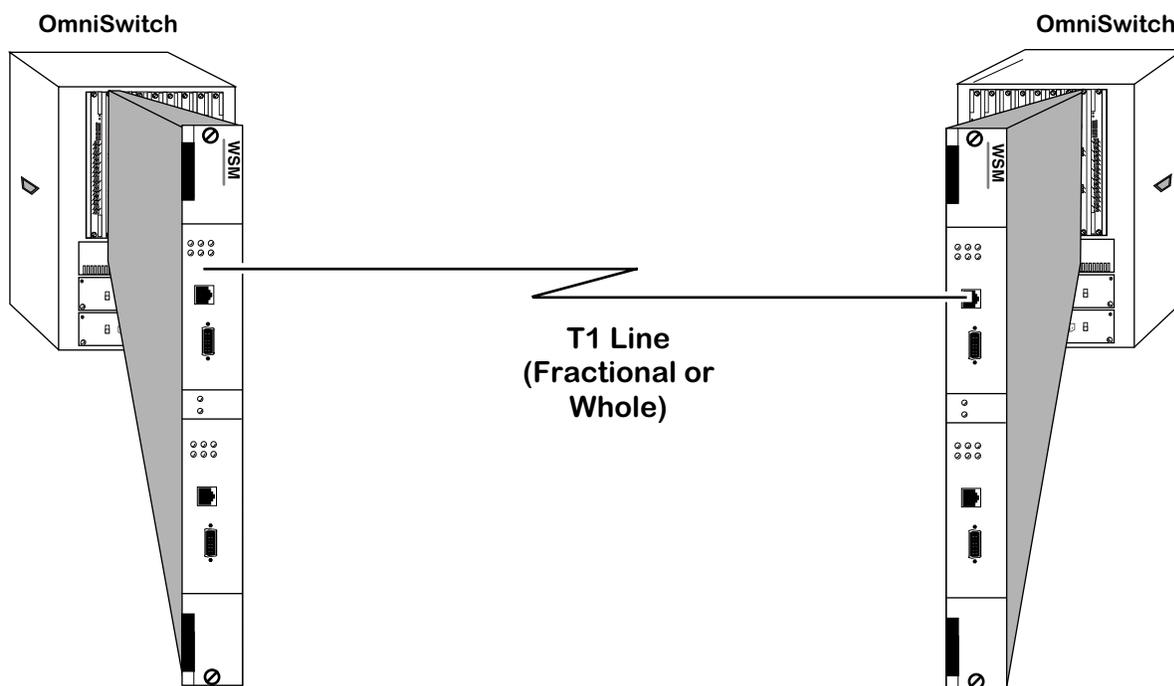
WSM/WSX Frame Relay Configuration Using Serial Ports

For serial ports, the WSM/WSX supports automatic detection of cable types. It also supports internal, external, and split clocking.

Software in the switch allows you to configure access rate, clocking and protocol-related parameters. Additional software commands allow you to view status at the WSM/WSX board, port, or protocol level. Extensive statistics are provided at each level, including a breakdown of traffic by frame type (Ethernet, IP, IPX, or BPDU) at the virtual circuit or PPP connection level.

Back-to-Back WSM/WSX Using T1 Ports

WAN switching modules may be connected “back-to-back” without an intervening Frame Relay network or switch. Because the T1 port internally provides a DSU/CSU function, an external DSU/CSU is not required. Such connections are made by using private leased lines, such as T1 lines, instead of public Frame Relay networks, usually over large geographic distances.

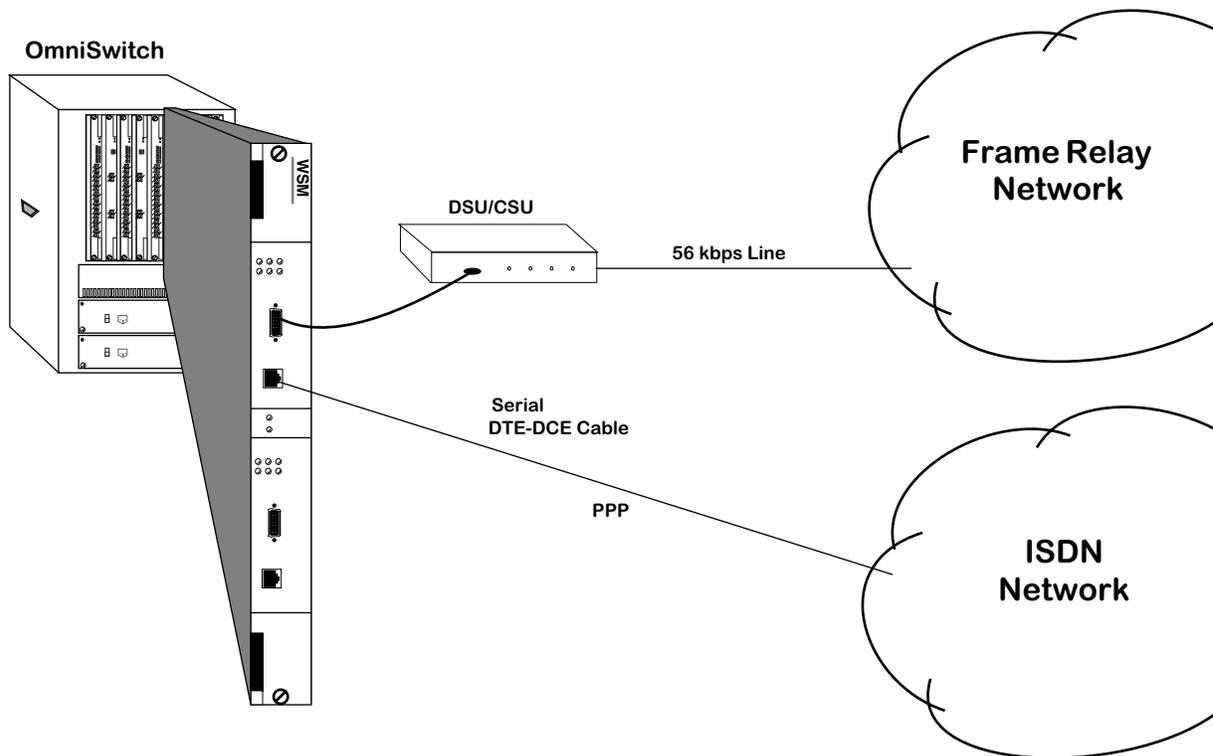


Back-to-Back Configuration Using Fractional T1 Ports

Combined Frame Relay with ISDN Backup

In a typical configuration, the WSM/WSX occupies either a slot in a switch chassis or a submodule on an OmniAccess 512. Because it is compatible with OmniSwitch any-to-any switching and VLAN architecture, you can switch other topologies in the LAN to Frame Relay or PPP. The WSM/WSX connects to a DSU/CSU or T1 multiplexer through a serial cable. The following diagram shows a typical WSM/WSX setup using a 56 kbps Frame Relay line (up to 2 Mbps access rates are supported)

Refer to the Chapter 49, “Managing Frame Relay,” and Chapter 55, “Backup Services,” for details on how to implement this configuration.



OmniSwitch WAN Modules

The OmniSwitch currently supports four Wide Area Network modules:

- WSM-S Provides two, four, or eight serial ports that support Frame Relay or PPP.
- WSM-SC Provides 4 or 8 serial ports that support the frame relay or PPP protocol. In addition, hardware compression is also supported.
- WSM-FT1/E1 Provides one or two T1/E1 ports and one or two serial ports that support Frame Relay or PPP.
- WSM-BRI Provides one USP (Universal Serial Port) and one ISDN-BRI port that support Frame Relay or PPP.

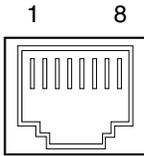
The Omni Switch/Router currently supports five Wide Area Network modules:

- WSX-S-2W Provides two serial ports that support the frame relay or PPP protocol.
- WSX-SC Provides 4 or 8 serial ports that support the frame relay or PPP protocol. In addition, hardware compression is also supported.
- WSX-FT1/E1-SC Provides one or two T1/E1 ports and one or two serial ports that support the frame relay or PPP protocol
- WSX-BRI-SC Provides one or two UPS (Universal Serial Port) and 1 or 2 ISDN-BRI ports that support Frame Relay or PPP
- WSX-M013 Provides two or four channelized DS3 ports

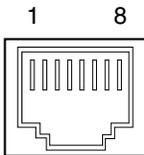
The WSX-S-2W, WSX-SC, WSX-FT1/E1-SC, and WSX-BRI-SC modules for the Omni Switch/Router are described in Chapter 3, “Omni Switch/Router Switching Modules.” The WSX-M013 module for the Omni Switch/Router is described in Chapter 56, “Managing Channelized DS3.” WAN modules for the OmniSwitch are described in the sections that follow.

WAN Pinouts

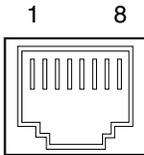
The figures and tables below and on the following pages illustrate the pinouts used on OmniSwitch WAN modules. Please note that the signal commonly known as “remote loop-back” (LL) is not supported on the WAN serial port (see *WAN Serial Port Specifications* on page 48-11). See Appendix B, “Custom Cables,” for information on cables used to connect the serial connector to different interface types.



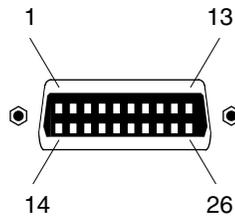
WAN BRI Port Specifications (S/T Interface)	
Pin Number	Standard Signal Name
1	Not Used
2	Not Used
3	Rcv + from TE
4,	Rcv - from TE
5	Xmt + from TE
6	Xmt - from TE
7	Not Used
8	Not Used



WAN BRI Port Specifications (U Interface)	
Pin Number	Standard Signal Name
1	Not Used
2	Not Used
3	Xmt to /Rcv from Network
4,	Xmt to /Rcv from Network
5	Not Used
6	Not Used
7	Not Used
8	Not Used



WAN T1/E1 Port Specifications	
Pin Number	Standard Signal Name
1	Rx_Ring
2	Rx_Tip
3	Chassis GND
4,	Tx_Ring
5	Tx_Tip
6	Chassis GND
7	Chassis GND (A jumper is provided for connecting Pins 7 and 8 to the chassis ground, if required.)
8	Chassis GND (A jumper is provided for connecting Pins 7 and 8 to the chassis ground, if required.)



WAN Serial Port Numbering

WAN Serial Port Specifications							
Generic Signal Name	Source	Alcatel SPI		EIA-530		RS-449	
		Mnemonic	Pin	Mnemonic	Pin	Mnemonic	Pin
Shield	--	Shield	1	--	1	--	1
Signal Ground	--	AB	7	AB	7	SG	19
Transmitted Data	DTE	TD(A)	2	BA(A)	2	SD(A)	4
		TD(B)	14	BA(B)	14	SD(B)	22
Received Data	DCE	RD(A)	3	BB(A)	3	RD(A)	6
		RD(B)	16	BB(B)	16	RD(B)	24
Transmit Clock	DCE	TC(A)	15	DB(A)	15	ST(A)	5
		TC(B)	12	DB(B)	12	ST(B)	23
Receive Clock	DCE	TC(A)	17	DD(A)	17	RT(A)	8
		TC(B)	9	DD(B)	9	RT(B)	26
Ext. Transmit Clock	DTE	XC(A)	24	DA(A)	24	TT(A)	17
		XC(B)	11	DA(B)	11	TT(B)	35
Request To Send	DTE	RS(A)	4	CA(A)	4	RS(A)	7
		RS(B)	19	CA(B)	19	RS(B)	25
Clear To Send	DCE	CS(A)	5	CB(A)	5	CS(A)	9
		CS(B)	13	CB(B)	13	CS(B)	27
Data Set Ready	DCE	DR(A)	6	CC(A)	6	DM(A)	11
		DR(B)	22	CC(B)	22	DM(B)	29
Data Terminal Ready	DTE	TR(A)	20	CD(A)	20	TR(A)	12
		TR(B)	23	CD(B)	23	TR(B)	30
Data Carrier Detect	DCE	CD(A)	8	CF(A)	8	RR(A)	13
		CD(B)	10	CF(B)	10	RR(B)	31
Local Loopback	DTE	LL	18	LL	18	LL	10
Remote Loopback	DTE	RL	21	RL	21	RL	14
Ring Indicator	DCE	RI/TM	25	--	--	--	--
Test Mode	DCE	RI/TM	25	TM	25	TM	18
Cable Type 4	--	CTP4	18		n/c		n/c
Cable Type 3	--	CTP3	26		n/c		n/c
Cable Type 2	--	CTP2	13				
Cable Type 1	--	CTP1	22				
Cable Type 0	--	CTP0	10				

continued on next page...

WAN Serial Port Specifications (cont.)							
Generic Signal Name	Source	X.21/X.26		V.35		RS232	
		Mnemonic	Pin	Mnemonic	Pin	Mnemonic	Pin
Shield	--	--	1	--	A	--	1
Signal Ground	--	G	8	102	B	AB	7
Transmitted Data	DTE	T(A)	2	103(A)	P	BA	2
		T(B)	9	103(B)	S		
Received Data	DCE	R(A)	4	104(A)	R	BB	3
		R(B)	11	104(B)	T		
Transmit Clock	DCE	--	--	114(A)	Y	DB	15
				114(B)	AA		
Receive Clock	DCE	S(A)	6	115(A)	V	DD	17
		S(B)	13	115(B)	X		
Ext. Transmit Clock	DTE	B(A)	7	113(A)	U	DA	24
		B(B)	14	113	W		
Request To Send	DTE	C(A)	3	105	C	CA	4
		C(B)	10				
Clear To Send	DCE	--	--	106	D	CB	5
Data Set Ready	DCE	--	--	107	E	CC	6
Data Terminal Ready	DTE	--	--	108	H	CD	20
Data Carrier Detect	DCE	I(A)	5	109	F	CF	8
		I(B)	12				
Local Loopback	DTE	--	--	141	L	LL	18
Remote Loopback	DTE	--	--	140	N	RL	21
Ring Indicator	DCE	--	--	125	J	CE	22
Test Mode	DCE	--	--	142	NN	TM	25
Cable Type 4	--		n/c		n/c		
Cable Type 3	--		n/c		n/c		
Cable Type 2	--						
Cable Type 1	--						
Cable Type 0	--						

WSM-S/SC

The WAN Switching Module (WSM) supports 2, 4, or 8 serial ports, each of which can provide access rates from 9.6 Kbps to 2 Mbps. The two-port version is known as the WSM-S-2. The four-port version is known as the WSM-SC-4. And the eight-port version is known as the WSM-SC-8. The WSM-SC-4 and WSM-SC-8 support STAC hardware compression and three types of clocking (internal, external, and split). However, the WSM-S-2 does *not* support hardware compression.

The WSM can sense and auto-configure for any of five serial cable types (RS-232, V.35, X.21, RS-530, and RS449). A WSM port is normally considered a physical DTE device. It can be turned into a physical DCE device—for speed or clocking purposes— by plugging in a DCE cable. The WSM board senses whether a DCE or DTE cable is connected.

Software in the switch allows you to configure parameters for the Frame Relay or Point-to-Point Protocol (PPP). Software commands allow you to view the status of the WAN connection at the WSM board, port, or virtual circuit level. Extensive statistics are provided at each level. Software commands for Frame Relay are described in Chapter 49, “Managing Frame Relay”; commands for PPP are described in Chapter 50, “Point to Point Protocol.”

The WSM is actually a submodule, or daughtercard, that attaches to a High-Speed Module (HSM). The HSM contains memory and processing power for switching modules that operate at speeds greater than 10 Mbps. You plug your cable into the WSM submodule, but it is the HSM module that connects to the switch’s backplane.

WSM Technical Specifications	
Number of ports	2, 4, or 8
Connector Type	High-density 26-pin shielded serial
Protocols Supported	Frame Relay and Point-to-Point (PPP)
Data Rates Supported	9.6, 19.2, 56, 64, 128, 256, 512, 768, 1024, 1536, 2048 Kbps
Compression (WSM-SC-2 and WSM-SC-8 only)	Hardware-based using STAC 9705
Clocking	Internal, External, or Split (i.e., “loop timing”)
Virtual Circuits Supported	Permanent Virtual Circuits (PVCs)
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	Physical Data Terminal Equipment (DTE) or Data Communication Equipment (DCE)
Cable Supported	DTE or DCE in the following types: R2-232, V.35, X.21, RS-530, RS-449

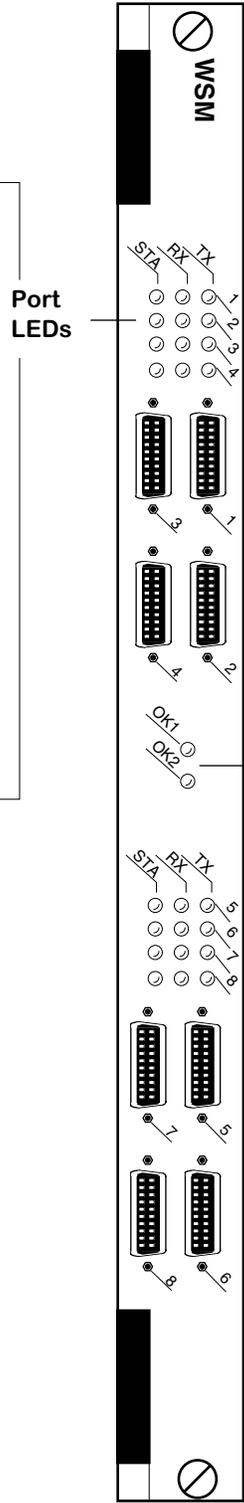
The module includes one row of LEDs for each port. The LEDs for a given port display in the row labeled with the port number. If the WSM module includes a total of eight ports, then the module contains two sets of four rows of LEDs. The second set of LEDs displays above the second set of ports.

STA (Status). On Green continuously when the port connection is operational. Off when the port is disabled or the cable is detached. Blinking On/Off if cable is attached but receive control data is detected as down.

This LED also blinks during initialization, diagnostics, or when invalid data is being exchanged on the port.

TX (Transmit). On “half-bright” Green when idle and Green with occasional flickers when the port is transmitting data.

RX (Receive). On “half-bright” Green when idle and Green with occasional flickers when the corresponding port is receiving data.



Module LEDs

OK1 (Hardware Status). On Green when the module has passed diagnostic tests successfully. On Amber when the hardware has failed diagnostics or if the corresponding image file for the module is not in flash memory.

OK2 (Software Status). Blinking Green when the module software was downloaded successfully and the module is communicating with the MPM. Blinking Amber when the module is in a transitional state. On Solid Amber if the module failed to download software from the MPM.

WSM Frame Relay Module With Eight Ports

WSM-FT1/FE1

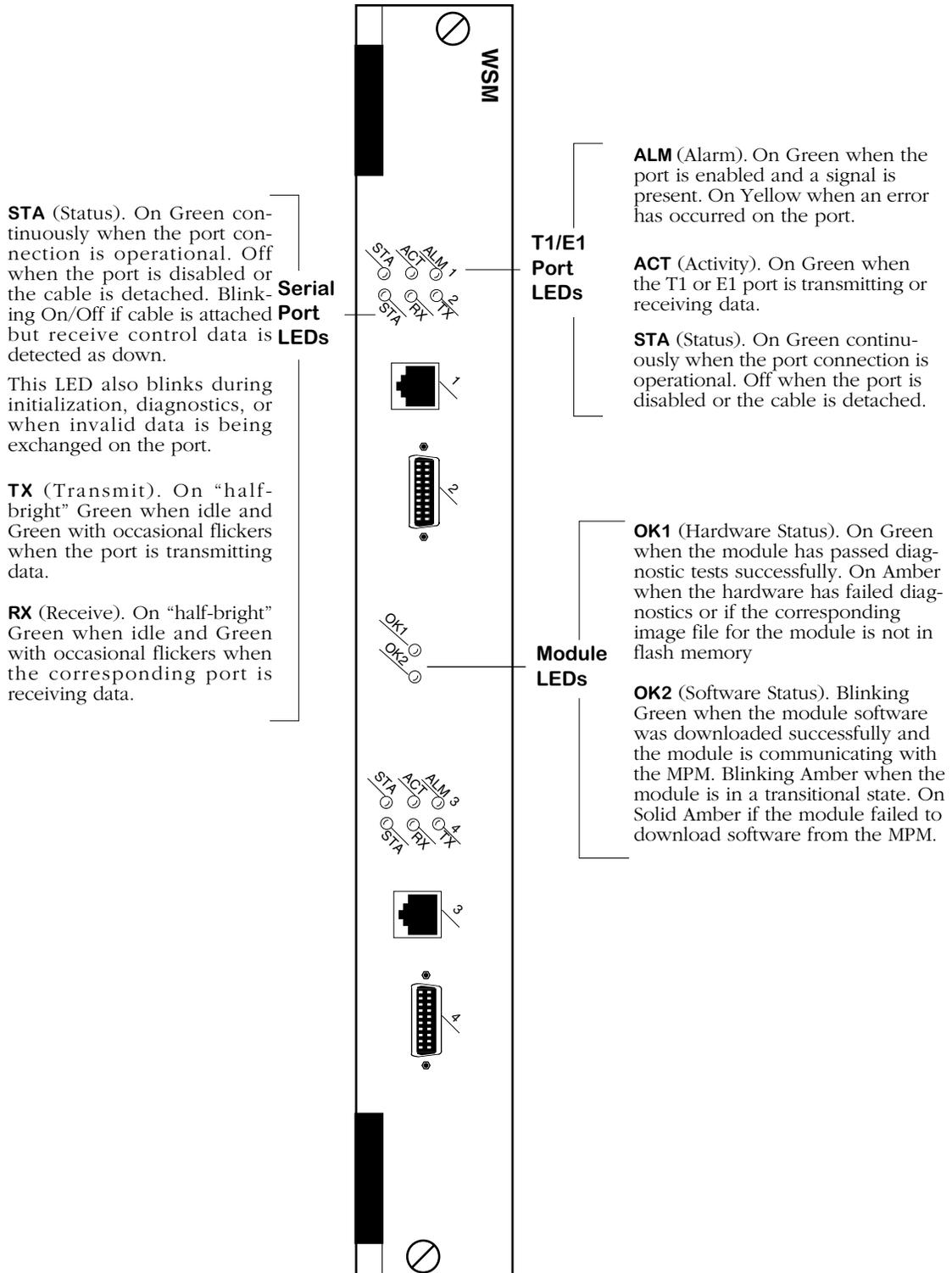
The WSM-FT1/FE1 module contains one or two T1 or E1 ports and one or two serial ports. T1 and E1 ports use RJ-48C connectors. The T1 version of this module is referred to as the WSM-FT1-SC; the E1 version is referred to as the WSM-FE1-SC. You can configure these ports to run either Frame Relay or the Point-to-Point Protocol (PPP).

This module includes an integrated CSU/DSU to enable direct connection to a T1/E1 device, such as a PBX.

You can configure physical port parameters through software commands. Configuration options include frame format, facility datalink, and line coding. In addition, the switch can store up to 24 hours of local and remote statistics. See Chapter 53, “Managing T1 and E1 Ports,” for more information on software-configurable parameters.

WSM-FT1/E1 Technical Specifications	
Number of ports	4 total 1 or 2 T1 or E1 ports 1 or 2 Universal Serial ports
Connector Types	T1/E1: RJ-45C Serial: High-density, 26-pin shielded
Standards Supported	RFCs 1406, 1213, 1659
Frame Formats	T1: Superframe, Extended Superframe, Unframed E1: E1, E1-CRC, E1-MF, E1-CRC-MF, Unframed
Line Coding	T1: B8ZS or AMI E1: HDB3 or AMI
Data Rates Supported	T1: 1.544 Mbps E1: 2.048 Mbps Serial: 56, 64, 128, 256, 384, 512, 768, 1024, 1536, 1544, 2048 Kbps
Facility Datalink Protocol	ANSI T1.403 and AT&T 54016
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Connections Supported	Physical Data Terminal Equipment (DTE) or Data Communication Equipment (DCE)
Cable Supported	Serial Ports DTE or DCE of the following types: R2-232, V.35, X.21, RS-530, RS-449

This module includes one set of LEDs for each port. The LEDs for a given port display above the port. If the WSM module includes four ports, then the module contains two sets of LEDs. The second set of LEDs displays above the third and fourth ports.



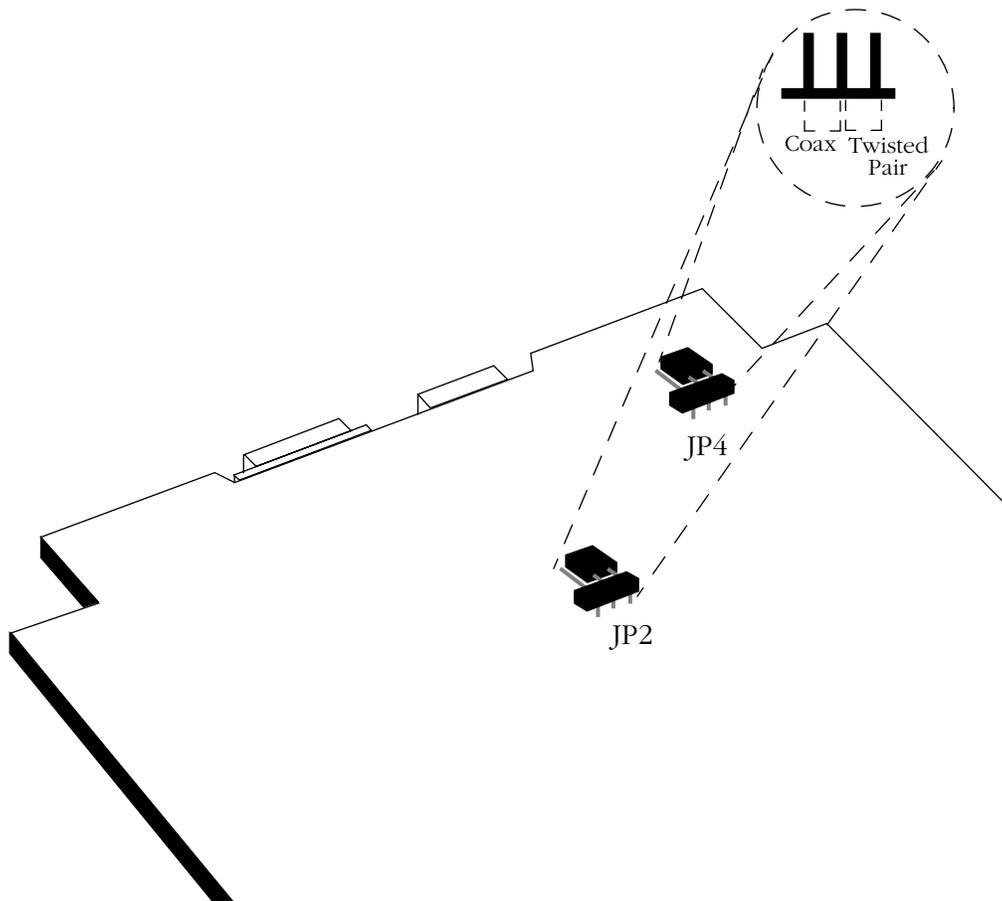
Fractional T1/E1 Module

Cabling/Jumper Settings

The E1 version of this module supports both twisted pair (120 ohm) and coaxial (75 ohm) cable types. Because of this you must set a pair of jumpers (JP2 and JP4) on the back of the board to correspond to the type of cable you are using. For more detailed information on the types of cables to use with this module, see Appendix B, "Custom Cables." The illustration below shows the correct jumper positions.

Note:

JP3 is reserved. Do not set a jumper across JP3.



Cable Termination Jumpers for WSM-FE1-SC

WSM-BRI

The ISDN Basic Rate Interface WAN Switching Module (WSM-BRI) supports 1 serial port and 1 BRI port. A WSM-BRI is actually a submodule, or daughtercard, that attaches to a High-Speed Switching Module (HSM-2). A maximum of two WSM-BRI modules can be installed into one HSM-2 module, providing a total of 2 serial ports and 2 BRI ports in one switch slot.

The serial port on a WSM-BRI module is essentially the same as the serial ports found on the WSM-S module. A WSM-BRI serial port can detect, and configure itself, for any of five serial cable types (RS-232, V.35, X.21, RS-530, and RS449). A WSM-BRI serial port is normally considered a physical DTE device, but it can be turned into a physical DCE device—for speed or clocking purposes—by simply plugging in a DCE cable. The board internally senses whether a DCE or DTE cable is connected and configures itself appropriately.

The BRI port on the WSM-BRI board can be configured as either a “U” or an “S/T” type of interface (the board is shipped set to “U”). Either type of interface supports two “B” channels operating at 56/64 Kbps and one “D” channel operating at 16 Kbps.

Software running in the switch allows you to configure the operation of the Point-to-Point Protocol (PPP) over the serial port or the BRI port. The serial port can also support the Frame Relay protocol. The software commands used to configure PPP are described in Chapter 50, “Point-to-Point Protocol.” The software commands used to configure Frame Relay are described in Chapter 49, “Managing Frame Relay.” The software commands used to configure the WAN “links” that support PPP connections are described in Chapter 51, “WAN Links.” Finally, the software commands used to manage the ISDN ports are described in Chapter 52, “Managing ISDN Ports.”

WSM-BRI Technical Specifications	
Number of ports	1 serial, 1 Basic Rate Interface (BRI)
Serial Connector Type	High-density 26-pin shielded serial
BRI Connector Type	RJ-45
Protocols Supported	Point-to-Point Protocol (PPP); Frame Relay (supported on the serial port only)
Data Rates Supported	2 “B” Channels at 56/64 Kbps 1 “D” Channel at 16 Kbps
Compression	Hardware-based using STAC 9705
MAC Addresses Supported	1,024; 2,048 with CAM upgrade option
Serial Port Connections Supported	Physical Data Terminal Equipment (DTE) or Data Communication Equipment (DCE)
Serial Cables Supported	DTE or DCE in the following types: R2-232, V.35, X.21, RS-530, RS-449
BRI Port Connections Supported	“U” interface or “S/T” interface (jumper-selectable; “U” is shipping default)
Switch Types Supported	National ISDN-1, AT&T 5ESS, Northern Telecom DMS100, ETSI Euro-ISDN Net3
ISDN Standards Supported	Q.921, Q.931, I.430, T1.601

The WSM-BRI module includes one set of LEDs for each port. The LEDs for a given port display in the set labeled with the port number. If the HSM module contains two WSM-BRI daughter cards, the second set of ports (one Serial and one BRI) are numbered as Ports 3 and 4 respectively, and include their own separate set of LEDs that function exactly like those related to Ports 1 and 2.

STA (Status). On Green continuously when the port connection is operational. Off when the port is disabled or the cable is detached. Blinking On/Off if cable is attached but receive control data is detected as down.

This LED also blinks during initialization, diagnostics, or when invalid data is being exchanged on the port.

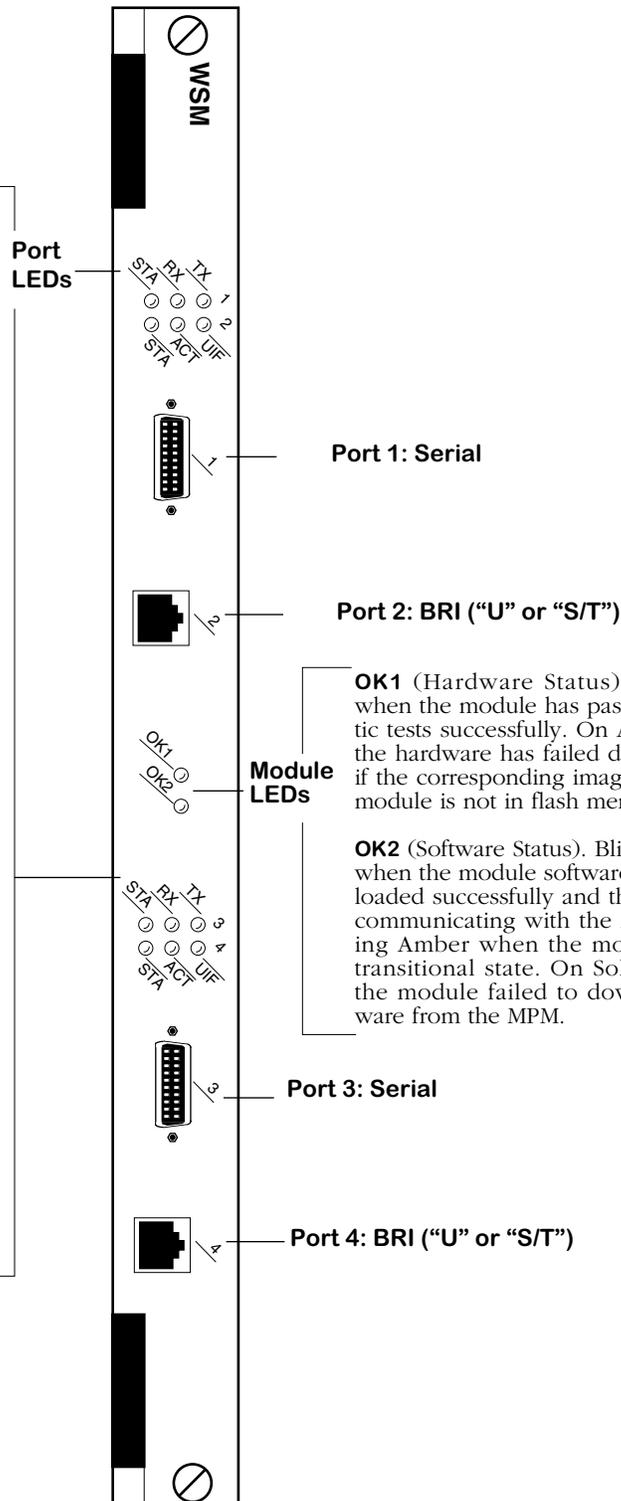
TX (Transmit). On “half-bright” Green when idle and Green with occasional flickers when the port is transmitting data.

RX (Receive). On “half-bright” Green when idle and Green with occasional flickers when the corresponding port is receiving data.

UIF (“U” Interface). On Green when the ISDN-BRI port is configured as a “U” type of interface. Off when the port is configured as an “S/T” type of interface.

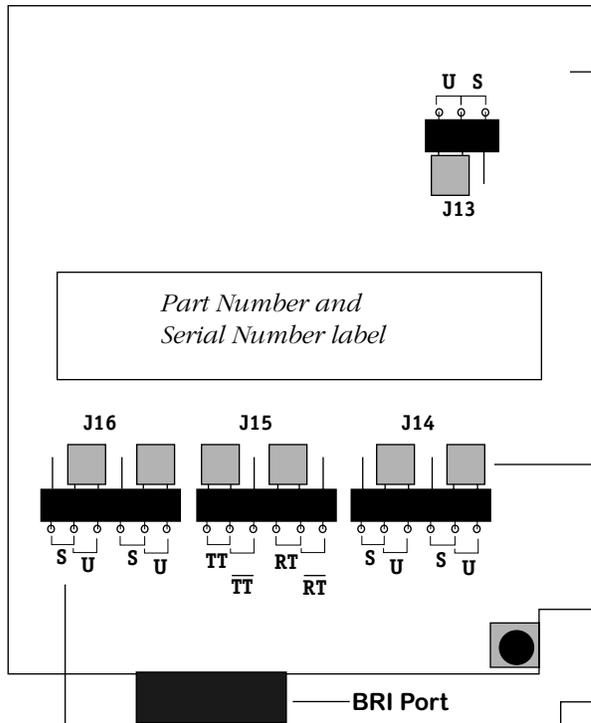
ACT (Activity). On Green when the ISDN-BRI port is sending or receiving data.

STA (Port 2/4 Status). On Green continuously when the port connection is operational. Off when the BRI port is disabled or the cable is detached. This LED blinks during initialization.



Two WSM-BRI Modules Installed in One HSM

**Jumper Configuration for the "U" Interface
(this is how the board is shipped)**

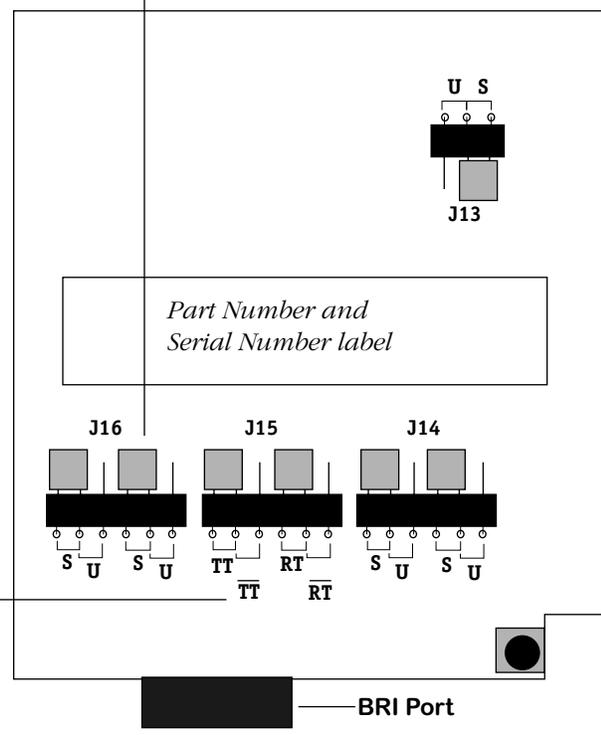


This is a simplified view of the bottom lower-right quadrant of the WSM-BRI board. Immediately above the BRI port are three jumper blocks labelled J14, J15, and J16. About two inches above and to the right is another jumper labeled J13. J13, J14, and J16 are used to switch between the "U" and "S/T" interfaces. J15 is used to set transmit and receive termination for the "S/T" interface.

The grey boxes are the jumper blocks

The small labels next to the jumper pins at J13, J14, and J16 indicate which pins must be bridged to set the BRI port to either the "U" or the "S/T" interface.

Small labels under the pins at J15 indicate which pins must be bridged to set Transmit Termination (tt) and Receive Termination (rt) to the "on" or "off" position (the two sets of letters with a line over them indicate the "off" settings).



**Jumper Configuration for the "S/T" Interface
(transmit/receive termination are set to "on")**

Cable Interfaces for Universal Serial Ports

The WSM/WSX automatically senses the cable type that you plug into one of its Universal Serial Ports. It can sense whether the cable type is DCE or DTE and whether it is one of the following interfaces:

- RS-232
- RS-449
- RS-530
- V.35
- X.21 (European)

All cable types (except RS-232) are capable of access rates from 9.6 kbps to 2 Mbps. The RS-232 cable is not compatible with speeds greater than 64 kbps. Each cable type is illustrated and described in Appendix B, "Custom Cables."

The WSM/WSX port is normally considered a physical DTE device. It is possible to turn it into a physical DCE device simply by plugging in a DCE cable. The WSM/WSX board internally senses whether a DCE or DTE cable is connected.

DTE/DCE Type and Transmit/Receive Pins

The RS-232 protocol, which is employed at the physical level for all cable types, always defines Transmit and Receive pins in relation to the DTE. So, the type of cable you attach (DCE or DTE) determines the direction of data flow on your connector's Transmit and Receive pins.

If the WSM/WSX port is a physical DTE, which is probably the most common configuration, then data is received on Receive pins and transmitted on Transmit pins. If you are using a WSM/WSX port as a physical DCE, then data is transmitted on the receive pins and received on the transmit pins.

Data Compression

Data compression allows you to get more data through the Frame Relay pipeline, further enhancing cost benefits. A typical data compression ratio on the WSM/WSX board at the hardware level is 4:1. In addition, the compression processor (STAC 9705) has its own memory (DRAM) that can store up to 100 compression histories (on a 4-port WSM/WSX) without degrading performance. An 8-port WSM/WSX can store up to 200 compression histories without performance degradation.

The WSM/WSX will only compress data if you enable compression through software and the bridge/router on the other end of the connection supports standard Frame Relay (FRF.9) or PPP (STAC-LZS) compression. (An OmniSwitch-to-OmniSwitch connection would support compression.) Negotiation is necessary because if compressed data is sent to a bridge/router that does not support compression, this bridge/router will not recognize the data and will automatically drop the unrecognizable frames.

If you enable compression, the WSM/WSX will query the Frame Relay or PPP device on the other end of the circuit to determine whether it supports compression. If it does, the WSM/WSX will compress all data except frame DLCMI (management) data and PPP control messages. If it does not support compression, data on that connection will be sent uncompressed. Refer to either Chapter 49, "Managing Frame Relay," or Chapter 50, "Point-To-Point Protocol," for information on enabling compression.

Note

Compression is not supported on the OmniSwitch WSM-S-2 and the Omni Switch/Router WSX-S-2W modules.

Loopback Detection

Loopback Detection is a common method for Carrier Service Providers to test clients' circuits in the event of suspected line transmission problems. For both Frame Relay and PPP, loopback detection involves periodically transmitting a message and looking for that message to be received. When implementing Loopback Detection, it is important to keep two issues in mind: the message must not violate any standards; the message must be unique in such a way that it can be differentiated from a message sent by a remote node.

The messages are transmitted in one of two fixed intervals. When the port is in normal mode, the message is transmitted once every second. When two consecutive messages are received that match the transmitted message, the port is considered to be in loopback. Once in loopback mode, the message is transmitted once every 100 milliseconds. After ten consecutive messages are transmitted without receiving a match, the port is returned to normal mode. Consequently, it takes up to 2 seconds to detect the loopback condition and an additional second to exit it.

The message sent on a Frame Relay port uses standard 1490 encapsulation with a SNAP header. The OUI (Organizationally Unique Identifier) of the SNAP header is the Alcatel OUI, so encapsulation is standard, but the message is proprietary. The message is transmitted using the lowest available DLCI, or 32 if there are no DLCI's operating on the port. Because the message is merely attempting to determine the state of the physical port, the state of the DLCI, whether active, inactive or non-existent, is not important; the Frame Relay switch will discard any data for non-existent or inactive DLCIs.

The message sent on a PPP port uses the standard LCP Echo message.

Uniqueness of messages is accomplished by including a word in the message that is based upon the configuration of the port and a free-running timer. For PPP, uniqueness is enhanced by negotiating the LCP magic number option.

The WAN Port Software Menu

User interface commands for the WSM board are on a separate menu that is accessed through the **wan** command. The WAN Port menu is a submenu of the Interface menu. Typing **wan** at any system prompt displays the following menu:

Command	Wide Area Networking Menu			
wpmodify	Modify a given WAN port's parameters			
wpdelete	Delete a given port's parameters, and restore defaults			
wpview	View WAN port parameters for a given slot and port			
wpstatus	View WAN port status of entire chassis, slot, or individual port			
fr	Enter the Frame Relay submenu			
ppp	Enter the PPP submenu			
isdn	Enter the ISDN-specific submenu			
link	Enter the link-specific submenu			
Main Interface	File Security	Summary System	VLAN Services	Networking Help

◆ **Note** ◆

The ISDN menu will only appear on systems with a least one WSM-BRI module installed.

You can start most of the commands by typing the first three (3) letters of the command name. For example, to use the **wpview** command, type **wpv**.

The following sections describe the use of commands on the WAN Port menu.

Setting Configuration Parameters

When you plug in a WSM board, it is automatically configured to the default settings. By default, the WSM uses Frame Relay protocol. In addition, the access rate for serial ports defaults to 64 kbps for RS-232 cables. The access rate for other cable types defaults to 2 Mbps. You can change these settings, as well as several other settings, such as clocking and protocol type, with the **wpmodify** command.

Modifying a Port

Use the **wpmodify** command to modify a port, as shown below:

wpmodify <slot>/<port>

in which **<slot>** is the slot number where the WSM board is located, and **<port>** is the port number on the WSM board that you want to modify. When this command is entered, the system automatically senses what type of port is being configured, and displays the appropriate screen for that type of port. The screen is different depending on the type of encapsulation used, either Frame-Relay or Point-to-Point Protocol.

Make changes by entering the line number for the option you want to change, an equal sign (=), and the value for the new parameter. When you have finished entering the new values, type **save** at the prompt to save the new parameters. The following sections describe the options you can alter through this menu. The following three examples show a typical setup screen for a serial port, an ISDN-BRI port, and a fractional T1 port, respectively.

Serial Port Example

In this example, port 1 on slot 3 is a serial port, using Frame-Relay. To modify serial port 3/1, enter:

```
wpm 3/1
```

A screen similar to following displays:

```

1) Admin Status ..... UP
   {(U)p, (D)own}
2) Speed in BPS ..... 2048000
   {9600, 19200, 56000, 64000, 128000, 256000, 512000, 768000}
   {1024000, 1544000, 2048000}
3) Clocking ..... External
   {(I)nternal, (E)xternal, (S)plit}
4) Protocol Type ..... Frame Relay
   {(F)rame Relay, (P)PP(Point to Point)}
7) Receive Clock ..... Normal
   {(N)ormal, (I)nverted}
8) TOS for Voice Data ..... a0
   TOS Value in Hex for Voice Data, 0 to disable TOS
9) TOS for Voice Signaling Data ..... 60
   TOS Value in Hex for Voice Signaling Data, 0 to disable TOS
10) TOS Mask for both TOS Value ..... e0
    TOS Mask in Hex for Type of Data
11) Signaling IP Address ..... 0.0.0.0
    IP Address range
12) Signaling IP Mask ..... 255.255.255.255
    IP Mask range
15) Loopback Timeout ..... 10
    {Timeout (0..255)}

```

If the interface was using PPP, the following screen would display:

```
1) Admin Status ..... UP
   {(U)p, (D)own}
2) Speed in BPS ..... 2048000
   {9600, 19200, 56000, 64000, 128000, 256000, 512000, 768000}
   {1024000, 1544000, 2048000}
3) Clocking ..... External
   {(I)nternal, (E)xternal, (S)plit}
4) Protocol Type ..... Frame Relay
   {(F)rame Relay, (P)PP(Point to Point)}
7) Receive Clock ..... Normal
   {(N)ormal, (I)nverted}
8) TOS for Voice Data ..... a0
   TOS Value in Hex for Voice Data, 0 to disable TOS
9) TOS for Voice Signaling Data ..... 60
   TOS Value in Hex for Voice Signaling Data, 0 to disable TOS
10) TOS Mask for both TOS Value ..... e0
   TOS Mask in Hex for Type of Data
11) Signaling IP Address ..... 0.0.0.0
   IP Address range
12) Signaling IP Mask ..... 255.255.255.255
   IP Mask range
13) KeepAlive Up Count ..... 0
   {Up Count (0..255)}
14) KeepAlive Down Count ..... 0
   {Down Count (0..255)}
15) KeepAlive Timeout ..... 10
   {Timeout (0..255)}
16) DTR Pulse Width ..... 0
   {Pulse Width (0..255)}
17) DTR Pulse Count ..... 0
   {Pulse Count (0..255)}
```

Admin Status

The options for the Admin Status are **UP** and **DN**. If **UP**, the port has been enabled and can transmit data as long as its Operational Status is also **UP**. If set to **DN**, the port will not pass data even, if its physical connection is good.

Speed in BPS

This option specifies the access rate for the Frame Relay or PPP line to the service provider. This parameter is the speed of the entire connection, not an individual virtual circuit. For example, if you have a 56 kbps line to your service provider, this field should be set to 56000. A full T1 line would have an access rate of 1,544,000 bps, and a full E1 line would have an access rate of 2,048,000 bps. For either T1 or E1, you can also have a fractional service with an access rate that is a multiple of 64 kbps. Enter a value that is the same as one of the values displayed below this field.

Note

If the port you are configuring is a physical DCE port (i.e., DCE cable plugged into the submodule port) that can control the access rate and clocking, always enter a value for this field. This value will be used in computing congestion control parameters, such as the Committed Information Rate (CIR). If the port is a DTE, this setting will have no effect, except for informational purposes.

Clocking

This field sets the type of clocking used to clock transmit and receive data on the serial port. If the clock goes out-of-phase, you will receive errors.

Note

The clocking value is only relevant if the port is a physical DCE port (i.e., DCE cable plugged into the submodule port). If the submodule port is a physical DTE port, clocking will default to External.

External Clocking

If you set this value to External, clocking will be controlled by the external DCE (a DSU or other DCE device on the other end of the cable from the submodule port). External clocking is the default option when the submodule is a physical DTE device (i.e., controlled by an external DCE device).

When the submodule is acting as a physical DTE and

- the speed is greater than 256 kbps, or
- excessive FCS errors or Aborts are being detected coming from the submodule at the remote port or line monitor

then it is recommended that the external DCE (usually a CSU/DSU) be set to take a transmit data clock from the external DTE transmit clock (TXCE).

You can set up the external DCE this way by configuring its DTE, or dataport, configuration options. Set the "Transmit Clock Source" to "External." In this mode of operation, the transmit clock is output by the DCE device and the submodule turns it around on the external transmit clock back to the DCE, eliminating any phase misalignment between transmit clock and transmit data.

If the external DCE does not provide a DTE configuration option for the transmit clock source, then try setting the "Transmit Clock *Polarity*" to "Invert." Note that Invert is the clock polarity for Transmit (not Receive) and should only be used when excessive FCS errors or Aborts are detected.

Internal Clocking

If you set this value to Internal, clocking is controlled by the internal DCE (the submodule). Internal clocking should only be selected if the submodule is a physical DCE device and you are using an RS-232 cable. Internal clocking is the default setting when the submodule is a physical DCE device and an RS-232 DCE cable is connected to this port.

Split Clocking

Split clocking, which is also known as “loop timing,” uses an additional control signal (TXCE) to keep the submodule and external DTE clocking synchronized. In split clocking, the external DTE takes the incoming transmit clock from the submodule and loops it back to TXCE. The submodule then uses this signal to clock in data from the external DTE device. Split clocking should only be used if the submodule is a physical DCE device and you are using a non-RS-232 cable, such as V.35.

◆ Important Note ◆

Split clocking is required if the access rate of the submodule port is greater than 256 kbps and it is acting as a DCE device. If split clocking is not used at these data rates, data out-of-phase errors, aborts, or CRC errors may occur.

Split clocking is the default when the submodule port is a physical DCE device and a non-RS-232 DCE cable is connected to the port.

Protocol Type

The protocol type can be set to either Frame Relay or Point to Point Protocol (PPP). The default setting is Frame Relay.

◆ Important Note ◆

A port must be set to either Frame Relay or PPP before any other protocol-related parameters can be set.

Receive Clock

Often, due to delays added to timestamps in when running through switch hardware, the receive clock time is significantly different than expected from the transmitting data source. To correct the problem, it is possible to set the receive clock to invert the delay information. The following options are available:

Normal

The port uses the internal clock time as the timestamp for receive data (timestamp information is not modified).

Inverted

The port uses an inverted timestamp for receive data.

TOS for Voice Data

Set the priority for voice data streams. The value must be entered in hexadecimal format translated from binary, and can use either IP Precedence or Differentiated Services Code Point (DSCP). Enter **0** to disable this feature. See *Type of Service (ToS)* on page 48-2 above for a more detailed explanation of ToS.

TOS for Voice Signaling Data

Set the priority for voice signaling data streams. The value must be entered in hexadecimal format translated from binary, and can use either IP Precedence or Differentiated Services Code Point (DSCP). Enter **0** to disable this feature. See *Type of Service (ToS)* on page 48-2 above for a more detailed explanation of ToS.

TOS Mask for both TOS Value

Set the mask bits for both voice data and signaling data. Enter **0** to disable this feature.

Signaling IP Address

When a data frame cannot be identified by the ToS voice data or ToS signaling data, the Signaling IP Address is checked. Matched frames are loaded on a High Priority Software Queue and a Nominal Hardware Queue.

Signaling IP Mask

The mask associated with the Signaling IP Address described above.

KeepAlive Up Count

If the switch detects that a port may be down, it will generate echo message requests to the far end of the connection. The KeepAlive Up Count is the number of requests sent from the port when the port transitions from Down to Up, to verify the status of the port. The valid range is 0-255.

KeepAlive Down Count

If the switch detects that a port may be down, it will generate echo message requests to the far end of the connection. The KeepAlive Down Count is the number of requests sent from the port when the port transitions from Up to Down, to verify the status of the port. This only displays if the port is using PPP as its encapsulation type. The valid range is 0-255.

KeepAlive Timeout

The number of 100 millisecond increments between generated echo message requests. This only displays if the port is using PPP as its encapsulation type. The valid range is 0-255.

DTR Pulse Width

A Data Terminal Ready (DTR) Pulse is sent at the hardware level to determine a port is still synchronized with its far end connection. The Pulse Width is the number of 100 millisecond increments that the pulse lasts. This only displays if the port is using PPP as its encapsulation type. The valid range is 0-255.

DTR Pulse Count

A Data Terminal Ready (DTR) Pulse is sent at the hardware level to determine a port is still synchronized with its far end connection. The Pulse Count is the number of pulses generated when a line is down. This only displays if the port is using PPP as its encapsulation type. The valid range is 0-255.

Loopback Timeout

Sets the transition time between proprietary messages sent over the link. These messages are analyzed to determine whether the link is in a loopback state. This only displays if the port is using Frame Relay as its encapsulation type. The valid range is 0-255.

ISDN-BRI Port Example

In this example: port 2 on slot 3 is an ISDN-BRI port. To modify ISDN-BRI port 2/2, enter:

```
wpm 3/2
```

A screen similar to following displays:

```
1) Admin Status ..... UP
   {(U)p, (D)own}
2) Speed in BPS ..... 2048000
   {9600, 19200, 56000, 64000, 128000, 256000, 512000, 768000}
   {1024000, 1544000, 2048000}
3) Clocking ..... External
   {(I)nternal, (E)xternal, (S)plit}
4) Protocol Type ..... Frame Relay
   {(F)rame Relay, (P)PP(Point to Point)}
8) TOS for Voice Data ..... a0
   TOS Value in Hex for Voice Data, 0 to disable TOS
9) TOS for Voice Signaling Data ..... 60
   TOS Value in Hex for Voice Signaling Data, 0 to disable TOS
10) TOS Mask for both TOS Value ..... e0
   TOS Mask in Hex for Type of Data
11) Signaling IP Address ..... 0.0.0.0
   IP Address range
12) Signaling IP Mask ..... 255.255.255.255
   IP Mask range
13) KeepAlive Up Count ..... 0
   {Up Count (0..255)}
14) KeepAlive Down Count ..... 0
   {Down Count (0..255)}
15) KeepAlive Timeout ..... 10
   {Timeout (0..255)}
16) DTR Pulse Width ..... 0
   {Pulse Width (0..255)}
17) DTR Pulse Count ..... 0
   {Pulse Count (0..255)}
```

Note that the only parameters you can set for an ISDN port from this screen is the Admin Status and the ToS settings. All other parameters must be set from the ISDN, PPP, peer or WAN link menus. For more details on ISDN ports, see Chapter 52, “Managing ISDN Ports.” For more details on managing PPP ports, see Chapter 51, “Point-to-Point Protocol.” For more information on managing WAN links, see Chapter 51, “WAN Links.”

◆ Note ◆

The ISDN **wpmmodify** menu displays PPP specific line options described in the section *Modifying a Port* on page 48-24. However, they do not apply to an ISDN port, and are not described below.

Admin Status

The options for the Admin Status are **UP** and **DN**. If **UP**, the port has been enabled and can transmit data as long as its Operational Status is also **UP**. If set to **DN**, the port will not pass data even if its physical connection is good.

Speed in BPS

This option specifies the access rate for the Frame Relay or PPP line to the service provider. This parameter is the speed of the entire connection, not an individual virtual circuit. For example, if you have a 56 kbps line to your service provider, this field should be set to 56000. A full T1 line would have an access rate of 1,544,000 bps, and a full E1 line would have an access rate of 2,048,000 bps. For either T1 or E1, you can also have a fractional service with an access rate that is a multiple of 64 kbps.

Enter a value that is the same as one of the values displayed below this field.

Note

If the port you are configuring is a physical DCE port (i.e., DCE cable plugged into the submodule port) that can control the access rate and clocking, always enter a value for this field. This value will be used in computing congestion control parameters, such as the Committed Information Rate (CIR). If the port is a DTE, this setting will have no effect, except for informational purposes.

Clocking

This field sets the type of clocking used to clock transmit and receive data on the serial port. If the clock goes out-of-phase, you will receive errors.

Note

The clocking value is only relevant if the port is a physical DCE port (i.e., DCE cable plugged into the submodule port). If the submodule port is a physical DTE port, clocking will default to External.

External Clocking

If you set this value to External, clocking will be controlled by the external DCE (a DSU or other DCE device on the other end of the cable from the submodule port). External clocking is the default option when the submodule is a physical DTE device (i.e., controlled by an external DCE device).

When the submodule is acting as a physical DTE and

- the speed is greater than 256 kbps, or
- excessive FCS errors or Aborts are being detected coming from the submodule at the remote port or line monitor

then it is recommended that the external DCE (usually a CSU/DSU) be set to take a transmit data clock from the external DTE transmit clock (TXCE).

You can set up the external DCE this way by configuring its DTE, or dataport, configuration options. Set the “Transmit Clock Source” to “External.” In this mode of operation, the transmit clock is output by the DCE device and the submodule turns it around on the external transmit clock back to the DCE, eliminating any phase misalignment between transmit clock and transmit data.

If the external DCE does not provide a DTE configuration option for the transmit clock source, then try setting the “Transmit Clock *Polarity*” to “Invert.” Note that Invert is the clock polarity for Transmit (not Receive) and should only be used when excessive FCS errors or Aborts are detected.

Internal Clocking

If you set this value to Internal, clocking is controlled by the internal DCE (the submodule). Internal clocking should only be selected if the submodule is a physical DCE device and you are using an RS-232 cable. Internal clocking is the default setting when the submodule is a physical DCE device and an RS-232 DCE cable is connected to this port.

Split Clocking

Split clocking, which is also known as “loop timing,” uses an additional control signal (TXCE) to keep the submodule and external DTE clocking synchronized. In split clocking, the external DTE takes the incoming transmit clock from the submodule and loops it back to TXCE. The submodule then uses this signal to clock in data from the external DTE device. Split clocking should only be used if the submodule is a physical DCE device and you are using a non-RS-232 cable, such as V.35.

◆ Important Note ◆

Split clocking is required if the access rate of the submodule port is greater than 256 kbps and it is acting as a DCE device. If split clocking is not used at these data rates, data out-of-phase errors, aborts, or CRC errors may occur.

Split clocking is the default when the submodule port is a physical DCE device and a non-RS-232 DCE cable is connected to the port.

Protocol Type

The protocol type can be set to either Frame Relay or Point to Point Protocol (PPP). The default setting is Frame Relay.

◆ Important Note ◆

A port must be set to either Frame Relay or PPP before any other protocol-related parameters can be set.

TOS for Voice Data

Set the priority for voice data streams. The value must be entered in hexadecimal format translated from binary, and can use either IP Precedence or Differentiated Services Code Point (DSCP). Enter **0** to disable this feature. See *Type of Service (ToS)* on page 48-2 above for a more detailed explanation of ToS.

TOS for Voice Signaling Data

Set the priority for voice signaling data streams. The value must be entered in hexadecimal format translated from binary, and can use either IP Precedence or Differentiated Services Code Point (DSCP). Enter 0 to disable this feature. See *Type of Service (ToS)* on page 48-2 above for a more detailed explanation of ToS.

TOS Mask for both TOS Value

Set the mask bits for both voice data and signaling data. Enter 0 to disable this feature.

Signaling IP Address

When a data frame cannot be identified by the ToS voice data or ToS signaling data, the Signaling IP Address is checked. Matched frames are loaded on a High Priority Software Queue and a Nominal Hardware Queue.

Signaling IP Mask

The mask associated with the Signaling IP Address described above.

Fractional T1 Port Example

In this example: port 1 on slot 3 is a fractional T1 port using Frame Relay. To modify fractional T1 port 2/1, enter:

wpm 3/1

A screen similar to following displays:

```

1) Admin Status ..... UP
   {(U)p, (D)own}
2) Speed in BPS ..... 1544000
3) Clocking ..... Local
4) Protocol Type ..... Frame Relay
   {(F)rame Relay, (P)PP(Point to Point)}
5) T1 Starting Time Slot ..... 1
   {T1 (1..24)}
6) T1 Number of Time Slots ..... 23
   {T1 (1..24)}
8) TOS for Voice Data ..... a0
   TOS Value in Hex for Voice Data, 0 to disable TOS
9) TOS for Voice Signaling Data ..... 60
   TOS Value in Hex for Voice Signaling Data, 0 to disable TOS
10) TOS Mask for both TOS Value ..... e0
   TOS Mask in Hex for Type of Data
11) Signaling IP Address ..... 0.0.0.0
   IP Address range
12) Signaling IP Mask ..... 255.255.255.255
   IP Mask range
15) Loopback Timeout ..... 10
   {Timeout (0..255)}
(save/quit/cancel)
:
```

If the interface was using PPP, the following screen would display:

```
1) Admin Status ..... UP
   {(U)p, (D)own}
2) Speed in BPS ..... 1544000
3) Clocking ..... External
   {(I)nternal, (E)xternal, (S)plit}
4) Protocol Type ..... PPP
   {(F)rame Relay, (P)PP(Point to Point)}
7) Receive Clock ..... Normal
   {(N)ormal, (I)nverted}
8) TOS for Voice Data ..... a0
   TOS Value in Hex for Voice Data, 0 to disable TOS
9) TOS for Voice Signaling Data ..... 60
   TOS Value in Hex for Voice Signaling Data, 0 to disable TOS
10) TOS Mask for both TOS Value ..... e0
   TOS Mask in Hex for Type of Data
11) Signaling IP Address ..... 0.0.0.0
   IP Address range
12) Signaling IP Mask ..... 255.255.255.255
   IP Mask range
13) KeepAlive Up Count ..... 0
   {Up Count (0..255)}
14) KeepAlive Down Count ..... 0
   {Down Count (0..255)}
15) KeepAlive Timeout ..... 10
   {Timeout (0..255)}
16) DTR Pulse Width ..... 0
   {Pulse Width (0..255)}
17) DTR Pulse Count ..... 0
   {Pulse Count (0..255)}
```

◆ **Note** ◆

The DTR Pulse settings do not apply to T1 and E1 interfaces, and are not described below.

Admin Status

The options for the Admin Status are **Enable** and **Disable**. If **Enable**, the port has been enabled and can transmit data as long as its Operational Status is also enabled. If set to **Disable**, the port will not pass data, even if its physical connection is good.

Speed in BPS

This field shows the speed for the T1/E1 port. This field is for reference only.

Clocking

This field shows the type of clocking set for the T1 port. This field is for reference only.

Protocol Type

The protocol type can be set to either Frame Relay or Point to Point Protocol (PPP).

◆ **Important Note** ◆

A port must be set to either Frame Relay or PPP before any other protocol-related parameters can be set.

T1/E1 Starting Time Slot

This field specifies the first time slot number to use on a T1 or E1 port. For a full T1 or E1 connection, specify time slot 1. For a fractional T1 or E1 connection, set this field to the starting time slot number as specified by your service provider.

T1/E1 Number of Time Slots

This field specifies the total number of 64 kbps time slots to use on the T1 or E1 connection. For a full T1, set this number to 24. For a full E1 connection, set this number to 30 if you are running multiframe; otherwise, set to 31. For fractional T1 or E1, you must set the number of time slots to the value specified by your service provider. For example, a 256 kbps service uses four time slots ($4 \times 64 = 256$).

TOS for Voice Data

Set the priority for voice data streams. The value must be entered in hexadecimal format translated from binary, and can use either IP Precedence or Differentiated Services Code Point (DSCP). Enter **0** to disable this feature. See *Type of Service (ToS)* on page 48-2 above for a more detailed explanation of ToS.

TOS for Voice Signaling Data

Set the priority for voice signaling data streams. The value must be entered in hexadecimal format translated from binary, and can use either IP Precedence or Differentiated Services Code Point (DSCP). Enter **0** to disable this feature. See *Type of Service (ToS)* on page 48-2 above for a more detailed explanation of ToS.

TOS Mask for both TOS Value

Set the mask bits for both voice data and signaling data. Enter **0** to disable this feature.

Signaling IP Address

When a data frame cannot be identified by the ToS voice data or ToS signaling data, the Signaling IP Address is checked. Matched frames are loaded on a High Priority Software Queue and a Nominal Hardware Queue.

Signaling IP Mask

The mask associated with the Signaling IP Address described above.

KeepAlive Up Count

If the switch detects that a port may be down, it will generate echo message requests to the far end of the connection. The KeepAlive Up Count is the number of requests sent from the port when the port transitions from Down to Up, to verify the status of the port. The valid range is 0-255.

KeepAlive Down Count

If the switch detects that a port may be down, it will generate echo message requests to the far end of the connection. The KeepAlive Down Count is the number of requests sent from the port when the port transitions from Up to Down, to verify the status of the port. This only displays if the port is using PPP as its encapsulation type. The valid range is 0-255.

KeepAlive Timeout

The number of 100 millisecond increments between generated echo message requests. This only displays if the port is using PPP as its encapsulation type. The valid range is 0-255.

Loopback Timeout

Sets the transition time between proprietary messages sent over the link. These messages are analyzed to determine whether the link is in a loopback state. This only displays if the port is using Frame Relay as its encapsulation type. The valid range is 0-255.

Viewing Configuration Parameters for the WSM

You can view all current parameters for a WSM port or an individual virtual circuit using the **wpview** command. These parameters will be either the default parameters or parameters you modified using the **wpmodify** command or network management software.

You have a choice of viewing parameters at the chassis, slot or port level. You receive different configuration choices depending upon which level you choose. The sections below describe both ways to use the **wpview** command.

Viewing Parameters for all Submodules in the Chassis

To view port parameters for all submodule boards in a chassis, enter the following command

```
wpview
```

or

```
wpv
```

A screen similar to following displays. In this example, the port parameters being displayed are for a system that contains a 2-port BRI submodule in slot 3.

Slot/Port	Port Type	Intf. Type	Admin/ Oper/ State	Protocol	Speed BPS	Clocking
3/1	Serial	*NONE*	UP/DN	FR	0	External
3/2	ISDN	ISDN-ST	UP/UP	PPP	N/A	External

This screen lists the current values for the listed parameters.

For **Port Type**, **Intf. Type** and **Oper/State**, these parameters are the same as those set through the **wpmodify** command. For detailed information on these values, see *Modifying a Port* on page 48-24. For **Protocol**, **Speed BPS** and **Clocking**, these parameters are the same as those set through the **wpstatus** command. See *Obtaining Status and Statistical Information* on page 48-46.

Viewing Parameters for all Ports in a Single Submodule

To view port parameters for all ports on a particular submodule, enter the **wpview** command, followed by the number of the slot. In the following three examples, the port parameters are displayed for an ISDN-BRI board, a serial board, and a T1 board.

ISDN-BRI Board Example

To display the parameters for all ports on the ISDN-BRI board (in slot 3), enter:

```
wpview 3
```

or

```
wpv 3
```

A screen similar to following displays:

Port	PortType	Intf. Type	Admin/ Oper/ State	Protocol	Speed BPS	Clocking
1	ISDN	ISDN-ST	UP/UP	PPP	N/A	N/A

Serial Board Example

To display the parameters for all ports on the serial board (in slot 3), enter:

```
wpview 3
```

or

```
wpv 3
```

A screen similar to following displays:

Port	PortType	Intf. Type	Admin/ Oper/ State	Protocol	Speed BPS	Clocking
1	Serial	V35DCE	UP/UP	PPP	2048000	Split

T1 Board Example

To display the parameters for all ports on the T1 board (in slot 3), enter:

```
wpview 3
```

A screen similar to following displays:

Slot/Port	PortType	Intf. Type	Admin/ Oper/ State	Protocol	Speed BPS	Clocking
3/1	T1	T1	UP/UP	FR	1544000	Loop

◆ Note ◆

E1 boards provide a similar display, except the port type and interface type display as **E1** and speed displays as **2048000**.

Viewing Port Parameters

To view port parameters, enter the following command:

```
wpview 3/<port>
```

where **3** is the slot number for WAN uplinks, and **<port>** is the port number for which you want to view information (either **1** or **2**). The following three examples show the configuration setup screens for a fractional T1 port, a universal serial port, and an ISDN-BRI port. The display is slightly different depending upon the encapsulation type, either Frame Relay or PPP.

Fractional T1 Port Example

The following example displays the configuration view screen for a fractional T1 port (port 1) using Frame Relay. To view 3/1, enter:

```
wpview 3/1
```

or

```
wpv 3/1
```

A screen similar to following displays:

```
Configuration View for Slot 3, Port 1.  
1) Admin Status ..... UP  
2) Protocol Type ..... Frame Relay  
3) T1/E1 Starting Time Slot ..... 1  
4) T1/E1 Number of Time Slots ..... 24  
8) TOS for Voice Data ..... a0  
9) TOS for Voice Signaling Data ..... 60  
10) TOS Mask for both TOS Value ..... e0  
11) Signaling IP Address ..... 0.0.0.0  
12) Signaling IP Mask ..... 255.255.255.255  
15) Loopback Timeout ..... 10
```

This next example displays the configuration view screen for a fractional T1 port (port 1) using PPP. To view 3/1, enter:

```
wpview 3/1
```

or

```
wpv 3/1
```

A screen similar to following displays:

```

Configuration View for Slot 3, Port 1.
1)  Admin Status ..... UP
2)  Protocol Type ..... Frame Relay
3)  T1/E1 Starting Time Slot ..... 1
4)  T1/E1 Number of Time Slots ..... 24
8)  TOS for Voice Data ..... a0
9)  TOS for Voice Signaling Data ..... 60
10) TOS Mask for both TOS Value ..... e0
11) Signaling IP Address ..... 0.0.0.0
12) Signaling IP Mask ..... 255.255.255.255
13) KeepAlive Up Count ..... 0
14) KeepAlive Down Count ..... 0
15) KeepAlive Timeout ..... 10
16) DTR Pulse Width ..... 0
17) DTR Pulse Count ..... 0
    
```

◆ Note ◆

The DTR Pulse setting do not apply to T1 and E1 interfaces, and are not described below.

Admin Status

The options for the Admin Status are **UP** and **DN**. If **UP**, the port has been enabled and can transmit data as long as its Operational Status is also **UP**. If set to is **DN**, the port will not pass data even if its physical connection is good.

Protocol Type

The protocol type can be set to either Frame Relay or Point to Point Protocol (PPP). The default setting is Frame Relay.

T1/E1 Starting Time Slot

This field specifies the first time slot number to use on a T1 or E1 port. For a full T1 or E1 connection, specify time slot 1. For a fractional T1 or E1 connection, set this field to the starting time slot number as specified by your service provider.

T1/E1 Number of Time Slot

This field specifies the total number of 64 kbps time slots to use on the T1 or E1 connection. For a full T1, set this number to 24. For a full E1 connection, set this number to 30 if you are running multiframe, or 31 if you are not. For fractional T1 or E1, you must set the number of time slots to the value specified by your service provider. For example, a 256 kpbs service uses four time slots (4 x 64 = 256).

TOS for Voice Data

Shows the priority for voice data streams. The value must be entered in hexadecimal format translated from binary, and can use either IP Precedence or Differentiated Services Code Point (DSCP). See *Type of Service (ToS)* on page 48-2 above for a more detailed explanation of ToS.

TOS for Voice Signaling Data

Shows the priority for voice signaling data streams. The value must be entered in hexadecimal format translated from binary, and can use either IP Precedence or Differentiated Services Code Point (DSCP). See *Type of Service (ToS)* on page 48-2 above for a more detailed explanation of ToS.

TOS Mask for both TOS Value

Shows the mask bits for both voice data and signaling data.

Signaling IP Address

When a data frame cannot be identified by the ToS voice data or ToS signaling data, the Signaling IP Address is checked. Matched frames are loaded on a High Priority Software Queue and a Nominal Hardware Queue.

Signaling IP Mask

The mask associated with the Signaling IP Address described above.

KeepAlive Up Count

If the switch detects that a port may be down, it will generate echo message requests to the far end of the connection. The KeepAlive Up Count is the number of requests sent from the port when the port transitions from Down to Up, to verify the status of the port.

KeepAlive Down Count

If the switch detects that a port may be down, it will generate echo message requests to the far end of the connection. The KeepAlive Down Count is the number of requests sent from the port when the port transitions from Up to Down, to verify the status of the port. This only displays if the port is using PPP as its encapsulation type.

KeepAlive Timeout

The number of 100 millisecond increments between generated echo message requests. This only displays if the port is using PPP as its encapsulation type.

Loopback Timeout

Sets the transition time between proprietary messages sent over the link. These messages are analyzed to determine whether the link is in a loopback state. This only displays if the port is using Frame Relay as its encapsulation type.

Universal Serial Port Example

The following example displays the configuration view screen for a universal serial port (port 2). To view 3/2, enter:

```
wpview 3/2
```

or

```
wpv 3/2
```

If the serial port is using Frame-Relay, a screen similar to following displays:

```
Configuration View for Slot 3, Port 2.
1) Admin Status ..... UP
2) Speed in BPS ..... 2048000
3) Clocking ..... Split
4) Protocol Type ..... Frame Relay
7) Receive Clock ..... Normal
8) TOS for Voice Data ..... a0
9) TOS for Voice Signaling Data ..... 60
10) TOS Mask for both TOS Value ..... e0
11) Signaling IP Address ..... 0.0.0.0
12) Signaling IP Mask ..... 255.255.255.255
15) Loopback Timeout ..... 0
```

If the serial port is using Frame-Relay, a screen similar to following displays:

```
Configuration View for Slot 3, Port 2.
1) Admin Status ..... UP
2) Speed in BPS ..... 2048000
3) Clocking ..... Split
4) Protocol Type ..... Frame Relay
7) Receive Clock ..... Normal
8) TOS for Voice Data ..... a0
9) TOS for Voice Signaling Data ..... 60
10) TOS Mask for both TOS Value ..... e0
11) Signaling IP Address ..... 0.0.0.0
12) Signaling IP Mask ..... 255.255.255.255
13) KeepAlive Up Count ..... 0
14) KeepAlive Down Count ..... 0
15) KeepAlive Timeout ..... 10
16) DTR Pulse Width ..... 0
17) DTR Pulse Count ..... 0
```

Admin Status

The options for the Admin Status are **UP** and **DN**. If **UP**, the port has been enabled and can transmit data as long as its Operational Status is also **UP**. If set to **DN**, the port will not pass data even if its physical connection is good.

Speed in BPS

This field displays the access rate for the Frame Relay line to the service provider. This parameter is the speed of the entire connection, not an individual virtual circuit. For example, if you have a 56 kbps line to your service provider, this field should be set to 56000. A full T1 line would have an access rate of 1,544,000 bps, and a full E1 line would have an access rate of 2,048,000 bps. For either T1 or E1, you can also have a fractional service with an access rate that is a multiple of 64 kbps.

Clocking

This field displays either **External**, **Internal**, or **Split**. For a more detailed discussion of clocking, see *Clocking* under *Modifying a Port* on page 48-24.

Receive Clock

Often, due to delays added to timestamps in when running through switch hardware, the receive clock time is significantly different than expected from the transmitting data source. To correct the problem, it is possible to set the receive clock to invert the delay information. The following options are available:

Protocol Type

The protocol type can be set to either Frame Relay or Point to Point Protocol (PPP). The default setting is Frame Relay.

TOS for Voice Data

Shows the priority for voice data streams. The value must be entered in hexadecimal format translated from binary, and can use either IP Precedence or Differentiated Services Code Point (DSCP). See *Type of Service (ToS)* on page 48-2 above for a more detailed explanation of ToS.

TOS for Voice Signaling Data

Shows the priority for voice signaling data streams. The value must be entered in hexadecimal format translated from binary, and can use either IP Precedence or Differentiated Services Code Point (DSCP). See *Type of Service (ToS)* on page 48-2 above for a more detailed explanation of ToS.

TOS Mask for both TOS Value

Shows the mask bits for both voice data and signaling data.

Signaling IP Address

When a data frame cannot be identified by the ToS voice data or ToS signaling data, the Signaling IP Address is checked. Matched frames are loaded on a High Priority Software Queue and a Nominal Hardware Queue.

Signaling IP Mask

The mask associated with the Signaling IP Address described above.

KeepAlive Up Count

If the switch detects that a port may be down, it will generate echo message requests to the far end of the connection. The KeepAlive Up Count is the number of requests sent from the port when the port transitions from Down to Up, to verify the status of the port.

KeepAlive Down Count

If the switch detects that a port may be down, it will generate echo message requests to the far end of the connection. The KeepAlive Down Count is the number of requests sent from the port when the port transitions from Up to Down, to verify the status of the port. This only displays if the port is using PPP as its encapsulation type.

KeepAlive Timeout

The number of 100 millisecond increments between generated echo message requests. This only displays if the port is using PPP as its encapsulation type.

DTR Pulse Width

A Data Terminal Ready (DTR) Pulse is sent at the hardware level to determine a port is still synchronized with its far end connection. The Pulse Width is the number of 100 milli-second increments that the pulse lasts. This only displays if the port is using PPP as its encapsulation type.

DTR Pulse Count

A Data Terminal Ready (DTR) Pulse is sent at the hardware level to determine a port is still synchronized with its far end connection. The Pulse Count is the number of pulses generated when a line is down. This only displays if the port is using PPP as its encapsulation type.

Loopback Timeout

Sets the transition time between proprietary messages sent over the link. These messages are analyzed to determine whether the link is in a loopback state. This only displays if the port is using Frame Relay as its encapsulation type.

ISDN-BRI Port Example

The following example displays the configuration view screen for an ISDN-BRI port (port 2). To view 3/2, enter:

```
wpview 3/2
```

or

```
wpv 3/2
```

A screen similar to following displays:

```
Configuration View for Slot 3, Port 2.
1) Admin Status ..... UP
2) Speed in BPS ..... 2048000
3) Clocking ..... Split
4) Protocol Type ..... Frame Relay
8) TOS for Voice Data ..... a0
9) TOS for Voice Signaling Data ..... 60
10) TOS Mask for both TOS Value ..... e0
11) Signaling IP Address ..... 0.0.0.0
12) Signaling IP Mask ..... 255.255.255.255
13) KeepAlive Up Count ..... 0
14) KeepAlive Down Count ..... 0
15) KeepAlive Timeout ..... 10
16) DTR Pulse Width ..... 0
17) DTR Pulse Count ..... 0
```

◆ Note ◆

The ISDN **wpview** menu displays PPP specific line options described in the section *Modifying a Port* on page 48-24. However, they do not apply to an ISDN port, and are not described below.

Admin Status

The options for the Admin Status are **UP** and **DN**. If **UP**, the port has been enabled and can transmit data as long as its Operational Status is also **UP**. If set to **DN**, the port will not pass data even if its physical connection is good.

Speed in BPS

This field displays the access rate for the Frame Relay line to the service provider. This parameter is the speed of the entire connection, not an individual virtual circuit. For example, if you have a 56 kbps line to your service provider, this field should be set to 56000. A full T1 line would have an access rate of 1,544,000 bps, and a full E1 line would have an access rate of 2,048,000 bps. For either T1 or E1, you can also have a fractional service with an access rate that is a multiple of 64 kbps.

Clocking

This field displays either **External**, **Internal**, or **Split**. For a more detailed discussion of clocking, see *Clocking* under *Modifying a Port* on page 48-24.

Protocol Type

The protocol type can be set to either Frame Relay or Point to Point Protocol (PPP). The default setting is Frame Relay.

TOS for Voice Data

Shows the priority for voice data streams. The value must be entered in hexadecimal format translated from binary, and can use either IP Precedence or Differentiated Services Code Point (DSCP). See *Type of Service (ToS)* on page 48-2 above for a more detailed explanation of ToS.

TOS for Voice Signaling Data

Shows the priority for voice signaling data streams. The value must be entered in hexadecimal format translated from binary, and can use either IP Precedence or Differentiated Services Code Point (DSCP). See *Type of Service (ToS)* on page 48-2 above for a more detailed explanation of ToS.

TOS Mask for both TOS Value

Shows the mask bits for both voice data and signaling data.

Signaling IP Address

When a data frame cannot be identified by the ToS voice data or ToS signaling data, the Signaling IP Address is checked. Matched frames are loaded on a High Priority Software Queue and a Nominal Hardware Queue.

Signaling IP Mask

The mask associated with the Signaling IP Address described above.

Deleting Ports

The **wpdelete** command allows you to delete configuration information for a WSM port. When you delete a this information, all WAN configuration parameters for the selected port revert back to default settings.

To delete a port configuration, enter the following command:

```
wpdelete slot/port
```

in which **slot** is the slot number for the WSM board and **port** is the port number on the WSM board that you want to delete. For example, to delete port 1 on the WSM board in slot 2, enter:

```
wpdelete 2/1
```

or

```
wpd 2/1
```

This system returns the following prompt to confirm the deletion:

```
This will delete Slot 2, Port 1. Continue? {(Y)es, (N)o} (N)
```

Enter a **Y** to confirm the deletion or press **Enter** to cancel the deletion.

Note

The **wpdelete** command requires that you indicate a slot and port number. For example,

```
wpdelete
```

would be an incorrect usage, whereas,

```
wpdelete 4/2
```

would be correct.

Obtaining Status and Statistical Information

You can obtain general and detailed WAN port statistical information on all WSM boards in the switch, a single WSM board, individual ports, and Frame Relay and PPP protocols. The **wpstatus** command is used to provide this information. This information includes types of physical interface, access rate of the Frame Relay line, and errors. In addition, the **wpstatus** command can display the number of frames received and transmitted.

Obtaining Information on All Boards in a Switch

To obtain status information on all WSM boards in a switch, you enter the **wpstatus** command without any parameters as follows:

```

wpstatus
or
wps
    
```

This command displays a screen similar to the following (In this example, the port parameters being displayed are for a system that contains a 2-port WSM-BRI module in slot 4, an 8-port WSM module in slot 5, and a 2-port WSM in slot 8.):

Slot/Port	PortType	Intf. Type	Admin/	Protocol	BPS	Speed	Utilization		
			Oper/			Clocking	10s	1m	5m
=====	=====	=====	=====	=====	=====	=====	=====	=====	=====
4/1	Serial	*NONE*	UP/DN	FR	EXT CLK	External	10%	10%	10%
4/2	ISDN	ISDN-ST	UP/DN	PPP	N/A	External	40%	30%	60%
5/1	Serial	V35DCE	UP/UP	PPP	2048000	Split	30%	60%	50%
5/2	Serial	V35DCE	UP/UP	FR	2048000	Split	100%	50%	70%
5/3	Serial	X21DCE	UP/DN	FR	2048000	Split	90%	80%	60%
5/4	Serial	V35DCE	UP/UP	FR	2048000	Split	20%	50%	50%
5/5	Serial	*NONE*	UP/DN	FR	EXT CLK	External	30%	30%	50%
5/6	Serial	*NONE*	UP/DN	FR	EXT CLK	External	100%	50%	80%
5/7	Serial	*NONE*	UP/DN	FR	EXT CLK	External	70%	50%	50%
5/8	Serial	*NONE*	UP/DN	FR	EXT CLK	External	100%	80%	30%
8/1	T1	T1	UP/UP	FR	1544000	External	80%	50%	70%
8/2	Serial	530DCE	UP/UP	FR	2048000	Split	10%	50%	40%

Each row in the table corresponds to a physical port on a WSM board in the switch. The following sections describe the columns shown in this table:

Field Descriptions

The following section explains the fields and their corresponding values.

Slot/Port

The first number in this column is the slot in the switch where this WSM is installed. The second number is the port number on the WSM.

Port Type

This column shows

- Serial
- ISDN
- T1
- E1

Intf Type

This column indicates the physical cable type connected to this port. This cable type is automatically sensed by the WSM/WSX hardware. This column indicates the cable type and whether it is DCE or DTE. The following values may appear in this column:

- **V35DTE** (V.35 DTE cable)
- **V35DCE** (V.35 DCE cable)
- **232DTE** (RS-232 DTE cable)
- **232DCE** (RS-232 DCE cable)
- **X21DTE** (X.21 DTE cable)
- **X21DCE** (X.21 DCE cable)
- **530DTE** (RS-530 or RS-449 EIA DTE cable)
- **530DCE** (RS-530 or RS-449 EIA DCE cable)
- **T1**
- **E1**
- **ISDN-ST**
- **ISDN-U**

The WSM sees RS-530 and RS-449 cables the same because they are electrically identical. However, this does not affect the operation of either cable type. Both RS-530 and RS-449 cables are supported.

If no cable is connected to a universal serial port, then this column will display:

NONE

If an error has been detected on the port (e.g., cable type could not be detected), the following value displays:

ERROR!

Admin/Oper State

This column shows the Administrative and Operational State of this WSM port. The value before the slash refers to the Admin Status. If **UP**, the port has been enabled and can transmit data as long as its Operational State is also **UP**. If the Admin Status is **DN**, the port will not pass data even if its physical connection is good.

The value after the slash refers to the Operational State. If **UP**, the port is capable of passing data as long as it has been logically enabled at the Administrative level. If **DN**, the port cannot pass data due to a problem in the physical connection (e.g., cable disconnected, WSM could not detect cable type) or because the port is administratively down. If the Operational State displays **LB**, the port is currently in Loopback (test) mode.

Protocol

The protocol type can be set to either Frame Relay or Point to Point Protocol (PPP).

Speed BPS

This column indicates the speed, or access rate, between the WSM serial port and DSU or other physical DTE device. The speed is expressed in bits per second (bps). This speed is the total bandwidth available on the line connected to this port. Virtual circuits on this port share this bandwidth.

Usually, the WSM port will be a physical DTE device and the speed will be determined by the DSU. In this case, this value will read **EXT CLK**, which means the WSM port gets its clocking from an externally attached DCE device (i.e., DTE cable plugged into WSM port) or no cable is attached. If the WSM port is a physical DCE device (i.e., DCE cable plugged into WSM port), then this value will be the actual clock rate used by the port.

Clocking

Indicates the type of clocking used on this port. The three types of clocking are described in *Clocking* on page 48-27.

Utilization

Indicates the amount of port usage, expressed in bandwidth percentage, over three durations: the previous ten seconds (**10s**), the previous minute (**1m**), and the previous five minutes (**5m**).

Obtaining Information on the Ports for a Single WSM Board

To obtain status information on a single WSM board, enter the **wpstatus** command and the slot number for the WSM board, as follows:

```
wpstatus slot
```

where **slot** is the slot number where the WSM board is installed. For example, if you wanted to obtain status information for the board in slot 4. In the following three examples, the port parameters being displayed are for a system that contains a 2-port WSM ISDN-BRI board in slot 4, an 8-port WSM serial board in slot 5, and a 2-port WSM T1 board in slot 8.)

ISDN-BRI Board Example

In this example, the board in slot 4 is a 2-port ISDN-BRI WSM board. To view the status of slot 4, enter:

```
wpstatus 4
```

or

```
wps 4
```

This command displays a screen similar to the following:

```
WAN Port Status for slot: 4
```

PT	Admin/ Oper Status	Intf Type	Speed BPS	Frames In	Frames Out	Octets In	Octets Out
1	UP/DN	*NONE*	EXT CLK	0	0	0	0
2	UP/DN	ISDN-ST	N/A	0	0	0	0

/Interface/WAN %

Each row in the table corresponds to a port on the WSM you requested information on.

8-Port WSM Board Example

In this example, the board in slot 5 is an 8-port WSM board. To view the status of slot 5, enter:

```
wpstatus 5
```

or

```
wps 5
```

This command displays a screen similar to the following:

```
WAN Port Status for slot: 5
```

PT	Admin/ Oper Status	Intf Type	Speed BPS	Frames In	Frames Out	Octets In	Octets Out
1	UP/UP	V35DCE	2048000	3	17	36	276
2	UP/UP	V35DCE	2048000	175	926	2034	25617
3	UP/UP	X21DCE	2048000	123	931	1722	55717
4	UP/UP	V35DCE	2048000	776	189	14430	7531
5	UP/DN	*NONE*	EXT CLK	0	0	0	0
6	UP/DN	*NONE*	EXT CLK	0	0	0	0
7	UP/DN	*NONE*	EXT CLK	0	0	0	0
8	UP/DN	*NONE*	EXT CLK	0	0	0	0

```
/Interface/WAN %
```

2-Port Fractional T1 WSM Board Example

In this example, the board in slot 8 is a 2-port Fractional T1 WSM board. To view the status of slot 8, enter:

```
wpstatus 8
```

or

```
wps 8
```

This command displays a screen similar to the following:

```
/Interface/WAN % wps 8
```

```
WAN Port Status for slot: 8
```

PT	Admin/ Oper Status	Intf Type	Speed BPS	Frames In	Frames Out	Octets In	Octets Out
1	UP/DN	T1	1544000	0	0	0	0
2	UP/UP	530DCE	2048000	45695	47761	10596229	2560992

```
/Interface/WAN %
```

Field Descriptions

The following section explains the fields and their corresponding values.

PT

The port number on the WSM board for which statistics are displayed.

Admin/Oper Status, Int Type, Speed Bps

These columns are described in the section, *Obtaining Information on All Boards in a Switch* on page 48-46. Please refer to this section for detailed information.

Frames In

The total number of frames received on this port since the last time the switch was initialized.

Frames Out

The total number of frames sent on this port since the last time the switch was initialized.

Octets In

The total number of octets, or bytes, received on this port since the last time the switch was initialized. This statistic includes the data and Frame Relay or PPP header fields, but does not include CRC or flag characters.

Octets Out

The total number of octets, or bytes, sent on this port since the last time the switch was initialized. This statistic includes the data and Frame Relay or PPP header fields, but does not include CRC or flag characters.

Viewing Information on a Single Port

To obtain status information on a single WSM port, enter the **wpstatus** command, followed by the slot number for the WSM board and the port number for which you want to receive information, as follows:

```
wpstatus <slot>/<port>
```

or

```
wps <slot>/<port>
```

where **<slot>** is the slot number where the WSM board is installed and **<port>** is the port number on the WSM board.

Frame Relay Example

In the following example, port 1 on slot 4 is configured for Frame Relay. To obtain status information for this port, enter:

wpstatus 4/1

A screen similar to the following will be displayed:

Frame Relay Status for slot 4, port 1:

Applicable to all port types.

Physical Level Information.

Displays for serial ports only

Logical (Frame Relay) Information

Virtual Circuit Level Information

```

Administrative/Operational Status .....Up/Up
Port Type.....Universal Serial Port
Protocol.....Frame Relay

Speed      Intf.      Receive      Receive      Receive      Transmit      Signal
BPS        Type       CRC Errors   Aborts       Overruns     Overruns     Errors
=====
2048000    V35DCE    0            0            0            0            0

Control    DTR      RTS      DSR      CTS      DCD
Signal     ON       ON       ON       ON       OFF

Frame Relay Information:
UniCast   Discarded   Error
Octets    Frames     Frames     Count
=====
IN         941079     0          0
Out       21334     0          0
IN+OUT    962413     0          0

Administrative/Operational Phase .... Up/Up

Last Error Type .....No Error Since Reset
Last Error Time .....0 days, 00:00:00
Interface failures .....0
Last interface failure time .....0 days, 00:00:00

DLCI Information:
Admin/
DLCI Oper  DLCI      Frames     Frames     Octets     Octets
Num  Status  Type      In         Out        In         Out
==== =====
0    UP/UP   Configured  1021      1021      16044      1494
31   UP/UP   Learned    17716     136       2746651    12663
32   UP/DN   Learned     0         0         0          0
        
```

This command displays three (3) layers of information. The top section provides information on the physical interface. The middle section provides information on the logical, or Frame Relay, interface. The bottom section provides information on the virtual circuits associated with this physical port.

For detailed descriptions of the fields, refer to Chapter 49 “Managing Frame Relay.”

PPP Example

In the following example, port 1 on slot 4 is configured for Point-To-Point Protocol (PPP). To obtain status information for this port, enter:

wpstatus 5/1

A screen similar to the following will display:

```

/Interface/WAN % wps 5/1
WAN Port Status for slot 5, port 1:
Administrative/Operation Status: ..... UP/UP
Port Type ..... Universal Serial Port
Protocol ..... PPP

Speed      Intf.      Receive      Receive      Receive      Transmit      Signal
BPS        Type      CRC Errors   Aborts       Overruns     Underruns     Errors
=====
2048000    V35DCE           0           0           0           0           0

Control    DTR  RTS  DSR  CTS  DCD
Signals    ON  ON  ON  ON  ON

PPP Management Statistics:

Admin      IP      IPX      BCP      CCP
Status     Mode   Oper    Oper    Oper    Oper
=====
UP         Normal Open    Close   Open    Open

LCP Pkts   IPCP Pkts  IPX Pkts  BCP Pkts  CCP Pkt
IN/OUT     IN/OUT     IN/OUT    IN/OUT    IN/OUT
=====
3/4        2/2        4/0       2/2       3/3

          Packets   Packets   Packets   Octets   Octets   %In   %Out
          In      Out      In+Out   In      Out      %In   %Out
          =====
Total          284     5809     6093     100333  344187
Ethernet       0     1337     1337       0    157846      0     45
8025           0         0         0         0         0      0     0
FDDI           0         0         0         0         0      0     0
IP            281      282      563     100216  22931     99     6
IPX           0         0         0         0         0      0     0
BPDU          3     4190     4193      117    163410      0     47

STAC-LZS      Compressed   Compressed   Uncompressed   Compression
Compression:  Frames      Octets      Octets          Ratio
          =====
In          284         8635         100333         11.6:1
Out         5809        96794         449230         4.6:1
In+Out      6093       105429         549563         5.2:1

/Interface/WAN %
    
```

◆ Note ◆

The section devoted to compressed data traffic statistics will be displayed only if the port has been configured for STAC-LZS compression.

For detailed descriptions of the fields, refer to Chapter 50, “Point-to-Point Protocol.”

Configuring 31 Timeslots on a WAN E1 Port

On WSM E1 ports, the unframed format is not supported since WSMs only support standard E1 framing for PPP or Frame Relay (the “unframed” format is only supported for unstructured Circuit Emulation T1 or E1 ports). WSM E1 ports *must* be set to one of the standard E1 Framing types (E1, E1-CRC, E1-MF, E1-MF-CRC) with the **temod** command. (See Chapter 53, “Managing T1 and E1 Ports,” for more information on the **temod** command.)

Most E1 services only allow a maximum of 30 usable timeslots since timeslot 0 is always used for Frame Synchronization (which is why you cannot use unframed for Frame Relay or PPP ports since you *must* specify how timeslot 0 is used) and timeslot 16 is usually used for multiframe sequencing.

The WSM can support 31 timeslots for cases where timeslot 16 is not used for multiframe control. When you configure the timeslots for a WSM E1 port, you specify a starting timeslot followed by a number of timeslots by using the **wpmodify** command. (See *Modifying a Port* on page 48-24 for more information on the **wpmodify** command.)

Normally, the WSM will use a default configuration that skips timeslot 16 automatically. In this way, it will select the E1 frame to generate E1 timeslot 0 (the “synchronization” timeslot), but leave timeslot 16 (the “multiframe control” timeslot) free. The WAN port configuration software when configured for 31 timeslots will then use all timeslots from 1 to 31 to give you a full E1 where timeslot 16 is also used for data. Again, this should only be done for facilities that do not require E1 Multi-Frame. For those types of E1 lines, they can support a maximum of 30 timeslots. Only those E1 lines that do not require E1 multiframe can be configured in the method described below.

To configure a WAN E1 port for 31 timeslots, follow the steps below:

1. Enter **temod <slot>/<port>** at the system prompt, where **<slot>** is the slot number of the module with the E1 port and **<port>** is the port number of the E1 port. For example, to configure WSM E1 port 4/2, enter **temod 4/2**.
2. Enter **2=4** at the prompt to set the frame type to E1 or enter **2=5** at the prompt to set the frame type to E1-CRC.
3. Enter **save** at the prompt to save your settings.
4. Enter **wpmodify <slot>/<port>** or **wpm <slot>/<port>** at the system prompt, where **<slot>** is the slot number of the module with the E1 port and **<port>** is the port number of the E1 port. For example, to configure WSM E1 port 4/2, enter **wpm 4/2**. (Note: **wpm** is the abbreviated form of **wpmodify**.)
5. Enter **3=1** to set the starting timeslot to 1.
6. Enter **4=31** to set the number of timeslots to 31.
7. Enter **save** at the prompt to save your settings.

49 Managing Frame Relay

The WAN Switching Module (WSM) family supports Frame Relay on universal serial, T1 or E1 ports. Management, data handling, compression, and multi-protocol encapsulation are compatible with current Frame Relay standards, such as RFC 1490 and FRF.9. The WSM supports all three major DLCMI management protocols.

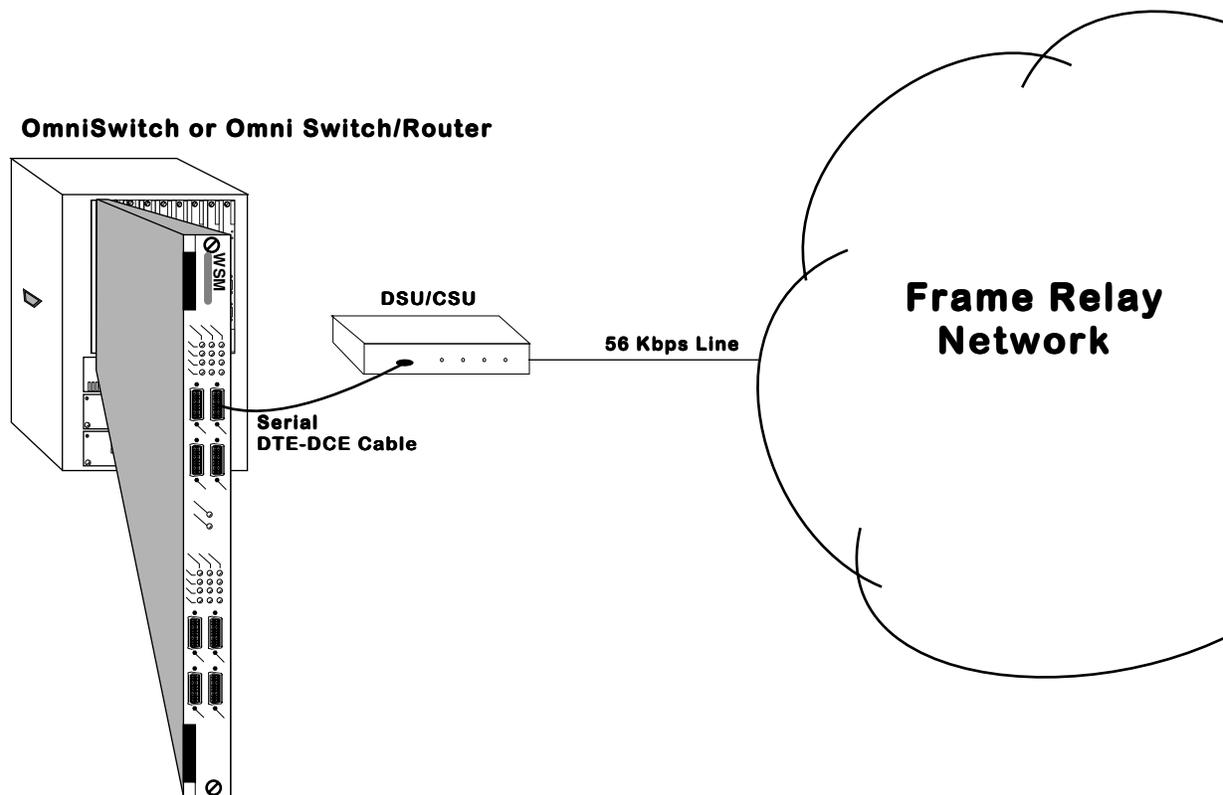
Note on Terminology

Although this chapter primarily uses the terms “OmniSwitch” and “WSM,” everything discussed in this chapter applies equally to the Omni Switch/Router and Omni Switch/Router WAN Switching Module (WSX).

WSM frame relay extends the power and flexibility of LAN switching over large geographic distances using a Frame Relay network or a leased line, such as a T1. In a Frame Relay network configuration, the WSM provides a cost effective link supporting multiple virtual circuits. In a leased line configuration, the WSM provides dedicated bandwidth to a single remote site.

VLAN architectures are preserved and consistent on both sides of a WAN link. The WSM supports frame relay trunking, so VLAN Groups on one side of a Frame Relay link are compatible with those on the other side. In addition, the WSM is capable of Frame Relay IP and IPX routing and complies with Inverse Address Resolution Protocol (InARP) RFC 1293.

In a typical configuration, the WSM occupies one slot in an OmniSwitch. Since it is compatible with OmniSwitch any-to-any switching and VLAN architecture, you can switch other topologies in the LAN to Frame Relay. The following diagram shows a typical WSM setup using a 56 Kbps Frame Relay line (up to 2 Mbps access rates are supported).



Typical WSM Frame Relay Setup Using Serial Ports

The WSM supports automatic detection of cable types attached to universal serial ports. It also supports three types of DLCMI management: LMI Rev. 1.0, ANSI T1.617 Annex D, and CCITT/ITU-T Q.933 Annex A.

Software in the switch allows you to configure access rate, clocking, DLCMI type, compression, and congestions controls, such as the Committed Information Rate (CIR). Additional software commands allow you to view the status of the Frame Relay connection at the WSM board, port, or virtual circuit level. Extensive statistics are provided at each level, including a breakdown of traffic by frame type (Ethernet, IP, IPX, or BPDU) at the virtual circuit level.

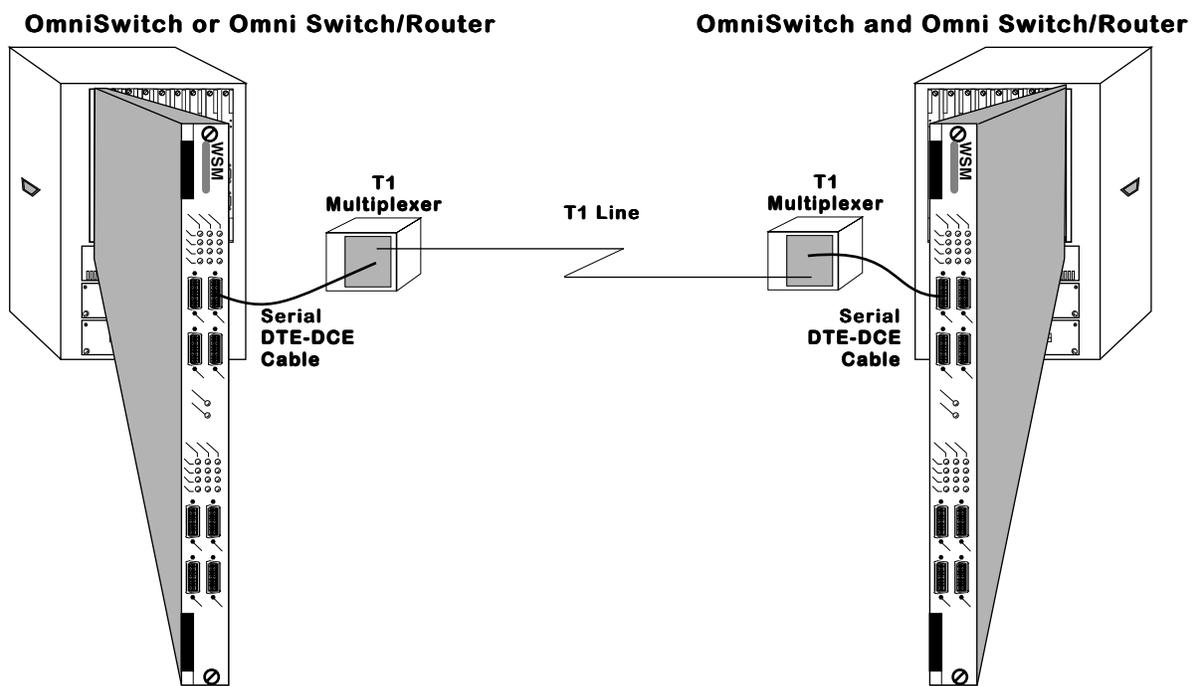
The WSM is designed to require as little configuration as possible. It senses the cable type installed and automatically maps virtual circuits to virtual ports as soon as you plug in the cable. The WSM supports 256 Permanent Virtual Circuits (PVCs), which is equivalent to the number of virtual ports allowed in an OmniSwitch.

In addition, you can set up a default bridging and a default routing Group. Virtual circuits are automatically assigned to these Groups as soon as they are configured or learned, which means Frame Relay frames can be bridged or routed without user-configuration.

Back-to-Back Frame Relay Configurations

Frame Relay switching modules may be connected “back-to-back” without an intervening Frame Relay network or switch. Such connections are made by using private leased lines, such as T1 lines, instead of public Frame Relay networks usually over large geographic distances.

No special user configuration is necessary for back-to-back connections. The WSM software automatically detects that a Frame Relay Logical DCE (i.e., Frame Relay switch) is not present and that there is another Frame Relay Logical DTE (i.e., another WSM, FRAD, bridge/router) on the other end of the WAN connection. The WSM then automatically brings up a Permanent Virtual Circuit identified with a DLCI of 32, which is the same value IBM uses in this scenario. The WSM does not bring up PVC DLCI 32 until it knows that it has established communication with another DTE device rather than a Frame Relay switch.



Back-to-Back Frame Relay Configuration Using Serial Ports

Universal Serial Port Cable Interfaces

The WSM automatically senses the cable type that you plug into one of its universal serial ports. It can sense whether the cable type is DCE or DTE and whether it is one of the following interfaces:

- RS-232
- RS-449
- RS-530
- V.35
- X.21 (European)

All cable types, except RS-232, are capable of access rates from 9.6 Kbps to 2 Mbps. The RS-232 cable is not compatible with speeds greater than 64 Kbps. Each cable type is illustrated and described in Appendix D, “Custom Cables.”

The WSM serial port is normally considered a physical DTE device. It is possible to turn it into a physical DCE device simply by plugging in a DCE cable. The WSM board internally senses whether a DCE or DTE cable is connected.

DTE/DCE Type and Transmit/Receive Pins

The RS-232 protocol, which is employed at the physical level for all cable types, always defines Transmit and Receive pins in relation to the DTE. So, the type of cable you attach (DCE or DTE) determines the direction of data flow on your connector’s Transmit and Receive pins.

If the WSM serial port is a physical DTE, which is probably the most common configuration, then data is received on Receive pins and transmitted on Transmit pins. If you are using a WSM port as a physical DCE, then data is *transmitted* on the Receive pins and *received* on the Transmit pins.

“Physical” and “Logical” Devices

This chapter refers to “physical” and “logical” DTE (Data Terminal Equipment) and DCE (Data Communication Equipment) devices. A physical device operates on the network layer, and is normally an actual piece of hardware, such as a WSM or CSU/DSU. Physical devices may further be differentiated as DTE and DCE devices. A physical DTE device would be a piece of hardware, such as a WSM, that does not control the access rate for virtual circuits. The physical DTE device is a conduit for data traffic but not a controller of data traffic. A physical DCE device is hardware, such as a CSU/DSU, that does control access rates of Frame Relay traffic. Normally physical DTE and DCE devices are directly connected to one another.

Logical devices operate on the Frame Relay protocol layer, and are sometimes referred to as “Frame Relay logical” devices. Logical devices can also be broken down into DTE and DCE devices. Logical DTE devices, again like the WSM, do not have direct control over the Frame Relay network and the various congestion and control parameters that govern it. Logical DTE devices do not control such actions as bringing up and tearing down virtual circuits; they act upon updates and commands generated by the Frame Relay network. Logical DCE devices, such as a Frame Relay switch, have a large span of control over Frame Relay network traffic. They bring up and tear down virtual circuits, set congestion control bits in packets, and communicate status to logical DTE devices.

Compression

Data compression allows you to get more data through the Frame Relay pipeline, further enhancing cost benefits. A typical data compression ratio on the WSM board at the hardware level is 4:1. In addition, the compression processor (STAC 9705) has its own DRAM that can store up to 100 virtual circuits (on a 4-port WSM) without performance degradation. An 8-port WSM can store up to 200 virtual circuits without performance degradation. Support for more than 100 compressed VCs (or 200 VCs on an 8-port WSM) is possible through swapping within memory, but compression performance may decrease at these levels.

The WSM will only compress data if you enable Compression Negotiation through software and the Bridge/Router on the other end of the Frame Relay virtual circuit supports standard FRF.9 compression. (An OmniSwitch-to-OmniSwitch connection would support compression.) Negotiation is necessary because if compressed data is sent to a Bridge/Router that does not support compression, then this Bridge/Router will not recognize the data and will automatically drop the unrecognizable frames.

If you enable Compression Negotiation, the WSM will query the Frame Relay device on the other end of the circuit (according to FRF.9 specifications) to see if it supports compression. If it does, then the WSM compresses all data except DLCMI (management) data. If it doesn't, then data on that virtual circuit is sent uncompressed. See *Setting Configuration Parameters* on page 49-21 for information on enabling compression.

Note

Compression is not supported on the 2 universal serial port OmniSwitch WSM and Omni Switch/Router WSX modules.

Virtual Circuits and DLCIs

The WSM supports Permanent Virtual Circuits (PVCs), but not Switched Virtual Circuits (SVCs). Most service carriers do not currently offer SVCs. PVCs are either static (configured) or dynamic (learned). Static PVCs are user-configured and consist of Management, or Control, PVCs and any configured Data PVCs. Management VCs are used by the WSM to communicate with the Frame Relay network. Dynamic PVCs are usually data circuits, which are controlled by the Frame Relay network and not configured in advance. A logical Frame Relay DTE device like the WSM does not create or control dynamic data VCs. It is only informed of their status through periodic Status updates from the Frame Relay network.

Each virtual circuit is locally defined by a Data Link Connection Identifier (DLCI). The Frame Relay network assigns the DLCIs and informs the WSM about them.

DLCI numbers from 0 to 15 and 992 to 1023 are reserved for Control VCs. If you are using Annex A or Annex D as your DLCMI, the management control VC will be assigned DLCI 0. If you are using the LMI Revision 1.0 DLCMI, then the management control VC will be assigned DLCI 1023.

DLCI numbers from 16 to 991 are reserved for Data VCs.

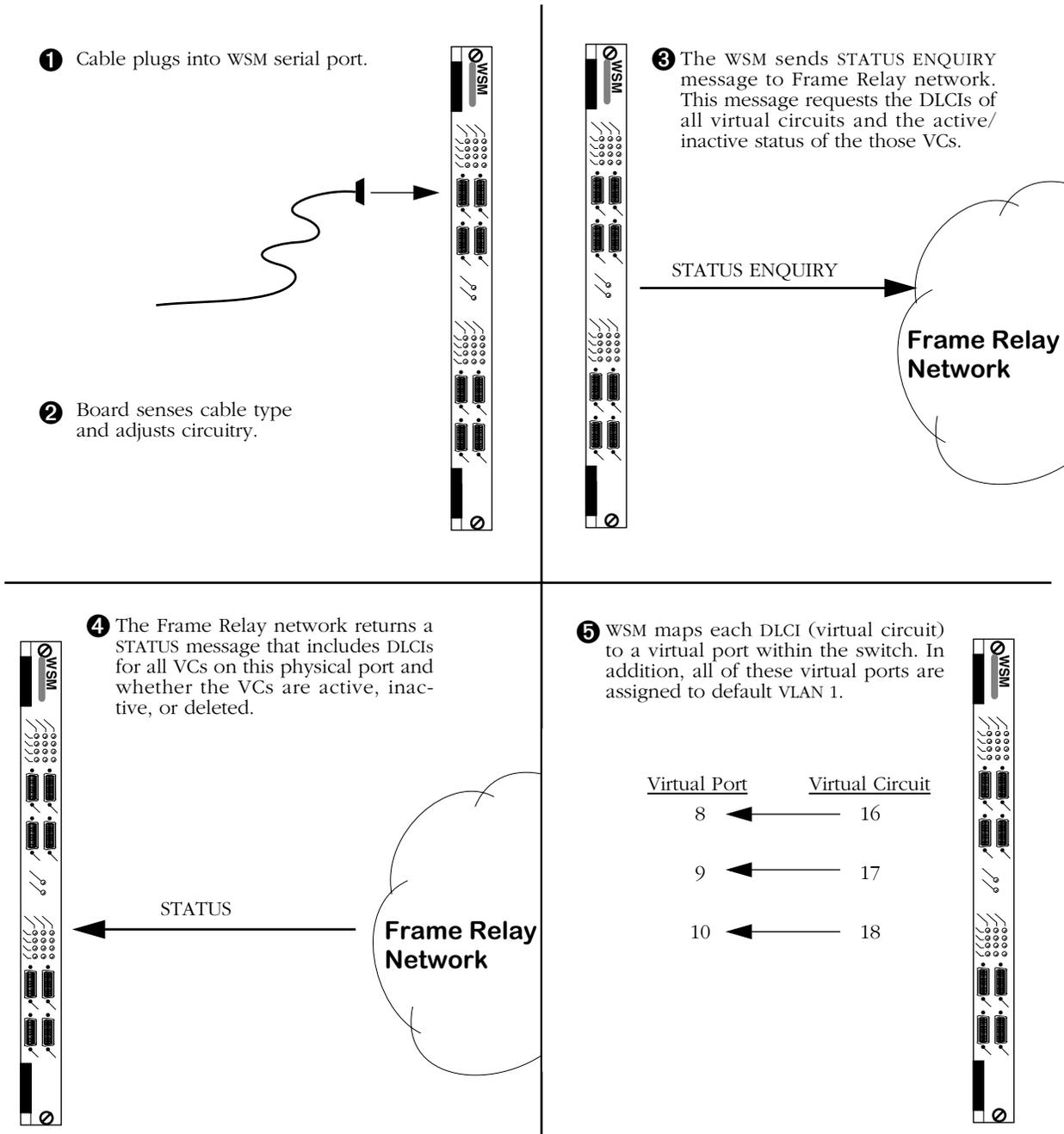
You may have up to 256 virtual circuits and up to 128 virtual ports on a WSM.

A VC may or may not have the same DLCI on each side of a WAN link. For example, if a WSM physical port contains three Frame Relay VCs on its local network with DLCIs 16, 17, and 18, these same VCs on the other side of the Frame Relay network might be 30, 31, and 32. The two sets of DLCIs are technically part of the same virtual circuits, but their values may or may not be different. DLCIs are only significant locally.

At any one time, a virtual circuit will be active, inactive or deleted. If a virtual circuit is Active it can transmit and receive data. If it is Inactive, the Frame Relay network still sees the virtual circuit, but there is a problem with it and it is discarding data. If the virtual circuit is Deleted, then the virtual circuit is not transmitting or receiving data and no DLCI exists for it.

WSM Self-Configuration and Virtual Circuits

The following diagram summarizes the self-configuration features of the WSM. This example assumes no configuration parameters are entered for the WSM. Default bridging is set up on Group 1, and no Routing or Trunking are configured.



WSM Initial Port and Virtual Circuit Configuration

After mapping virtual circuits to virtual ports, the WSM is ready to send data. STATUS ENQUIRIES are repeated periodically by the WSM. The intervals between STATUS ENQUIRES can be configured through software. See *Setting Configuration Parameters* on page 49-21 for information on setting these parameters.

Congestion Control

Use of Frame Relay lines tends to be “bursty,” with heavy use at times and light use at others. During heavy periods of congestion, data may be discarded. However, Frame Relay uses several software-configurable parameters and techniques to control congestion and to avoid data loss on the network during these heavy periods. These software parameters are set on a VC-by-VC basis. This section describes these parameters.

Note

The parameters in this section describe how the Frame Relay network handles congestion. The WSM supports these parameters, but they must match those used by your Frame Relay service provider.

Regulation Parameters

The **Committed Information Rate (CIR)**, which is also referred to as “VC Throughput,” is the minimum bandwidth a virtual circuit will provide under normal circumstances. Frames transmitted within the CIR are not tagged by the Frame Relay network as being eligible for discard. Frames transmitted above the CIR are tagged for discard, but they will normally only be discarded if the virtual circuit or network becomes congested. For example, if the CIR is 16 Kbps and you have a 56 Kbps line, then this virtual circuit will always get at least 16 of the available 56 Kbps. The extra 40 Kbps ($56-16=40$) is normally available to this virtual circuit as long as it is not being used by other virtual circuits and depending on how you have configured the **Committed Burst Size (Bc)** and **Excess Burst Size (Be)**, which are described below.

The CIR is normally a rate given by your service provider. Your service provider may not allow a CIR, in which case your CIR would be 0 (no committed data rate for the virtual circuit).

The **Committed Burst Size (Bc)** is the amount of data that the network will guarantee to transfer under normal conditions. The data may or may not be contiguous and is expressed in kilobits. This number is related to your CIR. In fact, the CIR is Bc divided by Tc where Tc is the time interval used to express the CIR. If Tc is equal to 1 second (a typical value for Tc) and your Bc is 16 kilobits, then your CIR is equal to 16 Kbps. So in many cases the Committed Burst rate will be the same number as the CIR expressed as a *quantity* of data (kilobits) rather than a data *rate* (kilobits per second).

The **Excess Burst Size (Be)** is the amount of data over-and-above the Committed Burst Size (Bc) that the network will transmit as long as excess bandwidth is available on the virtual circuit. The number is also expressed in kilobits. Data at this level is not guaranteed transfer. Any data exceeding the Committed Burst Size may be part of the Excess Burst Size. If there is no bandwidth available on the virtual circuit or if the network is congested, the first data to be dropped is part of this Excess Burst data.

The Excess Burst Size is related to the Committed Burst Size and the access rate of the Frame Relay line. The Excess Burst Size plus the Committed Burst Size should be less than or equal to the access rate of the Frame Relay line. So, if you have a 56 Kbps line and the Committed Burst size is 16 kilobits, then the Excess Burst Size could range from 0 to 40 kilobits.

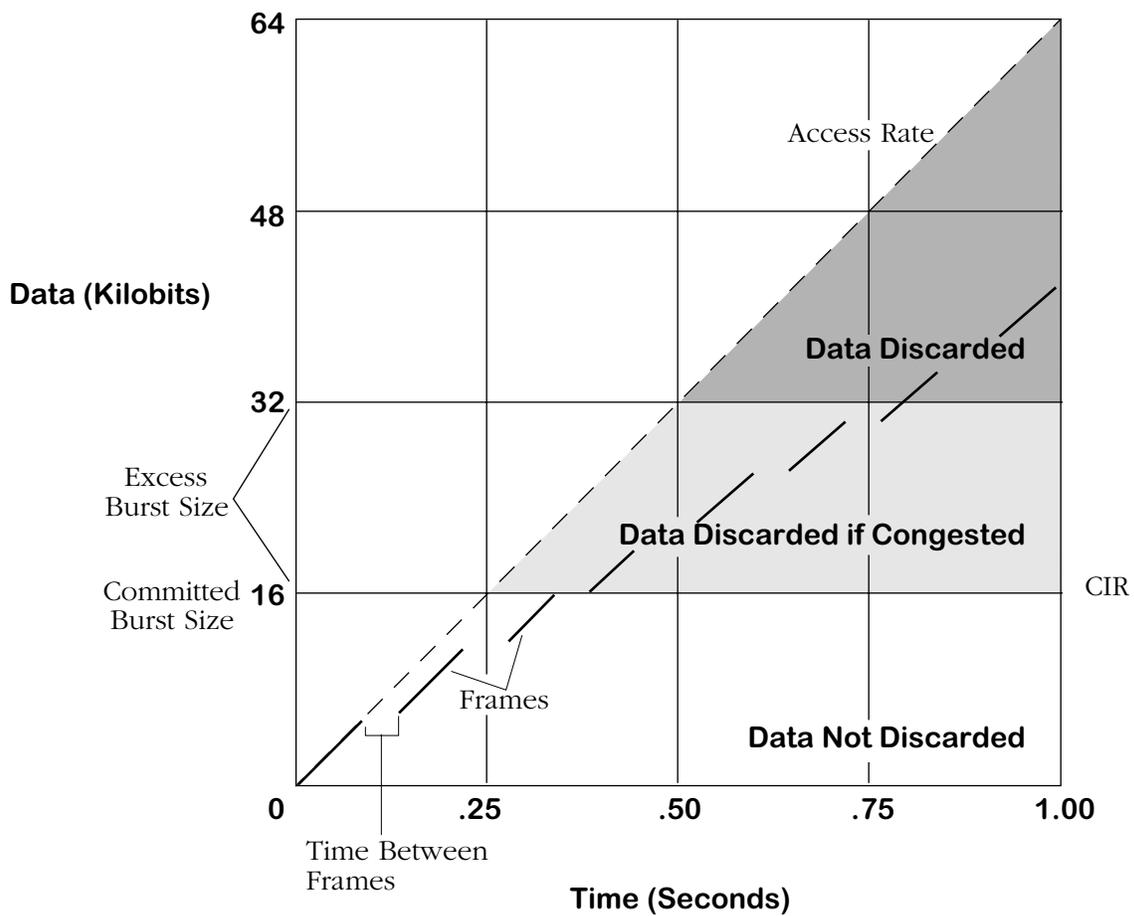
By default all of these congestion control parameters are set to zero (0), meaning that congestion control is disabled and data flows at the access rate for learned virtual circuits. Congestion control is not enabled until you set one or more of these parameters to a non-zero number.

Discard Eligibility (DE) Flag

The Frame Relay network keeps track of data that is eligible for discard by using a single bit within each frame. When the data rate exceeds the CIR, frames are tagged (i.e., the DE bit is set to 1). If congestion in the network nears saturation, those frames tagged with the DE bit will be dropped before untagged frames. Unless totally congested, data below the CIR level on all virtual circuits is usually guaranteed delivery. Normally, frames are not dropped on an entire Frame Relay connection, but only those frames that exceed the pre-defined CIR level.

Interaction Among Congestion Parameters

The following example helps illustrate the interaction among congestion regulation parameters. A Frame Relay line has an access rate of 64 Kbps. The guaranteed Committed Information Rate (CIR) is 16 Kbps. The Committed Burst Size is 16 Kilobits and the Excess Burst Size is also 16 Kilobits. These parameters mean that any data exceeding 16 Kilobits (within a Tc sample period) normally will be tagged with a Discard Eligibility flag and could be discarded if congestion occurs on the virtual circuit. In addition, since the Excess Burst Size is 16 kilobits, any frames sent exceeding 32 Kbps will have a higher probability of being discarded. The following graph illustrates this example.



Effect of Congestion Control Parameters on Data

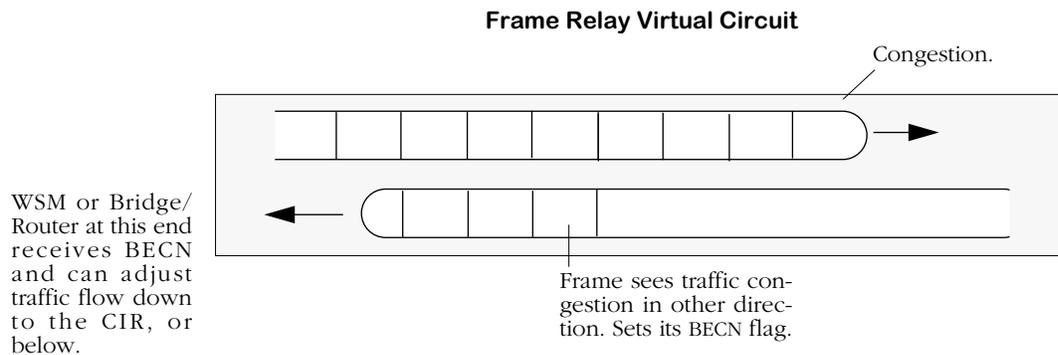
Congestion Control

Frames are shown as broken lines below the Access Rate line. The space between frames indicates the delay between the transmission of each frame. For each second, frames sent within the white zone below the diagonal Access Rate line get through. The shaded area just above the white area contains frames that are stamped for Discard Eligibility that will get through as long as the VC is not congested. The darkest shaded area shows frames that may not get through because they exceed the Excess Burst Size allowed in one second.

Notification By BECN

Each data link header contains a congestion control flag called BECN (Backwards Explicit Congestion Notification), which is usually pronounced “beckon.” Normally this flag is turned off. As with other WAN packet-based networks, frames in Frame Relay may build up in queues at certain points. When a queue is full, due to congestion, frames will be dropped. The senders of this data (Bridge/Router or WSM) may not be aware of the congestion. Frame Relay uses a congestion notification technique to notify the Bridge/Router that traffic is jammed further down the circuit.

When a frame on one side of the bi-directional virtual circuit sees data congested on the other side, the Frame Relay network sets the frame’s BECN flag On. Any subsequent frames that see the congestion also have their BECN flag set On. These BECN frames continue down the virtual circuit until they reach the Bridge/Router or WSM on the other end. The receiving WSM sees the BECN flags and adjusts data flow in the opposite direction. Normally the WSM will slow the speed of data down to the CIR. If the BECNs persist, then data flow is stepped down even further. Data flow will gradually increase back up to the normal rate as soon as BECNs or FECNs (see below) are no longer received.

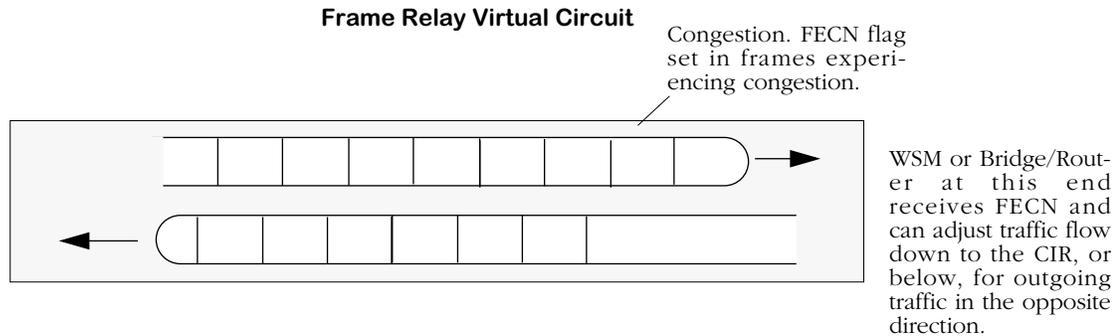


Congestion Notification Using a BECN

BECN notification only works if traffic flows in both directions. If traffic in the uncongested direction did not exist then there would be no frames for the Frame Relay network to set BECN flags on.

Notification By FECN

Frame Relay headers also contain a congestion control bit called FECN (Forwards Explicit Congestion Notification), which is usually pronounced “Feckon.” Like BECN, the FECN bit also notifies a WSM or Bridge/Router of congestions problems. However, it is set by the Frame Relay network in frames that are actually experiencing congestion. When the WSM receives frames with their FECN bit set, it knows that congestion is already occurring on the virtual circuit in the direction that these FECN frames are travelling. The WSM reacts by reducing the data flow down to the CIR for data in the opposite direction. If the FECNs persist, then data flow is stepped down even further. Data flow will gradually increase back up to the normal rate as soon as FECNs or BECNs are no longer received.



Congestion Notification Using a FECN

Frame Formats Supported

Frames coming in from the Frame Relay network are not translated, but they are manipulated to be compatible for transport over the switch's VBUS. Incoming frames must contain RFC 1490 headers. The following standard 1490 frame types are supported:

- BPDU
- Ethernet 802.3
- Token Ring 802.5 (see Note below)
- FDDI (see Note below)
- IP Routed
- ARP/InARP Routed
- IPX Routed
- Compressed (which decompresses to one of the above supported formats)

Note

Source Routing is not supported on Token Ring and FDDI frames.

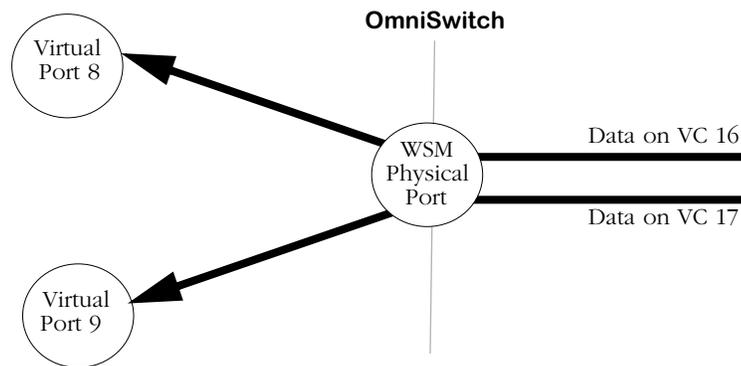
All other frames types from the network are discarded at the physical port level.

Frames coming from the switch to the Frame Relay network are optionally translated if they are a non-Ethernet frame (e.g., FDDI and Token Ring) for a Bridged VLAN. In this case, the frame is translated to an Ethernet frame before it is sent to the Frame Relay interface. Frames from non-Ethernet interfaces can also be sent as is without translation. This translation, which is called Default Bridging Mode, can be configured at the service or port level. In addition, BPDU and Routed frames (IP, ARP, InARP, IPX) are accepted.

Bridging Services

All Frame Relay Virtual Circuits (VCs) belong to a service, whether it be a Bridge, Router, or Trunk service. By default, a virtual circuit belongs to a bridge service. No configuration is necessary for a VC to support bridging on Group 1. However, configuration is necessary for a VC to support Frame Relay Routing, Trunking, or Bridging on a Group other than Group 1.

For bridging there is a one-to-one map between Frame Relay virtual circuits and switch virtual ports. When data is received from a virtual circuit at the physical port level it automatically maps to the corresponding virtual port. For example, if Frame Relay virtual circuit 16 maps to virtual port 8, then all incoming data on this circuit would be incoming data on switch virtual port 8. And if virtual circuit 17 maps to virtual port 9, then all incoming data would be on virtual port 9.



One-to-One Mapping Between Virtual Ports and Virtual Circuits

Frame Relay bridging uses standard Spanning Tree as defined in 802.1d. Typically, one bridge port within the WAN will act as the designated root bridge (and may be the actual root bridge) and maintain a single path through the Frame Relay network. To avoid duplication and loops, some paths will not be allowed.

As far as Spanning Tree is concerned, the virtual ports that map off a Frame Relay physical port are LAN ports. Each port will come up as default bridging on VLAN 1.

A unique aspect of Frame Relay bridging is that MAC addresses must be learned for each DLCI and for each virtual port. So, although the virtual circuits map directly to virtual ports, the bridge must still learn their MAC addresses separately. Also, Frame Relay BPDUs do not have MAC addresses.

One of the disadvantages of bridging in Frame Relay is that broadcasts must be sent across all virtual circuits that are associated with a given physical port for a given group. This requirement can create duplication across the Frame Relay network. At the extreme, on a full T1 line with 96 virtual circuits defined, 96 copies of each broadcast would have to be sent for the same Group. When using access rates at the higher end of the Frame Relay spectrum, you could separate virtual circuits into separate Groups to decrease the size of each broadcast domain. Or, you could use a Routing (IP or IPX) or Trunking configuration to more efficiently manage the data flow.

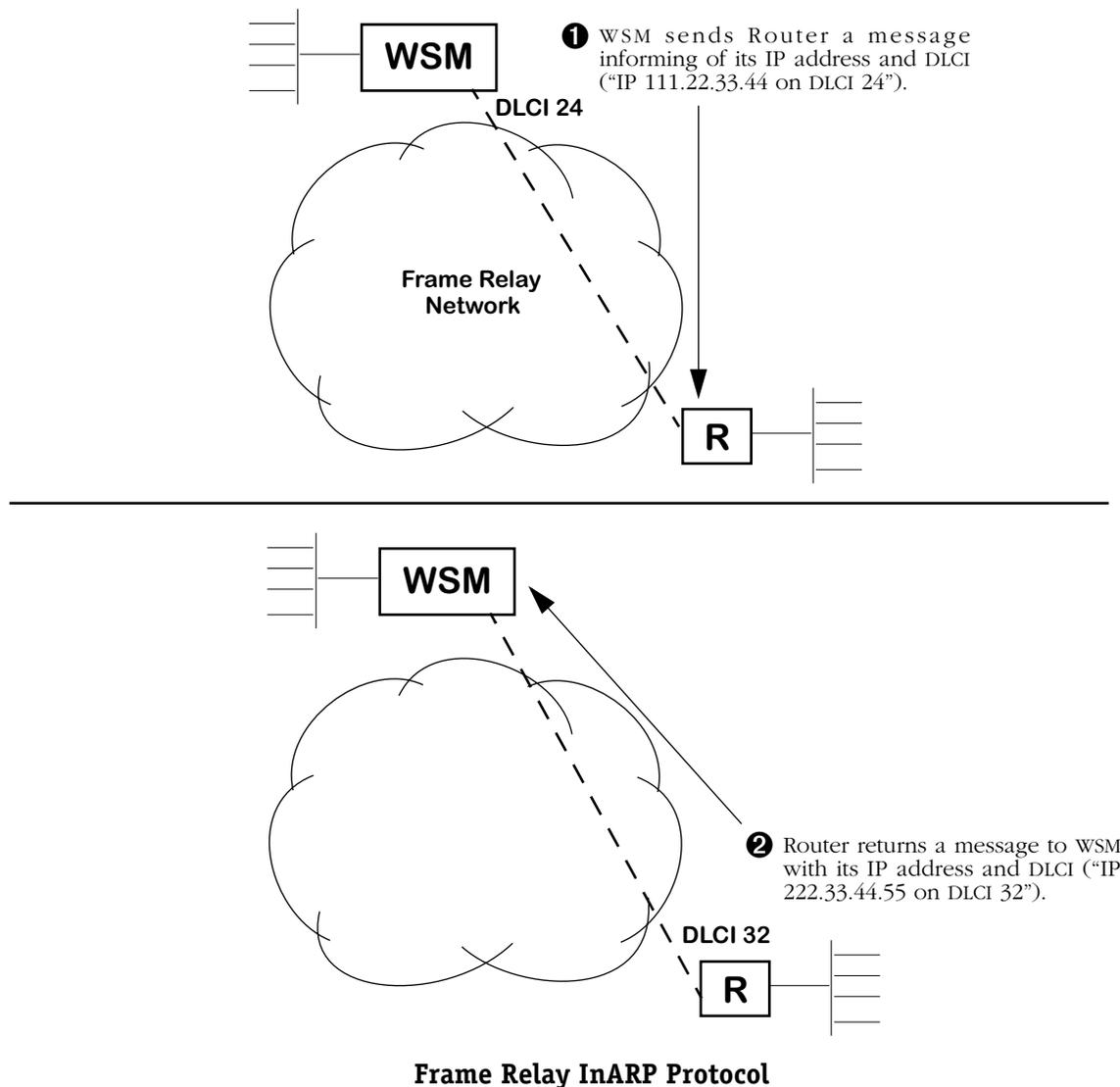
The configuration of bridging services is described in *Configuring a Bridging Service* on page 49-54.

Frame Relay IP Routing

Frame Relay routing is different than standard LAN IP Routing. In normal LAN IP Routing MAC addresses are used as source and destination addresses. In Frame Relay IP Routing, no MAC addresses are included in a routed frame. In fact, the only address in a routed Frame Relay frame is the DLCI, or virtual circuit identifier. The DLCI is the main identifier for source and destination addresses.

Because Frame Relay uses 10-bit DLCIs as the main addressing units, routed Frame Relay frames require less overhead than LAN IP frames, which use LAN standard 48-bit addresses. However, due to the nature of DLCIs on a WAN, Frame Relay routing requires a special version of the IP protocol. The DLCI for a single VC may or may not be different on both sides of a Frame Relay connection. That's why Frame Relay uses the Inverse Address Resolution Protocol (InARP) to resolve DLCI issues and to automatically learn the IP addresses of remote routers.

The InARP protocol ensures that before any data passes between two Frame Relay routers, those routers notify each other of their IP addresses and associated DLCIs. So, the first communication over a routed Frame Relay network is normally initiated by InARP.

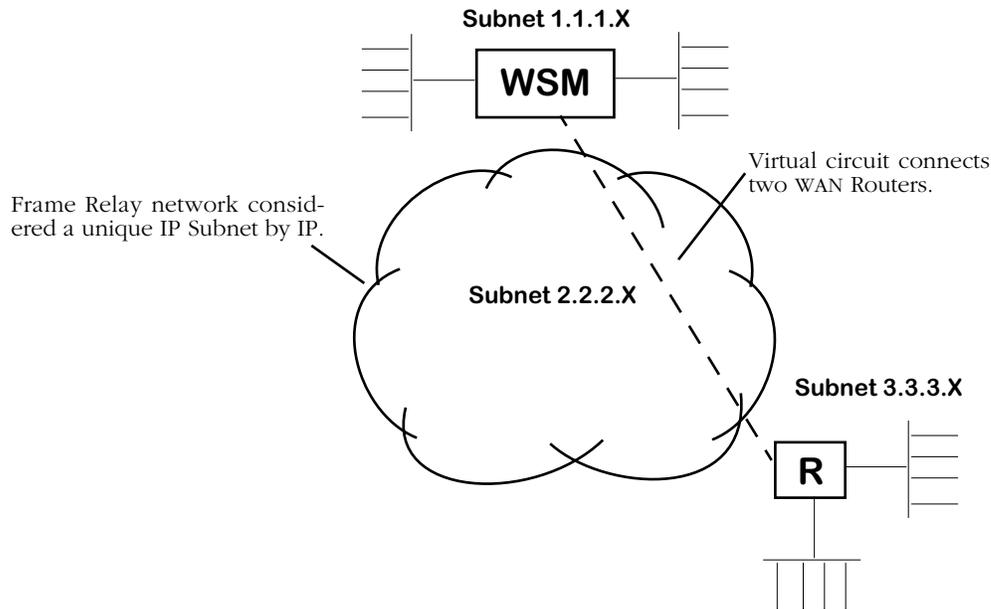


Frame Relay IP Routing

An InARP message is sent between the two routers indicating their IP addresses and associated VC. Once they know each other's IP address and the DLCI of the VC on each end of the link (the same VC may have a different DLCIs on each end), then they can begin normal routing of RIP frames, etc.

The Frame Relay Subnet and "Split Horizon"

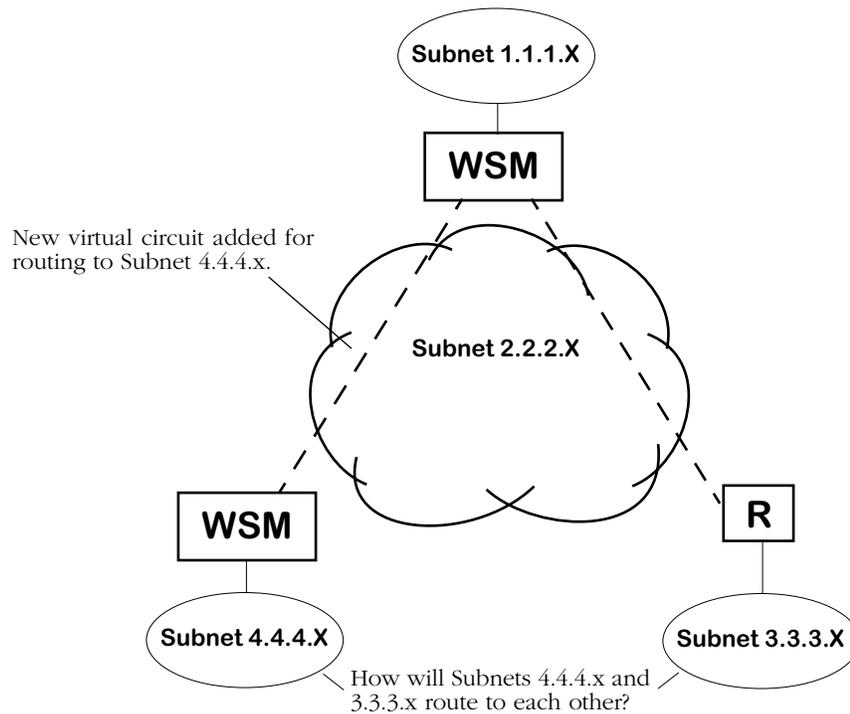
The IP protocol must account for the Frame Relay network in making routing decisions. After all, the WAN network is more than just a single cable, or even several cables, attaching two routers. The solution is to assign the Frame Relay network a unique IP subnet.



Frame Relay Network Is an IP SubNet

In the configuration shown above, one virtual circuit connects the WSM router on IP Subnet 1.1.1.x and the other router on IP Subnet 3.3.3.x. The Frame Relay network, for routing purposes, is considered to be IP Subnet 2.2.2.x. Routing decisions are straightforward in this setup. But if another Router and another IP Subnet were added, a special routing technique must be devised.

If an additional Router and Subnet were added to the network and a new VC was added to connect the new location, then much of the WAN routing load would fall on the WSM attached to Subnet 1.1.1.x.



Adding A New Router Raises New Questions

The new WSM attached to Subnet 4.4.4.x connects to the WAN through the addition of a new virtual circuit connecting directly to the WSM attached to Subnet 1.1.1.x. However, for the new WSM to route to Subnet 3.3.3.x it must go through the WSM router attached to Subnet 1.1.1.x. This is okay for the initial routed path decision. But IP will try to find the most efficient route between Subnet 4.4.4.x and 3.3.3.x. Unfortunately the most efficient route—which would be a direct path between the two routers—is not possible because no WAN link exists between the two.

Frame Relay routing allows the new Subnet, 4.4.4.x, and Subnet 3.3.3.x to route through the WSM router attached to Subnet 1.1.1.x. Normal IP would have a problem with this solution because it does not allow “backtracking” through IP Subnets, which is exactly what must be done in this case. Routed frames actually pass through the Frame Relay Network Subnet 2.2.2.x twice—once to get the WSM Router attached to Subnet 1.1.1.x and another time to get to the Router attached to either Subnet 4.4.4.x or 3.3.3.x.

Standard routing uses a technique called “split horizon” that prevent loops through the same Subnet from occurring. *Frame Relay enhances split horizon to account for the nature of virtual circuits.* Loops through a LAN Subnet are inefficient, but Frame Relay routing makes allowances to compensate for the fact that a WAN does not enjoy the same flexibility with router connections as a LAN.

Note

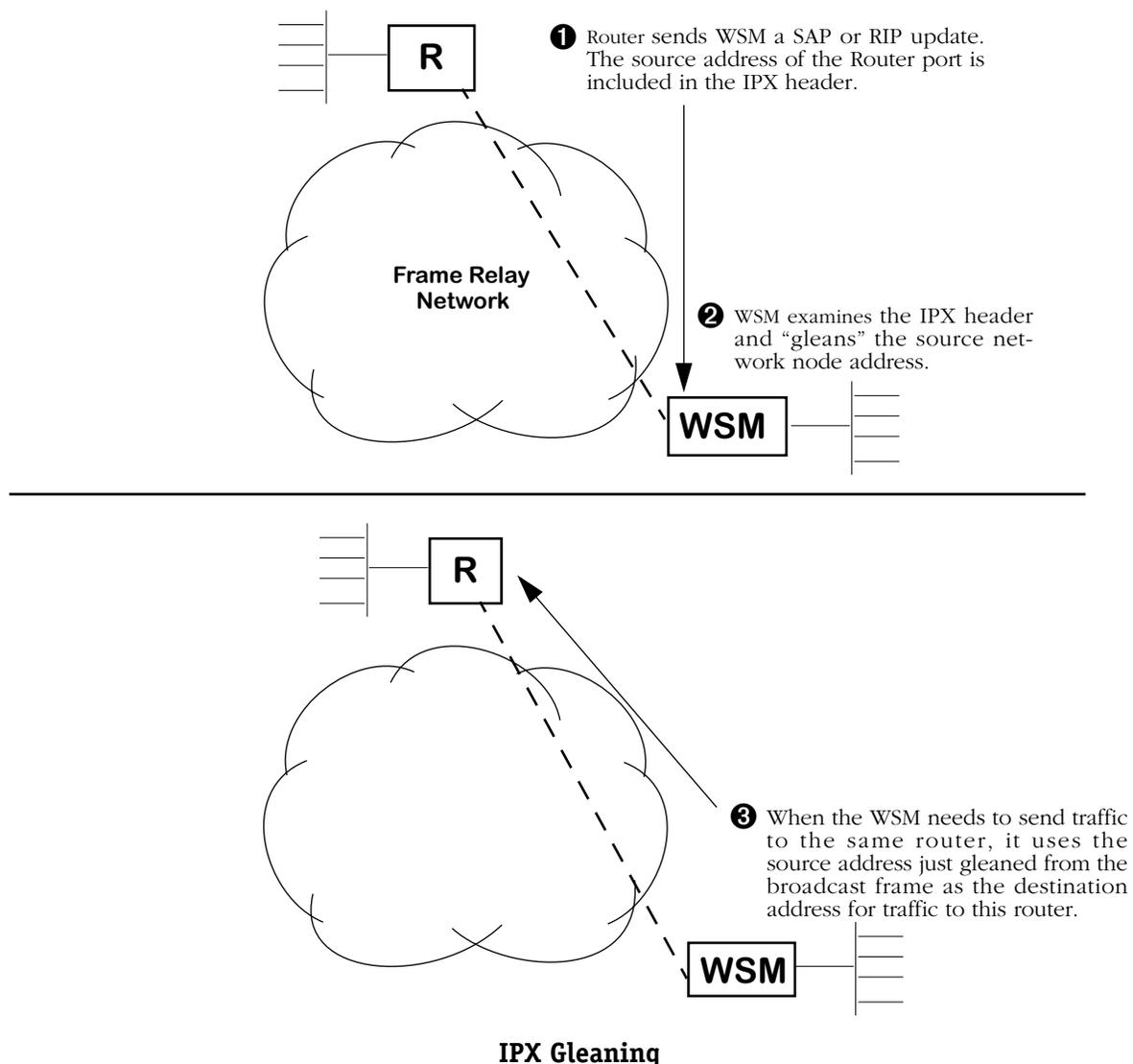
Backtracking in InARP is allowed only through the IP Subnet defined for the Frame Relay network.

The configuration of WSM routing services is described in *Configuring a WAN Routing Service* on page 49-56.

Frame Relay IPX Routing

Frame Relay IPX and IP routing differ in the way they determine the address of a router at each end of a virtual circuit. Instead of using Inverse ARP, IPX uses a process called “gleaning” to determine routing information. In gleaning, the IPX routing protocol on one end of a virtual circuit obtains the network node number for the router at other end of the virtual circuit.

A WSM or router continuously receives RIP and SAP updates on a given virtual circuit. When it receives the first such broadcast, the IPX process looks at, or gleans, the source address from the frame’s IPX header. When the router needs to send traffic on that router later, it uses the source address it just obtained as the destination address for that router. The following diagram illustrates IPX Gleaning.



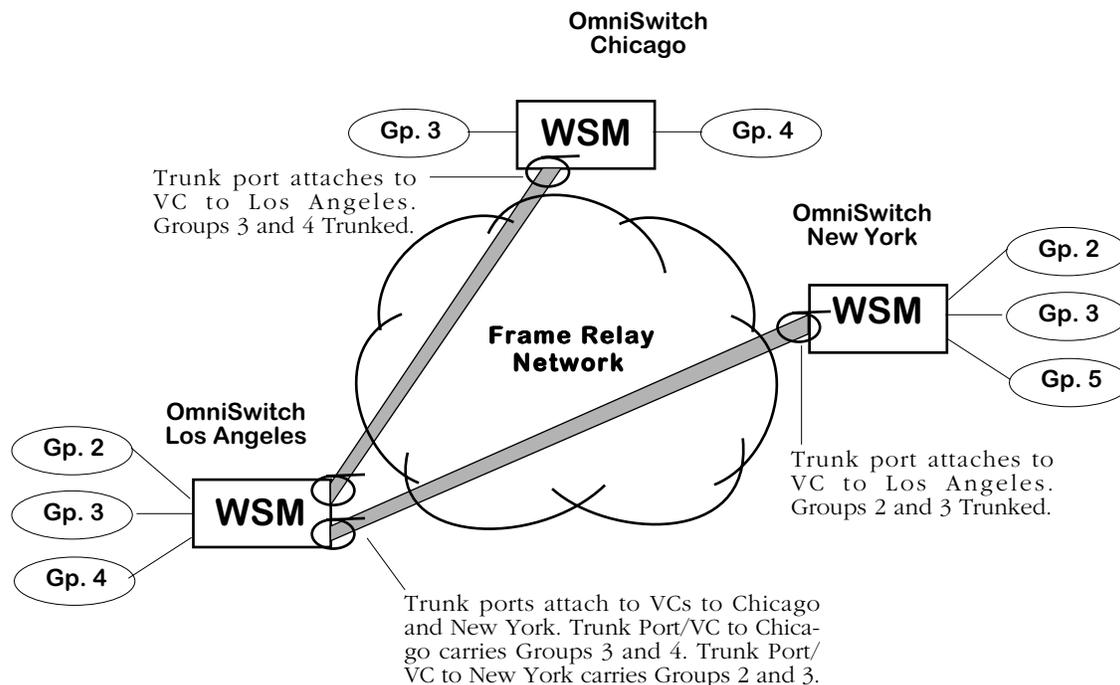
Not all Routers support IPX gleaning. If you need to interoperate with a Router that does not support gleaning, then you may need to statically map addresses on that Router.

The configuration of WSM routing services is described in *Configuring a WAN Routing Service* on page 49-56.

Trunking

A trunking service must be set up for each virtual circuit that will support trunking. When trunking is set up, you specify the slot, port, DLCI, and Groups that are going to be trunked over the virtual circuit.

The illustration below shows a sample trunking configuration. The WSM in Los Angeles has two trunk ports, one to Chicago and one to New York.



Trunk Ports and Virtual Circuits Over Frame Relay Network

Frame Relay virtual ports are mapped one-to-one to virtual circuits, so each of these trunk ports is connected to a virtual circuit. When setting up Trunking you need to be aware of your virtual circuit configurations, their DLCIs, and their termination points. Configuring a Trunking Service is described in *Configuring a Trunking Service* on page 49-59.

Note

No standard exists for trunking Groups or VLANs over Frame Relay. Therefore, you must configure Trunking using Alcatel's method.

The Frame Relay Software Menu

User interface commands for Frame Relay are on a separate menu that you can access through the **fr** command. The Frame Relay menu is a sub-menu of the **Interface/WAN** menu. Typing **fr** at any system prompt displays the following menu:

Command	Frame-Relay Menu
frstatus	Status of entire chassis, slot, port, and DLCI (e.g., 4/1/32).
frview	View a given slot, port, or DLCI (e.g., 4/1/32).
frmodify	Modify a given slot, port, or DLCI (e.g., 4/1/32).
frdelete	Delete a given port or DLCI (e.g., 4/1/32).
fradd	Add a DLCI with slot, port, DLCI (e.g., 4/1/32)
Main	File Summary VLAN Networking
Interface	Security System Services Help

You can start any of the commands by typing just the first three (3) letters of the command name. For example, to use the **frview** command you could type only **frv**.

The following sections describe the use of commands on the Frame Relay menu.

Setting Configuration Parameters

When you plug in a WSM board it is automatically configured with default settings. The WSM board will default the WAN port protocol to frame relay for WSM serial ports, T1 and E1 ports. Commands generic to the WSM module can be found in Chapter 49.

By default the WSM frame relay software uses ANSI T1.617 Annex D for the Data Link Control Management Interface (DLCMI) and uses a Committed Information Rate (CIR) of 0. In addition, the access rate defaults to 64 Kbps for RS-232 cables and to 2 Mbps for all other cable types. You can change these settings as well as several other settings with the **frmodify** command.

You have a choice of modifying parameters at the port or DLCI (virtual circuit) level. You receive different configuration choices depending upon which level you choose. The two sections below describe both ways to use the **frmodify** command.

Modifying a Port

To modify a port, enter the following command

```
frmodify <slot>/<port>
```

where **<slot>** is the slot number where the WSM board is located, and **<port>** is the port number on the WSM board that you want to modify. For example, if you wanted to modify port number 1 on the WSM board in switch slot 3, you would enter

```
frmodify 3/1
```

or

```
frm 3/1
```

Setting Configuration Parameters

A screen similar to the following displays:

Modifying Frame Relay port for Slot 2, Port 1.

- 1) Description..... =
 {Enter Up to 30 Characters}
- 2) Administrative Status = Up
 {(U)p, (D)own}
- 3) DLCMI Type = ANSI T1.617 Annex D
 {(L)MI Rev. 1.0, T1.617 Annex (D), Q.933 Annex (A), (N)one }
 31) LMI Procedure Type = Bidirectional
 { (B)idirectional, (U)ser, (N)etwork }
- 4) Polling Interval T391/nT1 = 10
 {1 through 255 seconds}
 41) Poll Verification Interval T392 (seconds). = 15
 {1 through 255 seconds}
- 5) Full Status Interval N391/nN1 = 6
 {1 through 10}
- 6) Error Threshold N392/nN2 = 3
 {1 through 10}
 61) Network Error Threshold N392 = 3
 {1 through 10}
- 7) Monitored Events Counter N393/nN3 = 4
 {1 through 10}
 71) Network Monitored Events Counter N393 = 4
 {1 through 10}
- 8) Default Bridging Group..... = 1
 {1-65535}
- 9) Default Frame Relay Bridging Mode..... = Bridge All
 {1=Bridge All, 2=Ethernet only,
 (AN) Bridge All No FCS, (EN) Ethernet Only No FCS}
- 10) Default Routing Group..... = 0
 {1-65535}
- 11) Default Compression Admin Status = Enabled
 {(E)nable, (D)isable}
- 12) Default Compression PRetry Time = 3
 {1-10}
- 13) Default Compression PRetry Count = 10
 {3-255}

To change a value, enter the corresponding number, an '=', and the new value. For example to set a new description, use

: 2=My new Description

To clear an entry specify the value as '.' as in

: 2=.

When complete enter "save" to save all changes, or cancel or Ctrl-C to cancel all changes. Enter ? to view the new configuration.

(save/quit/cancel)

:

You make changes by entering the line number for the option you want to change, an equal sign (=), and then the value for the new parameter. When you are done entering all new values, type **save** at the colon prompt (:) and all new parameters will be saved. The following sections describe the options you can alter through this menu.

◆ **Caution** ◆

Several of the parameters in this menu (**Polling Interval, Full Status Interval, Error Threshold, and Monitored Events Counter**) are set to Frame Relay defaults and do not need to be changed except in rare cases. These options should only be modified by experienced Frame Relay network administrators. Changes to these options will probably also require coordination with the service provider.

In addition, the **DLCMI Type** option must be entered correctly or the WSM will not be able to communicate with the Frame Relay network. The WSM board is self-configuring in many ways, but it cannot compensate for an incorrect DLCMI Type.

1) Description

Enter a description for this port. The description can be up to 30 characters long.

2) Administrative Status

This option enables or disables the port. If set to **UP**, then the port has been enabled and can transmit data as long as its Operational Status is also UP. If set to **DN**, then the port will not pass data even if its physical connection is good.

3) DLCMI Type

This field specifies the Data Link Control Management Interface (DLCMI) that you want to use for Frame Relay and virtual circuit management. You have three choices for this protocol, each of which corresponds to an existing widely-used protocol. The letters used in the **frmodify** screen correspond to the following DLCMIs:

- L** LMI rev. 1.0 (LMI)
- D** ANSI T1.617 Annex D
- A** CCITT-ITU-T Q.933 Annex A
- N** None

Enter your choice by specifying the letter corresponding to your choice.

◆ **Important Note** ◆

The DLCMI protocol that you enter must match that used by your service provider. Entering an incorrect DLCMI protocol may cause the port to not operate. The WSM needs to know the protocol you are using to establish communication with the Frame Relay network.

31) LMI Procedure Type

This field specifies the Local Management Interface (LMI) procedure type for this Frame Relay port. You have three choices for the LMI procedure type. The letters used in the **frmodify** screen correspond to the following:

- B** Bidirectional
- U** User (the default)
- N** Network

Enter your choice by specifying the letter corresponding to your choice.

◆ Important Note ◆

To configure a Frame Relay (FR)/ATM Internetworking Function (IWF) service or network, you *must* set the LMI Procedure Type to **Network** or **Bidirectional**. For more information on FR/ATM IWF services and networks, see Chapter 39, “Frame Relay/ATM Internetworking.”

4) Polling Interval T391/nT1

This interval is the time in seconds between WSM port polls of the Frame Relay network. The WSM port polls the network by sending STATUS ENQUIRY messages, which check the link integrity of the Frame Relay connection. By default this interval is set to 10 seconds, but you can increase or decrease it. The default is the standard Frame Relay value. Increasing the polling interval lightens the data load on the port, as it does not have to poll as often. The interval may range from 1 second to 4 minutes and 15 seconds (255 seconds).

◆ Important Note ◆

This option should only be modified by experienced Frame Relay network administrators.

5) Full Status Interval N391/nN1

This interval is the time in seconds between FULL STATUS ENQUIRIES initiated by the WSM to the Frame Relay network. The Frame Relay network returns a list of all virtual circuits and whether they are active or inactive. You can set this interval from 1 to 10 seconds. By default, this interval is set to 6 seconds, which is the standard Frame Relay default value.

◆ Important Note ◆

This option should only be modified by experienced Frame Relay network administrators.

6) Error Threshold N392/nN2

The number of DLCMI protocol errors that will be tolerated before determining the Frame Relay line is down and all associated virtual circuits are inactive. These errors may include timeouts from STATUS ENQUIRY polls and invalid STATUS messages returned from the Frame Relay network. By default, this threshold is set to 3, which is the standard Frame Relay default value.

◆ Important Note ◆

This option should only be modified by experienced Frame Relay network administrators.

7) Monitored Events Counter N393/nN3

The number of status polling intervals over which the **Error Threshold** is counted. This value should be greater than or equal to the **Error Threshold**. If the station received the number of errors specified in **Error Threshold** within the number of polling intervals specified for the **Monitored Events Counter**, then the Frame Relay line is considered down and all associated virtual circuits are considered inactive. By default, this counter is set to 4, which is the standard Frame Relay default value.

◆ Important Note ◆

This option should only be modified by experienced Frame Relay network administrators.

8) Default Bridging Group

The default Group for bridging any virtual circuits (user-configured or learned from the Frame Relay network) that are not specifically assigned to a Bridging service. If you set this value to 0, then virtual circuits will not perform bridging unless assigned to a bridging service. By default, the Default Bridging Group is set to 1. By entering a value here you can change the default for this port.

◆ Important Note ◆

The **Default Bridging Group** only applies to user-side (i.e., the LMI Procedure Type has been set to **User**) Frame Relay ports.

9) Default Frame-Relay Bridging Mode

This field sets the default translation option for this port. When set to **All**, no translation is performed on frames before they are sent out to the Frame Relay network; frames are sent as is. When set to **Eth-only**, non-Ethernet frames are first translated to the default Ethernet frame format for this port before they are sent out to the Frame Relay network. Any MAC translations configured through the Switch menu are valid.

◆ Important Note ◆

The **Default Frame-Relay Bridging Mode** only applies to user-side (i.e., the LMI Procedure Type has been set to **User**) Frame Relay ports.

10) Default Routing Group

The default Group for bridging any virtual circuits (user-configured or learned from the Frame Relay network) that are not specifically assigned to a Routing service. If you set this value to 0 (the default value), then virtual circuits will not perform Routing unless specifically assigned to a Routing service.

This option is intended to simplify Routing configuration if you do not need to route many Groups over a Frame Relay physical port. The WSM learns about Data virtual circuits from the Frame Relay network. To enable routing on each of these learned virtual circuits, you would have to set up each circuit individually. However, if you already know the Routing Group for your VCs, then you can specify it here and all VCs will be placed in that Group with an extra configuration on your part. Note that you still need to set up a Frame Relay Routing Group through the **crgp** command. See *Configuring a WAN Routing Service* on page 49-56 for more information.

◆ Important Note ◆

The **Default Routing Group** only applies to user-side (i.e., the LMI Procedure Type has been set to **User**) Frame Relay ports.

11) Default Compression Admin Status

This option indicates whether compression negotiation is enabled or disabled for virtual circuits that are learned from the Frame Relay network. Configured virtual circuits are enabled for compression through the **fradd** or **frmodify** (virtual circuit level) commands. The compression negotiation status that you set up for a specific virtual circuit overrides the status you enter here for the physical port.

12) Default Compression PRetry Time

This option sets the number of seconds between compression negotiation messages. If compression negotiation is enabled, the WSM will send compression negotiation messages as many times as you indicate in the Default Compression PRetry Count. The time between these tries is indicated in this field. The number of seconds between retries may range between 1 and 10 seconds. The default is 3 seconds. This default can be by using the **frmodify** command on an individual virtual circuit.

◆ Important Note ◆

The **Default Compression PRetry Time** should only be modified by experienced Frame Relay network administrators. In addition, it should match the setting for the remote OmniSwitch or Bridge/Router.

13) Default Compression PRetry Count

This option sets the total number of compression negotiation messages that will be sent before giving up and not running compression. You enter the time between these retries in the Default Compression PRetry Time field. The number of retries can range from 3 to 255. The default is 10. This default can be by using the **frmodify** command on an individual virtual circuit.

◆ Important Note ◆

The **Default Compression PRetry Time** should only be modified by experienced Frame Relay network administrators. In addition, it should match the setting for the remote switch or Bridge/Router.

Modifying a Virtual Circuit

To modify a virtual circuit, enter the following command:

```
frmodify <slot>/<port>/<DLCI>
```

where **<slot>** is the slot number where the WSM board is located, **<port>** is the port number on the WSM board, and **<DLCI>** is the number used to identify the virtual circuit that you want to modify. For example, if you wanted to modify DLCI 17 on Port number 1 of the WSM board in slot 3, you would enter

```
frmodify 3/1/17
```

or

```
frm 3/1/17
```

A screen similar to the following displays:

Modifying Frame Relay DLCI for Slot 3, Port 1, DLCI 17.

- 1) Administrative State = U
 {(U)p, (D)own}
- 2) Committed Information Rate (CIR) in BPS = 0
 {0 through line speed in BPS}
- 3) Committed Burst Rate(Bc) = 0
 {0 through positive number in bits}
- 4) Excess Burst Rate(Be) = 0
 {0 through positive number in bits}
- 5) Compression Administrative Status = Enabled
 {(E)nabled, (D)isabled}
- 6) Compression PRetry Time = 3
 {1..10}
- 7) Compression PRetry Count = 10
 {3..255}

To change a value, enter the corresponding number, an '=', and the new value. For example to set a new DLCI Active/Inactive Traps, use
: 5=d

When complete enter "save" to save all changes, or cancel or Ctrl-C to cancel all changes. Enter ? to view the new configuration.

You make changes by entering the line number for the option you want to change, an equal sign (=), and then the value for the new parameter. When you are done entering all new values, type **save** at the colon prompt (:) and all new parameters will be saved. The following sections describe the options you can alter through this menu.

Administrative State

This option enables and disables the virtual circuit you are modifying. Setting this option to **Up** enables the circuit and allows data to be sent or received on it as long as the Operational Status is also Up. Setting this option to **Down** disables the circuit; no data can be sent on the circuit. This may be a good option to use when preconfiguring a virtual circuit in advance of live network operation.

Committed Information Rate (CIR)

This field sets the Committed Information Rate (CIR) for this virtual circuit. See *Congestion Control* on page 49-8 for further information on the CIR.

◆ Important Note ◆

The **CIR** that you enter must match that used by your service provider. This option should only be modified by experienced Frame Relay network administrators.

Committed Burst Size (Bc)

The Committed Burst Size (BC) is the amount of data that the network will guarantee to transfer under normal conditions. See *Congestion Control* on page 49-8 for further information.

◆ Important Note ◆

The **Committed Burst Rate** that you enter must match that used by your service provider. This option should only be modified by experienced Frame Relay network administrators.

Excess Burst Size (Be)

The Excess Burst Size (Be) is the amount of data over-and-above the Committed Burst Size (BC) that the network will transmit as long as excess bandwidth is available. See *Congestion Control* on page 49-8 for further information.

◆ Important Note ◆

The **Excess Burst Rate** that you enter must match that used by your service provider. This option should only be modified by experienced Frame Relay network administrators.

Compression Administrative State

This field enables and disables compression negotiation for this virtual circuit. If set to enable, then the WSM will query the Bridge/Router on the other end of the Frame Relay link as to whether it supports compression. Compressed data will be sent only when the other Bridge/Router also supports compression. If the Bridge/Router on the other end is an OmniSwitch, then data would be sent compressed as long as you set the Compression Administrative State to Enabled.

Disabling Compression Administrative State means that data will not be sent compressed even if the other Bridge/Router supports compression. Data compression is always negotiated before it is activated.

Compression PRetry Time

This option sets the number of seconds between compression negotiation messages on this virtual circuit. If compression negotiation is enabled, the WSM will send compression negotiation messages as many times as you indicate in the Compression PRetry Count. The time between these tries is indicated in this field. The number of seconds between retries may range between 1 and 10 seconds. The default is 3 seconds. The value you enter for this field overrides the **Default Compression PRetry Time** set up for the physical port with which this virtual circuit is associated.

◆ Important Note ◆

The **Compression PRetry Time** that should only be modified by experienced Frame Relay network administrators. In addition, it should match the setting for the remote OmniSwitch or Bridge/Router.

Compression PRetry Count

This option sets the total number of compression negotiation messages that will be sent before giving up and not running compression on this virtual circuit. You enter the time between these retries in the Compression PRetry Time field. The number of retries can range from 3 to 255. The default is 10. The value you enter for this field overrides the **Default Compression PRetry Count** set up for the physical port with which this virtual circuit is associated.

◆ Important Note ◆

The **Compression PRetry Count** that should only be modified by experienced Frame Relay network administrators. In addition, it should match the setting for the remote switch or Bridge/Router.

Adding a Virtual Circuit

Data virtual circuits and their DLCIs are normally learned through status messages with the Frame Relay network. However, it may be convenient to pre-configure these virtual circuits before connecting to a live network. In such a case you will need to use the **fradd** command to set parameters for the virtual circuit. The information for the virtual circuit will be stored in the WSM database. This method of configuration is different than using the **frmodify** command, which changes virtual circuit parameters after the circuit has been learned from the network or configured through **fradd**.

To set up a data virtual circuit, enter the following command

```
fradd <slot>/<port>/<DLCI>
```

where **<slot>** is the slot number where the WSM board is located, **<port>** is the port number on the WSM board, and **<DLCI>** is the number used to identify the virtual circuit that you want to add. For example, if you wanted to add DLCI 32 on Port number 1 of the WSM board in slot 2, you would enter

```
fradd 2/1/32
```

or

```
fra 2/1/32
```

A screen similar to the following displays:

```
Adding Frame Relay port for Slot: 2, Port: 1 DlcI: 32.
```

- 1) **Administrative State** = **UP**
 {(U)p, (D)own}
- 2) **Committed Information Rate (CIR) in BPS** = **0**
 {0 through line speed in BPS}
- 3) **Committed Burst Rate (Bc) in bits** = **0**
 {0 through positive number in bits}
- 4) **Excess Burst Rate (Be) in bits** = **0**
 {0 through positive number in bits}
- 5) **Compression Administrative Status** = **Enabled**
 {(E)nabled, (D)isabled}
- 6) **Compression PRetry Time** = **3**
 {1..10}
- 7) **Compression PRetry Count** = **10**
 {3..255}

Enter the value for each parameter after the colon prompt (:). An additional field, **DLCI Number**, is displayed if you do not specify a DLCI number in the **fradd** command. The remaining parameters are the same ones used for the **frmodify** command. See *Modifying a Virtual Circuit* on page 49-28 for information on each of these parameters.

When you have entered values in all fields, the following prompt displays

```
Do you want to configure additional DLCIs? {(Y)es, (N)o}
```

Enter a **Y** to set up additional virtual circuits or enter **N** to exit the **fradd** command. If you enter **Y**, then you are prompted for all virtual circuit parameters again.

Viewing Configuration Parameters for the WSM

You can view all current parameters for a WSM port or an individual virtual circuit using the **frview** command. These parameters will be either the default parameters or parameters you modified using the **frmodify** command or network management software.

You have a choice of viewing parameters at the chassis, port or DLCI (virtual circuit) level. You receive different configuration choices depending upon which level you choose. The sections below describe both ways to use the **frview** command.

Viewing Parameters for all WSMs in the Chassis

To view port parameters for all WSM boards in a chassis, enter the following command

```
frview
```

```
or
```

```
frv
```

A screen similar to following displays:

Frame Relay Configuration for Chassis:

Slot/Port	Intf Type	Speed BPS	Clocking	Default Bridging Grp	Default Routing Grp
3/1	V35DTE	0	External	1	0
3/2	V35DCE	0	External	1	0
3/3	*NONE*	0	External	1	0
3/4	*NONE*	0	External	1	0

Only ports configured as frame relay (see the **wpm** command in Chapter 49) will be displayed in this screen. This screen lists all the current values for the listed parameters. These parameters are the same ones set through the **frmodify** command. For detailed information on these values, see *Modifying a Port* on page 49-21. For detailed information on the **Intf Type** column, see *Intf Type* on page 49-38.

Viewing Port Parameters

To view port parameters, enter the following command

```
frview <slot>/<port>
```

where **<slot>** is the slot number where the WSM board is located, and **<port>** is the port number on the WSM board on which you want to view information. For example, if you wanted to view configuration parameters for Port number 1 on the WSM board in slot 2, you would enter

```
frview 2/1  
or  
frv 2/1
```

A screen similar to following displays:

Frame Relay port for Slot 2, Port 1.

```
1) Description..... = Port1
2) Administrative Status ..... = UP
3) DLCMI Type..... = ANSI T1.617 Annex D
   31) DLCMI Type ..... = User
4) Poll Verification Interval T392 (seconds ) ..... = 15
5) Full Status Interval N391/nN1 ..... = 6
6) Error Threshold N392/nN2 ..... = 3
7) Monitored Events Counter N393 ..... = 4

8) Default Bridging Group ..... = 1
9) Default Frame-Relay Bridging Mode ..... = Bridge All
10) Default Routing Group ..... = 0
11) Default Compression Admin Status..... = Enabled
12) Default Compression PRetry Time ..... = 3
13) Default Compression PRetry Count ..... = 10
```

This screen lists all the current values for the listed parameters. These parameters are the same ones set through the **frmodify** command. For detailed information on these values, see *Modifying a Port* on page 49-21.

Viewing Virtual Circuit Parameters

To view virtual circuit parameters, enter the following command

```
frview <slot>/<port>/<DLCI>
```

where **<slot>** is the slot number where the WSM board is located, **<port>** is the port number on the WSM board, and **<DLCI>** is the number used to identify the virtual circuit that you want to view. For example, if you wanted to view configuration parameters for DLCI 17 on Port number 1 of the WSM board in switch slot 3, you would enter

```
frview 3/1/17
```

or

```
frv 3/1/17
```

A screen similar to the following displays:

Frame Relay DLCI for Slot 3, Port 1, DLCI 17.

```
1) Administrative State ..... = UP
2) Committed Information Rate (CIR) in BPS ..... = 16000
3) Committed Burst Rate(Bc) in bits ..... = 16000
4) Excess Burst Rate(Be) in bits..... = 40000
5) Compression Administrative Status..... = Enabled
6) Compression PRetry Time ..... = 3
7) Compression PRetry Count ..... = 10
```

This screen lists all the current values for the listed parameters. These parameters are the same ones set through the **frmodify** command. For detailed information on these values, see *Modifying a Virtual Circuit* on page 49-28.

Deleting Ports and Virtual Circuits

You can delete a WSM port or virtual circuit. When you delete a port or virtual circuit all configuration parameters revert back to default settings. You can use the **frdelete** command to delete:

- a single virtual circuit, or
- a port and all of its associated virtual circuits

The **frdelete** command always requires you to indicate at least a slot and port number. You cannot, for example, enter **frdelete** along with no slot and port parameters.

Deleting a Virtual Circuit

You can delete a single virtual circuit as long as you know its DLCI number and the WSM port where it exists. Deleting a virtual circuit resets the configuration parameters on that circuit to configuration and bridging defaults. By default, a virtual circuit is assigned to Group 1.

Virtual circuits are also not actually “deleted” when you use **frdelete**. The Frame Relay network stills sees them as active or inactive. If the virtual circuit was configured (management circuit or a circuit configured through **frmodify**), then the database record for the circuit is deleted; the VC is still present as long as it was present before you deleted it. If the virtual circuit is learned (through status updates from the Frame Relay network), then the database record for the circuit is deleted, but the circuit is still present.

To delete a virtual circuit, enter the following command

```
frdelete <slot>/<port>/<DLCI>
```

where **<slot>** is the OmniSwitch slot number for the WSM board, **<port>** is the port to which the virtual circuit maps, and **<DLCI>** is the identification number for the virtual circuit. For example, if you wanted to delete virtual circuit 32 on Port 1 of the WSM board in slot 2, then would enter:

```
frdelete 2/1/32
```

or

```
frd 2/1/32
```

This system returns the following prompt to confirm the deletion:

```
This will delete Slot 2, Port 1, DLCI 32. Continue? {(Y)es, (N)o} (N)
```

Enter a **Y** to confirm the deletion or press **<Enter>** to cancel the deletion.

Deleting a Port and Its Virtual Circuits

You can delete a port as well as all of its associated virtual circuits. Deleting a port means that all configuration parameters on the port and all learned virtual circuits will revert back to default settings. The port is not logically deleted, and can still be reconfigured after the delete. To truly “delete” a port you must disconnect its cable or set its Administrative Status to Disable.

To delete a virtual circuit, enter the following command:

```
frdelete <slot>/<port>
```

where **<slot>** is the OmniSwitch slot number for the WSM board, **<port>** is the port number on the WSM board that you want to delete. For example, if you wanted to delete Port 1 of the WSM board in slot 2, then would enter:

```
frdelete 2/1
```

or

```
frd 2/1
```

This system returns the following prompt to confirm the deletion:

```
This will delete Slot 2, Port 1 and its DLCIs. Continue? {(Y)es, (N)o} (N)
```

Enter a **Y** to confirm the deletion or press **<Enter>** to cancel the deletion.

Obtaining Status and Statistical Information

You can obtain general and detailed Frame Relay statistical information on all WSM boards in the switch, a single WSM board, individual ports, and individual virtual circuits. The **frstatus** command is used to provide this information. This information includes types of physical interface, access rate of the Frame Relay line, and errors. In addition, the **frstatus** command can display the number of frames received and transmitted categorized by frame type (i.e., compressed/uncompressed, Ethernet, IP, IPX, BPDU).

Information on All Boards in a Switch

To obtain status information on all WSM boards in a switch, you enter the **frstatus** command without any parameters as follows:

```
frstatus
```

This command displays a screen similar to the following:

```

Frame Relay Status for the Chassis:
      Admin/      Intf      Speed      VC's
      Oper      Status      Type      BPS      Clocking      Active/
      Status      Type      BPS      Clocking      Inactive
=====
 4/1  UP/UP  V35DCE  2048000  Split      2/0
 4/2  DN/DN  *NONE*  EXT CLK  External   0/0
 4/3  UP/DN  *NONE*  EXT CLK  External   0/0
 4/4  UP/UP  232DCE   56000   Internal  19/1

```

Only ports configured as frame relay (see the **wpm** command in Chapter 49) will be displayed in this screen. Each row in the table corresponds to a physical port on a WSM board in the switch. The following sections describe the columns shown in this table:

Slot/Port

The first number in this column is the slot in the switch where this WSM is installed. The second number is the port number on the WSM.

Admin/Oper Status

This column shows the Administrative and Operational Status of this WSM port. The status indicator before the slash refers to the Administrative Status. If **UP**, then the port has been enabled and can transmit data as long as its Operational Status is also **UP**. If the Administrative Status is **DN**, then the port will not pass data even if its physical connection is good.

The status indicator after the slash refers to the Operational Status. If **UP**, then the port is capable of passing data as long as it has been logically enabled at the Administrative level. If **DN**, then the port cannot pass data because of a problem in the physical connection (e.g., cable disconnected, WSM could not detect cable type) or because the port is Administratively Down.

Intf Type

This column indicates the physical cable type connected to this port. This cable type is automatically sensed by the WSM hardware. This column indicates the cable type and whether it is DCE or DTE. The following values may display in this column

- **V35DTE** (V.35 DTE cable)
- **V35DCE** (V.35 DCE cable)
- **232DTE** (RS-232 DTE cable)
- **232DCE** (RS-232 DCE cable)
- **X21DTE** (X.21 DTE cable)
- **X21DCE** (X.21 DCE cable)
- **530DTE** (RS-530 or RS-449 EIA DTE cable)
- **530DCE** (RS-530 or RS-449 EIA DCE cable)
- **T1** (T1 port)
- **E1** (E1 port)

The WSM sees RS-530 and RS-449 cables the same because they are electrically identical. However, this does not affect the operation of either cable type. Both RS-530 and RS-449 cables are supported. If no cable is connected to a port, then this column will display

NONE

If an error has been detected on the port (e.g., cable type could not be detected), then the following value displays:

ERROR!

Speed BPS

This column indicates the speed, or access rate, between the WSM serial port and DSU or other “physical” DTE device. The speed is expressed in bits per second (bps). This speed is the total available bandwidth on the line connected to this port. Virtual circuits on this port share this bandwidth.

Usually, the WSM port will be a physical DTE device and the speed will be determined by the DSU. In this case, this value will read **EXT CLK**, which means the WSM port gets its clocking from an externally attached DCE device (i.e., DTE cable plugged into WSM port) or no cable is attached. If the WSM port is a physical DCE device (i.e., DCE cable plugged into WSM port), then this value will be the actual clock rate used by the port. The speed on a T1 port will always be 1544000; the speed for an E1 port will always be 2048000.

Clocking

This field indicates the type of clocking used to clock transmit and receive data in and out of the serial port. When the clock is out-of-phase, you receive errors. If this value is set to External, then clocking is controlled by the external DCE (a DSU or other DCE device on the other end of the cable from the WSM port). External clocking is the default option when the WSM is a physical DTE device (i.e., controlled by an external DCE device).

Note

See Chapter 49, “Managing WAN Modules,” for documentation on setting the clocking mode for serial ports, see Chapter 54, “Managing T1 and E1 Ports,” for documentation on setting the clocking mode for T1 and E1 ports, and see Chapter 55, “Managing DS3/E3 Modules,” for documentation on setting the clocking mode for DS3 and E3 ports.

If this value is set to Internal, then clocking is controlled by the internal DCE (the WSM). Internal clocking should only be selected if the WSM is a physical DCE device and you are using an RS-232 cable. Internal clocking is the default when the WSM is a physical DCE device and an RS-232 DCE cable is connected to this port. For T1 and E1 ports, internal clocking is equivalent to local timing.

Note

The Clocking value only makes a difference if the WSM port is a physical DCE port (i.e., DCE cable plugged into the WSM port). If the WSM port is a physical DTE port, then Clocking will default to External.

Split clocking, which is also known as “loop timing,” uses additional control signals (TXCE and RXCE) to keep the WSM and DSU clocking in sync. Split clocking takes the incoming clock signals (TX clock and RX clock) and loops them back out to the DSU. The WSM and DSU uses these additional signals to communicate the current status of their clocks. Split clocking should only be used if the WSM is a physical DCE device and you are using a non-RS-232 cable, such as V.35.

◆ Important Note ◆

Split clocking is required if the access rate of the Frame Relay line is greater than 256 Kbps. If Split clocking is not used at these data rates, then data out-of-phase errors, aborts, or CRC errors may occur.

Split clocking is the default when the WSM is a physical DCE device and a non-RS-232 DCE cable is connected to the port. For T1 and e1 ports, external or split clocking is the same as loop timing.

VCs Active/Inactive

Each port will have one or more associated virtual circuits. This column tells you the current status of *Data* virtual circuits. These counts do not apply to management virtual circuits. The first number is the number of active VCs and the second is the number of inactive VCs. An **Active** virtual circuit is one that is operationally Up and capable of transmitting data; it may not necessarily be transmitting at this time. An **Inactive** virtual circuit is present, but for some reason is operationally Down. It is not capable of passing data because either its administrative status was set to Down or the Frame Relay network indicated it was present but Down.

Information on the Ports for One WSM Board

To obtain status information on a single WSM board, you enter the **frstatus** command along with the slot number for the WSM board, as follows:

```
frstatus <slot>
```

where **<slot>** is the slot number where the WSM board is installed. For example, if you wanted to obtain status information for the board in slot 4, you would enter:

```
frstatus 4
```

This command displays a screen similar to the following:

Frame Relay Status for slot: 4

	Admin/ Oper PTStatus	Intf Type	Speed BPS	VCs Active/ Inactive	Frames In	Frames Out	Octets In	Octets Out
	=====	=====	=====	=====	=====	=====	=====	=====
1	UP/UP	V35DTE	2048000	2/0	364	128	8962	2650
2	DN/DN	*NONE*	9600	0/0	0	0	0	0
3	UP/DN	232DTE	56000	0/0	89	90	890	895
4	UP/UP	V35DTE	256000	19/1	9	21	124	245

Each row in the table corresponds to a port on the WSM you requested information on.

PT

The Port number on the WSM board for which statistics are displayed.

Admin/Oper Status, Int Type, Speed Bps, DLCI Active/Inactive

These columns are described in the section, *Information on All Boards in a Switch* on page 49-37. Please refer to this section for detailed information.

Frames In

The total number of frames received on this port since the last time the switch was initialized.

Frames Out

The total number of frames sent on this port since the last time the switch was initialized.

Octets In

The total number of Octets, or bytes, received on this port since the last time the switch was initialized. This statistic includes the data and Frame Relay header fields, but does not include CRC or flag characters.

Octets Out

The total number of Octets, or bytes, sent on this port since the last time the switch was initialized. This statistic includes the data and Frame Relay header fields, but does not include CRC or flag characters.

Information on One Port

To obtain status information on a single WSM port, you enter the **frstatus** command along with the slot number for the WSM board and the port number for which you want to receive information, as follows:

```
frstatus <slot>/<port>
```

where **<slot>** is the slot number where the WSM board is installed and **<port>** is the port number on the WSM board. For example, if you wanted to obtain status information for Port 1 on the WSM module in Slot 4, you would enter:

```
frstatus 4/1
```

This command displays a screen similar to the following:

Frame Relay Status for slot 4, port 1:

Physical Level Information	<pre>Administrative/Operational Status Up/Up Speed Intf. Receive Receive Receive Transmit Signal BPS Type CRC Errors Aborts Overruns Overruns Errors ===== 2048000 V35DTE 18 12 0 0 2 Control DTR RTS DSR CTS DCD Signal ON ON ON ON OFF</pre>
Logical (Frame Relay) Information	<pre>Frame Relay Information: Octets UniCast Discarded Error ===== Frames Frames Count IN 8962 120 2 0 Out 2650 24 5 0 IN+OUT 11612 144 7 0 Administrative/Operational Phase Up/Up Last Error TypeNo Error Since Reset Last Error Time 0 Seconds Interface failures 0 Last interface failure time 0 Seconds</pre>
Virtual Circuit Level Information	<pre>DLCI Information: Admin/ DLCI Oper DLCI Frames Frames Octets Octets Num Status Type In Out In Out ==== ===== 0 UP/UP Configured 10 10 160 140 31 UP/UP Learned 31 20 4196 1250 32 UP/DN Learned 145 110 4813 1450</pre>

This command displays three (3) layers of information. The top section provides information on the physical interface. The middle section provides information on the logical, or Frame Relay, interface. The bottom section provides information on the virtual circuits associated with this physical port.

Physical Layer Information

The statistics shown in this section are taken at the physical, or serial, interface level.

Administrative/Operational Status

This field shows the Administrative and Operational Status of this WSM port. The status indicator before the slash refers to the Administrative Status. If **UP**, then the port has been enabled and can transmit data as long as its Operational Status is also UP. If the Administrative Status is **DN**, then the port will not pass data even if its physical connection is good.

The status indicator after the slash refers to the Operational Status. If UP, then the port is capable of passing data as long as it has been logically enabled at the Administrative level. If **DN**, then the port cannot pass data because of a problem in the physical connection (e.g., cable disconnected, WSM could not detect cable type) or because the port is Administratively Down.

Speed BPS

The configured speed of the port. For a physical DTE port, the actual rate is determined by the DCE device to which the WSM is attached (i.e., a modem or DSU). For a physical DCE port, the actual rate is the rate configured through the **frmodify** command.

Intf Type

The type of cable that is plugged into the WSM port. The cable may be DCE or DTE and one of 5 different serial types. See *Intf Type* on page 49-38 for further information.

Receive CRC Errors

The total number of frames with an invalid frame check sequence received on the port since the last time the switch was initialized.

Receive Aborts

The total number of frames received that were terminated with an HDLC abort sequence since the last time the switch was initialized. An abort sequence consists of 7 contiguous bits of ones (1111111).

Receive Overruns

The total number of frames that were not received on the port because the system could not keep up with the data flow. Receive overrun errors include buffer errors and errors reported by the RISC processor.

Transmit Overruns

The total number of frames that were not transmitted on the port because the system could not keep up with the data flow. Transmit overrun errors include buffer errors and errors reported by the RISC processor.

Signal Errors

The total number of frames that failed to be received or transmitted due to a loss of modem signals since the last time the switch was initialized. If the WSM port is a physical DTE, then this count is the number of frames dropped due to a loss of the Data Set Ready (DSR) signal. If the WSM port is a physical DCE, then this count is the number of frames dropped due to a loss of the Data Terminal Ready (DTR) signal.

Control Signal

This table (which displays only for serial ports, not T1 or E1 ports) lists two or more control signals along with their current state. If a V.35, RS-232, RS-530, or RS-449 cable is attached then this table lists the following signals:

- **DTR** (Data Terminal Ready.)
- **RTS** (Request To Send.)
- **DSR** (Data Set Ready.)
- **CTS** (Clear To Send.)
- **DCD** (Data Carrier Detect.)

The ON/OFF indicator below the signal name tells you the current status of the signal. Under normal operating conditions (physical connection is good and VC is administratively enabled), all signals should be On.

Whether the signal is an input or an output depends on whether the WSM is a physical DTE or DCE. The following table shows the Input/Output status of each signal type.

Signal	Signal Direction When Port Is...	
	DCE	DTE
DTR	In	Out
RTS	In	Out
DSR	Out	In
CTS	Out	In
DCD	Out	In

If using an X.21 cable, then the table shown in the sample display is replaced by the following table:

Control Signal	C(Control) ON	I(Indicator) ON
----------------	---------------	-----------------

This X.21 table shows 2 rather than 5 signal statuses. The **C** signal is similar to the RTS (Request To Send) signal. The **I** signal is similar to the DCD (Data Carrier Detect) signal. Under normal operating conditions, both the **C** and **I** signals should be On.

Whether the signal is an input or an output depends on whether the WSM is a physical DTE or DCE. The following table shows the Input/Output status of each signal type.

Signal	Signal Direction When Port Is...	
	DCE	DTE
C	In	Out
I	Out	In

Frame Relay Information

The statistics shown in the section are gathered at the Frame Relay protocol level.

Octets

The total octets, or bytes, received (first row) and sent (second row) on this port. The third row shows the cumulative number of octets that have passed through the port (sent and received). This statistic includes the data and Frame Relay header fields, but does not include CRC or flag characters.

UniCast Frames

The total number of Unicast frames received (first row) and sent (second row) on this port. The third row shows the cumulative number of Unicast frames that have passed through this port (sent and received).

Unicast frames are destined for a specific virtual circuit, and are normally sent from one local DLCI to the corresponding DLCI on the other side of the Frame Relay link. In Frame Relay terms, these unicast frames are sent from a logical DTE, such as a WSM port, to a Remote logical DTE, such as a WSM port on the other side of the Frame Relay link.

Discarded Frames

The number of frames discarded due to an error.

Error Count

Frames that contained Frame Relay type errors, such as DLCMI protocol errors and invalid frame format. This count does not include standard physical errors, such as CRC and abort errors.

Administrative/Operational Status

This field shows the Administrative and Operational Status of this WSM port. The status indicator before the slash refers to the Administrative Status. If **UP**, then the port has been enabled and can transmit data as long as its Operational Status is also UP. If the Administrative Status is **DN**, then the port will not pass data even if its physical connection is good.

The status indicator after the slash refers to the Operational Status. If **UP**, then the port is capable of passing data as long as it has been logically enabled at the Administrative level. If **DN**, then the port cannot pass data due to a problem in the physical connection (e.g., cable disconnected, WSM could not detect cable type) or because the port is Administratively Down.

Last Error Type

The last type of Frame Relay DLCMI protocol error received on this port. The following list describes the error types displayed:

Unknown Error	An error occurred but it can not be classified into one of the standard Frame Relay error types.
Receive Short	The receive frame was not long enough to allow demultiplexing. The address field was incomplete, or the protocol identifier was missing or incomplete.
Receive Long	The receive frame exceeded the maximum length for this port.
Illegal DlcI	The DLCI address field in a frame did not match the configured format.
Unknown DlcI	A frame was received on a virtual circuit that was not active or was administratively disabled.
Dlcmi Protocol Error	An Unspecified error occurred while trying to interpret the Link Maintenance frame.
Dlcmi Unknown IE	DLCMI Unknown Information Element. The Link Maintenance frame contained an Information Element type that is not valid for the configured DLCMI protocol.
Dlcmi Sequence Error	The Link Maintenance frame contained a sequence flag that was different than the expected flag.
Dlcmi Unknown RPT	DLCMI Unknown Report Type. The Link Maintenance frame contained a Report Type Information Element with a value that is not valid for the configured DLCMI protocol.
No Error Since Reset	No error has occurred since the last time this port was initialized.

Last Error Time

The time since the last Frame Relay protocol error was received. A value of zero (0) indicates no Frame Relay protocol errors have been received. The type of error that was last received is indicated in the **Last Error Type** field.

Interface Failures

The number of times this Frame Relay port has gone down since it was initialized.

Last Interface Failure Time

The time since the interface was taken down due to excessive errors. Excessive errors are defined as the time when a DLCMI error exceeds the **Error Threshold** or the errors within the **Monitored Events Counter**. A value of zero (0) indicates the interface has not been taken down due to excessive errors. These error parameters are configured through **frmodify** and in most cases should be set to defaults. See *Setting Configuration Parameters* on page 49-21 for more information.

DLCI Layer Information

The information in this section of the display provides statistics on virtual circuits. Each row in this table corresponds to one virtual circuit.

DLCI Num

The DLCI number assigned to this virtual circuit. This value is only valid locally; the same virtual circuit on the other end of the Frame Relay line may or may not use the same DLCI for this VC.

Admin/Oper Status

This field shows the Administrative and Operational Status of this virtual circuit. The status indicator before the slash refers to the Administrative Status. If **UP**, then the virtual circuit has been enabled and can transmit data as long as its Operational Status is also UP. If the Administrative Status is **DN**, then the VC will not pass data even if its physical connection is good.

The status indicator after the slash refers to the Operational Status. If UP, then the virtual circuit is capable of passing data. If **DN**, then the VC cannot pass data because the network has declared the virtual circuit inactive, the network does not respond to STATUS ENQUIRY messages, or the VC is Administratively Down.

DLCI Type

The type of virtual circuit will be either **Configured** or **Learned**. Configured means this VC is a management, or control, circuit that is used by Frame Relay protocols, such as the DLCMI protocols, to pass various status messages. The Frame Relay network does not self-configure management virtual circuits. Data VCs can become “configured” if you use **frmodify** to change any of the default settings for the Data VC. Learned means this is a Data VC that the Frame Relay network informed the WSM module about through status messages (using a Control VC).

Note

The **VC Type** of the management DLCI (0 or 1023) is always **configured** since the Frame Relay network does not dynamically configure management virtual circuits.

Frames In

The number of frames received on this VC since it was created.

Frames Out

The number of frames transmitted on this VC since it was created.

Octets In

The number of octets, or bytes, received on this VC since it was created.

Octets Out

The number of octets, or bytes, transmitted on this VC since it was created.

Information on One Virtual Circuit

To obtain status information on a single virtual circuit, you enter the **frstatus** command along with the slot number for the WSM board, the port number, and DLCI number for the virtual circuit on which you want information, as follows:

```
frstatus <slot>/<port>/<DLCI>
```

where **<slot>** is the slot number where the WSM board is installed, **<port>** is the port number on the WSM board, and **<DLCI>** is the virtual circuit identifier. For example, if you wanted to obtain status information for the board in slot 4, port 1, DLCI 32, you would enter:

```
frstatus 4/1/32
```

This command displays a screen similar to the following:

```

Frame Relay Status for slot 4, port 1, DLCI 32
Admin/Oper Status: UP:UP for 0 days, 00:34:40.59
Compression Administrative Status/Operational Phase: Enabled/Operation

      Frames      Frames      Frames      Octets      Octets
      In          Out          In+Out      In          Out          %In      %Out
      =====      =====      =====      =====      =====      =====
Total                200          250          450          20000       17000
Ethernet             100          150          250          10000       11000      50     65
802.5                 0            0            0            0            0         0      0
FDDI                  0            0            0            0            0         0      0
IP                    0            4            4            0            2000       0      12
IPX                   90           99          185          9560        3960       48     23
BPDU                  10            1            11           440          40         2      <1
DE Bit                10            0            10
FECN Bit              5
BE CN Bit             7
Discarded             0

FRF.9
Compression:  Compressed Compressed Uncompressed      Compression
                Frames      Octets      Octets              Ratio
                =====      =====      =====      =====
In                200          10000       20000              2.0:1
Out               250          15000       17000              1.2:1
In+Out            450          25000       37000              1.5:1
    
```

The top of the display provides information on the status of this virtual circuit. The **Admin/Oper Status** field indicates the current Administrative and Operation Status for this virtual circuit. The next informational field, **Compression Administrative Status/Operational Phase**, indicates the current Administrative and Operational status for Compression Negotiation on this VC. The Administrative Status will be either **Enabled** or **Disabled**. The Operational Phase will be **Disabled** (compression negotiation not enabled), **Initialization** (compression negotiation in progress), or **Operation** (negotiation successful, data being compressed).

The table below the status information breaks down traffic on the virtual circuit by protocol type. Each row corresponds to a frame type, such as Ethernet or IPX. For each frame type, the number of frames received, frames transmitted, octets received, and octets transmitted is given. The final two columns of the table (**%In** and **%Out**) represent the total percentage of traffic (octets, not frames) for that protocol type.

The final table provides information on compressed data on this virtual circuit. The following sections describe information in the table.

Total (Protocol)

Statistics in this row indicate traffic for all protocol (Ethernet, IP, IPX, and BPDU) frames and octets on this VC. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

Ethernet

Statistics in this row indicate traffic for Ethernet (bridged 802.3 or trunked format) frames and octets on this virtual circuit. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

802.5

Statistics in this row indicate traffic for Token Ring (802.5 format) frames and octets on this virtual circuit. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

FDDI

Statistics in this row indicate traffic for FDDI frames and octets on this virtual circuit. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

IP

Statistics in this row indicate traffic for routed IP, ARP, and Inverse ARP format frames and octets on this virtual circuit. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

IPX

Statistics in this row indicate traffic for routed IPX format frames and octets on this virtual circuit. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

BPDU

Statistics in this row indicate traffic for BPDU frames and octets on this virtual circuit. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

DE Bit

Statistics in this row indicate the number of frames sent and received that have been marked for Discard Eligibility (the DE bit in the frame is set to 1). No statistics are given for Octets in this row. See *Discard Eligibility (DE) Flag* on page 49-9 for more information on the DE bit.

FECN Bit

This value indicates the total number of frames received from the network indicating forward congestion. This occurs when the Frame Relay network sets the frame's Forward Discard Eligibility (FECN) flag. These frames experienced congestion coming over the virtual circuit. Statistics are given only for Frames In for FECN Bit since the Frame Relay network sets it. See *Notification By FECN* on page 49-12 for more information on the FECN bit.

BECN Bit

This value indicates the number of frames received from the network indicating backward congestion. This occurs when the Frame Relay network sets a frame's Backward Discard Eligibility (BECN) flag. These frames observed congestion occurring in the opposite direction during their path over the virtual circuit. Statistics are given only for Frames In since the Frame Relay network sets the BECN bit. See *Notification By BECN* on page 49-11 for more information on the BECN bit.

Discarded

The number of inbound frames that were dropped due to format errors or because the VC was inactive.

Compressed Frames

Statistics in this column indicate traffic for compressed frames on this virtual circuit. Compressed frames are only sent if both sides of a Frame Relay link successfully negotiate for compression (i.e., both must support compression).

Compressed Octets

Statistics in this column indicate traffic for compressed octets on this virtual circuit. Compressed frames are only sent and received if both sides of a Frame Relay link successfully negotiate for compression (i.e., both must support compression). Statistics for octets include the data, Frame Relay header, and Data Compression header fields, but they do not include CRC or flag characters.

Uncompressed Octets

Statistics in this column indicate traffic for uncompressed octets on this virtual circuit. These values apply to the compressed data before compression or just after decompression. Statistics for octets include the uncompressed data and Frame Relay header fields, but they do not include CRC or flag characters.

Compression Ratio

Statistics in this column indicate the compression that was achieved for this type of traffic. For example, in the sample table Outgoing traffic had compression ration of

1.2:1

meaning that each compressed octet is 1.2 uncompressed octets.

Resetting Statistics Counters

You can reset the statistics counters for a single WSM board, a WSM port, or a specific DLCI. The statistics that are cleared on those that are displayed through the **frstatus** commands. The **frclear** command is used to reset statistics.

Resetting Statistics for a WSM Board

To reset statistics on a single WSM board, enter the **frclear** command along with the slot number for the WSM board, as follows:

```
frclear <slot>
```

where **<slot>** is the slot number where the WSM board is installed. For example, if you wanted to clear statistics for the board in slot 4, you would enter:

```
frclear 4
```

or

```
frc 4
```

Resetting Statistics for a WSM Port

To reset statistics on a single WSM port, enter the **frclear** command along with the slot number for the WSM board and the port number as follows:

```
frclear <slot>/<port>
```

where **<slot>** is the slot number where the WSM board is installed and **<port>** is the port number on the WSM board. For example, if you wanted to reset statistics for Port 1 on the WSM module in Slot 4, you would enter:

```
frclear4/1
```

or

```
frc 4/1
```

Resetting Statistics for a Virtual Circuit (DLCI)

To reset statistics on a single virtual circuit, you enter the **frclear** command along with the slot number for the WSM board, the port number, and DLCI number for the virtual circuit on which you want to reset statistics, as follows:

```
frclear <slot>/<port>/<DLCI>
```

where **<slot>** is the slot number where the WSM board is installed, **<port>** is the port number on the WSM board, and **<DLCI>** is the virtual circuit identifier. For example, if you wanted to reset statistics for the board in slot 4, port 1, DLCI 32, you would enter:

```
frclear 4/1/32
```

or

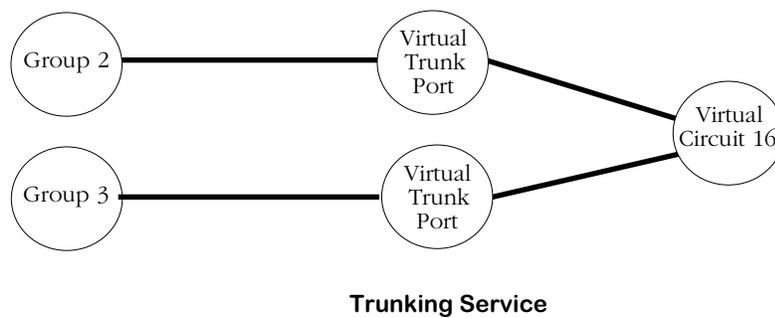
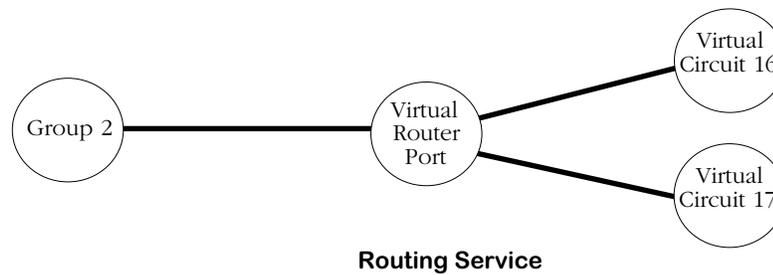
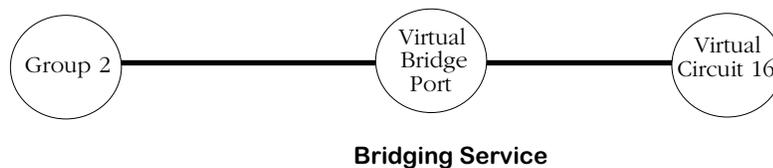
```
frc 4/1/32
```

Managing Frame Relay Services

By default, all virtual circuits on a WSM port have a Bridging service and are assigned to Group 1. The **frmodify** command allows you to change this default bridging service to another Group and to set up a default routing service for the port. See *Setting Configuration Parameters* on page 49-21 for information on the **frmodify** command.

To extend your control over a Frame Relay service, you can use Service menu commands. These command allow you to create and modify bridging, routing, and trunking services by assigning specific virtual circuits and Groups to the services.

Setting up a bridging service requires you to map a virtual circuit to a Group. Setting up a routing service requires you to map one or more virtual circuits to a Group. And setting up a Trunking service requires you to map a single virtual circuit to one or more Groups. The diagrams below illustrate the relationship between Groups, virtual ports and virtual circuits for each Frame Relay service type:



An overview of each type of service and how each operates in a Frame Relay environment can be found earlier in this chapter in the following sections:

- Bridging See *Bridging Services* on page 49-14.
- Routing See *Frame Relay IP Routing* on page 49-15 and *Frame Relay IPX Routing* on page 49-18.
- Trunking See *Trunking* on page 49-19.

The decision to set up one service over another is determined by your network configuration and amount of traffic. In general, you can follow these guidelines:

1. If all your Frame Relay connections are through OmniSwitches, then Trunking is probably the best choice. Trunking is normally set up exclusively for a virtual circuit. No bridging or Routing service needs to be configured on the same virtual circuit where a Trunking service has already been set up.
2. If interoperability is important, then Bridging or Routing is a good choice. In an environment where broadcast traffic is low and high CIRs are deployed, Bridging is a simpler and better choice. In environments with higher broadcast traffic and lower CIRs, Routing is a good solution. However, if you choose to set up a Routing service in an environment with different types of routers, all must support RFC 1490 encapsulation.
3. Bridging and routing services may share a virtual circuit.

The following sections describe how to configure each service type and then how to modify, view, and delete your Frame Relay services.

Configuring a Bridging Service

Frame Relay traffic is automatically bridged for Group 1 in a switch. You can alter this default through two different commands: **frmodify** and **cas**.

The **frmodify** command allows you to change the default Bridging Group from Group 1 to another Group or to turn off bridging completely. This command configures bridging on a port-by-port basis, but does not configure bridging on a virtual circuit basis—all virtual circuits may also be assigned to the Group specified in **frmodify**. See *Modifying a Port* on page 49-21 for more information on the **frmodify** command.

The **cas** command provides more control over bridging service configuration. In addition to naming, enabling and disabling bridging services through **cas**, you can assign specific virtual circuits to a bridging service. Follow the steps below to set up a bridging service through the **cas** command.

1. Enter the **cas** command followed the slot number, a slash (/), the port number, and then the service number for the bridging service:

```
cas 2/3 3
```

A screen similar to the following displays:

```
Slot 1 Port 2 Service 3 Configuration
1) Description ..... = Frame-Relay
   {Enter up to 30 characters}
2) Service Type ..... = Bridging
   {(T)runking, (R)outing, (B)ridging}
3) Administrative Status ..... = Enabled
   {(E)nable, (D)isable}
4) VC(s) ..... = 0
5) VLAN Group(s) ..... = 0
6) Frame-Relay Bridging Mode (Applies to Bridging Only).. = Bridge All
   {Bridge (a)ll, (E)thernet only}

(save/quit/cancel)
:
```

You make changes to the options in this screen at the colon prompt (:). You make changes by entering the line number for the option you want to change, an equal sign (=), and then the value for the new parameter.

2. Enter a description of this bridging service by entering 1, an equal sign (=), and then a description for this service. Your description can be up to 30 characters long.

```
1=<bridge service name>
```

When you are done entering a description, press **<Enter>**.

3. Specify that this is a bridging service by entering a 2, an equal sign, and a **B** as follows:

```
2=B
```

This specifies that you want to set up a bridging service, as opposed to a Trunking or Routing service. Press **<Enter>**.

4. By default, the bridging service is Enabled. This means that as soon as you are done configuring the service, it will begin bridging Frame Relay traffic. If you would like to disable this bridging service now and enable it later, enter **3=D** and press **<Enter>**.

5. You need to specify the DLCI for the virtual circuit to include in this bridging service. Only one virtual circuit may be specified for each bridging service. There is a one-to-one mapping between the Group and the virtual circuit. Enter a 4, an equal sign (=), and the DLCI number for the virtual circuit. The example below includes the virtual circuit with DLCI 16 in the bridging service:

4=16

Press **<Enter>**.

6. Specify the Group number that you want to be part of this bridging service. Enter a 5, an equal sign (=), and the Group number. Remember, by default a virtual circuit already bridges on Group 1. The example below includes Group 3 in the bridging service:

5=3

Press **<Enter>**.

7. Indicate whether or not you want frames to be translated on this virtual bridge port. When the **Frame-Relay Bridging Mode** field is set to **Bridge all**, no translation is performed on frames before they are sent out to the Frame Relay network; enter an **A** at this field to select this option.

When the **Frame-Relay Bridging Mode** field is set to **Ethernet only**, non-Ethernet frames are first translated to the default Ethernet frame format for this port before they are sent out to the Frame Relay network. Any MAC translations configured through the Switch menu are valid. Enter an **E** at this field to select this option.
8. Type **save** at the colon prompt (:) and press **<Enter>**. All parameters for this bridging service are saved.

Configuring a WAN Routing Service

There are two main steps to configuring WAN routing for frame relay:

1. Enable and configure routing for a specific WAN Routing group with the **crgrp** command. (Frame Relay Groups are different from other Groups as far as router configurations are concerned.)
2. Set up a WAN routing service through the **cas** command.

Both of these steps are described in the next two sections.

Step 1. Set Up a Frame Relay Routing Group

You enable WAN routing for a Group when you create the Group through the **crgrp** command. The steps for setting up a Group are described in Chapter 24, “Managing Groups and Ports.” Please see that chapter for the generic steps used to create a Group. Also, understand the following points where WAN Groups differ from other Groups.

- During the process of configuring the Group, the **crgrp** command will prompt you with the following prompt:

Enable WAN Routing? (n):

If you want to configure WAN routing on this Group, then you must answer Yes to this prompt. Otherwise, the Group will not be tagged correctly and will not be able to route Frame Relay traffic.

- When configuring IP and IPX Routing, you do not specify a default framing type since Frame Relay routing always uses 1490 encapsulation.
- You do not set up physical interfaces (virtual ports) through the **crgrp** command. All physical mappings for Frame Relay are done through services, as described in Step 2 of this section.

You can configure all virtual circuits to automatically be assigned to the WAN Routing Group you set up in this step. The **frmodify** command contains a parameter, **Default Routing Group**, that you can set to a WAN routing Group. All dynamically learned virtual circuits will automatically be assigned to this Group without any configuration required. See *Modifying a Port* on page 49-21 for more information on the **frmodify** command.

You can also configure a Frame Relay service using the **cas** command as described in *Step 2. Set Up a Frame Relay Routing Service* on page 49-57.

Step 2. Set Up a Frame Relay Routing Service

You create a Frame Relay routing service using the **cas** command. Follow the steps below to set up a routing service.

1. Enter the **cas** command followed the slot number, a slash (/), the port number, and then the service number for the routing service:

```
cas 2/3 1
```

A screen similar to the following displays:

```
Slot 1 Port 2 Service 3 Configuration
1) Description ..... = Frame-Relay
   {Enter up to 30 characters}
2) Service Type ..... = Bridging
   {(T)runking, (R)outing, (B)ridging}
3) Administrative Status ..... = Enabled
   {(E)nable, (D)isable}
4) VC(s)..... = 0
5) VLAN Group(s)..... = 0
6) Frame-Relay Bridging Mode (Applies to Bridging Only).. = Bridge All
   {Bridge (a)ll, (E)thernet only}
```

```
(save/quit/cancel)
```

```
:
```

You make changes to the options in this screen at the colon prompt (:). You make changes by entering the line number for the option you want to change, an equal sign (=), and then the value for the new parameter.

2. Enter a description of this routing service by entering 1, an equal sign (=), and then a description for this service. Your description can be up to 30 characters long.

```
1=<router service name>
```

When you are done entering a description, press **<Enter>**.

3. Specify that this is a routing service by entering a 2, an equal sign, and an **R** as follows:

```
2=5
```

This specifies that you want to set up a routing service, as opposed to a Trunking or Bridging service. Press **<Enter>**.

4. By default, the routing service is Enabled. This means that as soon as you are done configuring the service, it will begin routing Frame Relay traffic. If you would like to disable this routing service now and enable it later, enter **3=D** and press **<Enter>**.
5. You need to specify the DLCIs of the virtual circuits to include in this routing service. Multiple VCs may be configured for a single routing service and all configured VCs will map to a single virtual router port. Enter a 4, an equal sign (=), and then the DLCI numbers for each virtual circuit. Separate DLCIs with spaces, as shown in the example below.

```
4=16 17
```

Press **<Enter>** after you enter all virtual circuit DLCIs.

6. Specify the Group number to which this router port belongs. Enter a 5, an equal sign (=), and the Group number. The example below includes Group 4 in the routing service:

5=4

Press **<Enter>**.

You must have previously configured this Group as a Frame Relay Routing Group through the **crgp** command. If you have not configured the Group for Frame Relay routing, then the following message displays:

Given Vlan Group is not a Frame-Relay Router Group

See the section, *Step 1. Set Up a Frame Relay Routing Group* on page 49-56 for further information on setting up a Frame Relay Group.

7. Disregard the **Frame-Relay Bridging Mode** field. It does not apply to virtual router ports.
8. Type **save** at the colon prompt (:) and press **<Enter>**. All parameters for this bridging service are saved.

Configuring a Trunking Service

To configure a Frame Relay Trunking service, you must use the **cas** command. Perform the following steps:

1. Enter the **cas** command followed the slot number, a slash (/), the port number, and then the service number for the Trunking service:

```
cas 2/3 1
```

A screen similar to the following displays:

```
Slot 1 Port 2 Service 3 Configuration
1) Description ..... = Frame-Relay
   {Enter up to 30 characters}
2) Service Type ..... = Bridging
   {(T)runking, (R)outing, (B)ridging}
3) Administrative Status ..... = Enabled
   {(E)nable, (D)isable}
4) VC(s) ..... = 0
5) VLAN Group(s) ..... = 0
6) Frame-Relay Bridging Mode (Applies to Bridging Only).. = Bridge All
   {Bridge (a)ll, (E)thernet only}
```

```
(save/quit/cancel)
```

```
:
```

You make changes to the options in this screen at the colon prompt (:). You make changes by entering the line number for the option you want to change, an equal sign (=), and then the value for the new parameter.

2. Enter a description of this Trunking service by entering 1, an equal sign (=), and then a description for this service. Your description can be up to 30 characters long.

```
1=<trunk service name>
```

When you are done entering a description, press **<Enter>**.

3. Specify that this is a Trunking service by entering a 2, an equal sign, and a **T** as follows:

```
2=T
```

This specifies that you want to set up a Trunking service, as opposed to a bridging or Routing service. Press **<Enter>**.

4. By default, the Trunking service is Enabled. This means that as soon as you are done configuring the service, it will begin Trunking Frame Relay traffic as you configure it through this menu. If you would like to disable this Trunking service now and enable it later, enter **3=D** and press **<Enter>**.

Configuring a Trunking Service

5. You need to specify the DLCI for virtual circuit that will be used to trunk traffic over the Frame Relay network. Only one virtual circuit may be specified for each Trunking service. Enter a 4, an equal sign (=), and the DLCI number for the virtual circuit similar to the example below:

4=16

Press **<Enter>**.

6. Specify the Group number or numbers that you want to be Trunked over the specified virtual circuit. A separate virtual Trunk port is created for each Group you specify here. Each Group and Trunk port maps down to a single virtual circuit. Enter a 5, an equal sign (=), and the Group number(s). The example below includes Groups 5 and 6 in the trunking service:

5=5 6

Press **<Enter>**.

7. Disregard the **Frame-Relay Bridging Mode** field. It does not apply to virtual trunk ports.
8. Type **save** at the colon prompt (:) and press **<Enter>**. All parameters for this bridging service are saved.

Viewing Frame Relay Services

You can view all Frame Relay services for an entire switch, a single WSM board, or a single WSM port. Use the **vas** command with the following parameters:

```
vas <slot>/<port> <service number>
```

The <slot>, <port> and <service number> parameters are not required but may be specified to narrow the range of the information displayed. For example, if you specify the **vas** command alone, without specifying information on a specific Frame Relay board, then you will obtain information on any FDDI and ATM services in the switch as well.

The **vas** command displays all services configured in the switch (ATM, FDDI, and Frame Relay). The following is an example of the Frame Relay portion of the **vas** command display:

Frame-Relay Services							
Slot	Port	VCs	Groups	Service Number	Vport	Description	Service Type
3	2	16	1	1	10	Virtual port (#10)	Bridging
3	3	16	1	1	11	Virtual port (#11)	Bridging
3	3	17	1	2	13	Virtual port (#13)	Bridging
3	2	17	1	2	14	Virtual port (#14)	Bridging
3	3	17	3	3	17	Virtual port (#17)	Routing
3	4	18	2	1	18	Virtual port (#18)	Trunking

The following sections describe the columns in this table.

Slot

The slot number where this WSM module is installed.

Port

The port number to which this service maps. A port may be listed more than once if multiple virtual circuits or multiple services are configured for it. The port is listed for each virtual circuit and for each service. For example, in the sample screen above Port 3 is listed three times—twice as a bridging service for virtual circuits 16 and 17 and again as a routing service for virtual circuit 17.

VCs

The DLCI of the virtual circuit supported by this service. A virtual circuit can be attached to more than one port and be supported by more than one service type.

Groups

The Group or Groups associated with this service. Only one Group is supported by a bridging or routing service. Trunking services may support multiple Groups.

Service Number

Each service for a port is assigned a number. This column lists the number for this service on this particular port. Note that in the sample screen, Port 2 has two services associated with it (Bridging for VC 16 and 17) and Port 3 has three services associated with it (Bridging for VC 16 and 17 and Routing for VC 17).

Vport

The virtual port associated with this service. For bridging services, there is a one-to-one mapping between a virtual port and a virtual circuit. For routing services, multiple virtual circuits may map to a single virtual port. For trunking services, multiple virtual ports can map to a single virtual circuit.

Description

The textual description given to this service when you set it up through the **cas** or **mas** command.

Service Type

A Frame Relay service may be **Bridging**, **Routing** or **Trunking**. All three service types are set up through the **cas** command. Bridging and Routing services may coexist on the same virtual circuit. Trunking cannot coexist with either Bridging or Routing on the same virtual circuit.

Modifying a Frame Relay Service

You can modify previously created Frame Relay services using the **mas** command. The **mas** command uses the same screen as the **cas** command. Simply enter **mas**, the slot, slash (/), port and service number. For example:

```
mas 2/3 1
```

would modify the first service on Port 3 for the WSM board in Slot 2. This command displays the same screen as the **cas** command. See the appropriate section for modifying the service type:

- Bridging See *Configuring a Bridging Service* on page 49-54.
- Routing See *Configuring a WAN Routing Service* on page 49-56.
- Trunking See *Configuring a Trunking Service* on page 49-59.

Deleting a Frame Relay Service

You can delete a Frame Relay service using the **das** command as follows:

1. Enter **das** followed by the slot, port and service number for the Frame Relay service that you want to delete. You can obtain the service number by using the **vas** command. See *Viewing Frame Relay Services* on page 49-61. For example, if you wanted to delete service number 2 for Port 2 on the WSM board in Slot 3, you would enter

```
das 3/2 2
```

and the following screen would display:

Frame-Relay Services							
Slot	Port	VCs	Groups	Service Number	Vport	Description	Service Type
====	====	====	====	====	====	====	====
3	2	16	1	1	10	Virtual port (#10)	Bridging
3	2	17	1	2	14	Virtual port (#14)	Bridging

```
Remove Frame Relay Slot 3 Port 2 Service 2 (n)? :
```

2. Enter **1** and press **<Enter>** to confirm the deletion of this service. The following messages display confirming the deletion of the service:

```
Removing Frame Relay Slot 3 Port 2 Service 2, please wait...
```

```
Frame Relay Slot 3 Port 2 Service 2 removed
```


50 Point-to-Point Protocol

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. The base protocol is specified in RFC 1661. Many other RFCs define additional capabilities for network protocol negotiation, management information databases (MIBs), and PPP operation over different kinds of serial channels.

PPP is comprised of three main components. The first component is a method of encapsulating multi-protocol datagrams so that the underlying protocol can be identified; the second component is the Link Control Protocol (LCP) that is used for establishing, configuring, and testing the datalink connection; the third component is a family of Network Control Protocols (NCPs) that are used for establishing and configuring different network-layer protocols such as IP and IPX.

The implementation of PPP for the OmniSwitch WAN Switching Modules supports bridging, IP routing and IPX routing. Data compression of the PPP packets is also supported when the WSM module contains a STAC 9705 Data Compression Coprocessor.

PPP Connection Phases

There are five phases to a PPP connection: Dead, Establish, Authenticate, Network, and Terminate:

Dead. The first phase is called the “Dead” phase because the physical channel has not yet been activated.

Establish. After the physical channel has been activated, the PPP connection enters the second phase, called “Establish,” wherein it attempts to negotiate link-level parameters and options using the Link Control Protocol (LCP). This phase ends when the LCP enters its own “open” state.

Authenticate. After LCP has reached its “open” state, the PPP connection enters the phase called “Authenticate” wherein it tries to identify the peer with which it is attempting to establish a connection. If the authentication option is enabled, either the Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP) is used to perform the authentication. If authentication is not enabled, the PPP connection proceeds to the next phase, “Network.”

Network. After the “Authenticate” phase is successful (or when it is not enabled), the PPP connection proceeds to the next phase, called “Network,” wherein the network protocols are negotiated using the appropriate Network Control Protocol (NCP). For example, to negotiate the use of IP over the PPP connection, the Internet Protocol Control Protocol (IPCP) is used. The details of the negotiation are specific to each network protocol, but may include such tasks as assigning network layer addresses. A network layer protocol must be negotiated successfully before the exchange of protocol packets can proceed; but, once negotiated, the protocol can begin to freely exchange packets. The PPP connection spends most of its time in the “Network” phase, because this is where the active transmission of data occurs.

Terminate. The final phase of a PPP connection is called the “Terminate” phase. This phase begins when authentication is unsuccessful or the channel becomes inoperative. Very often, this phase is simply bypassed, and PPP will return to the idle (Dead) phase when a channel is disconnected.

Data Compression

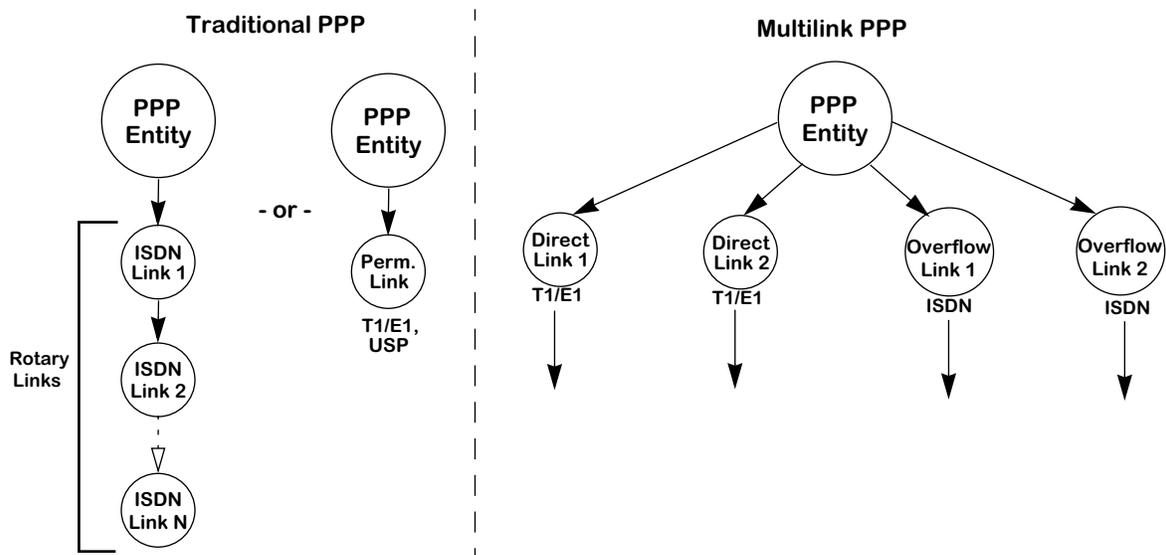
RFC 1974 specifies the use of STAC-LZS compression with PPP. Data compression allows the payload of a PPP packet, including the protocol ID, to be compressed, saving valuable bandwidth. Compression is negotiated during the Network phase using Compression Control Protocol (CCP), which includes the negotiation of a data compression algorithm and any parameters specific to the algorithm. Once negotiated, all data packets (i.e., non-control protocol packets) from all successfully negotiated protocols are compressed before transmission. The compression algorithm negotiated includes any mechanism for synchronizing the compressor and decompressor.

STAC-LZS's maximum data compression ratio is 30:1. The LZS algorithm is optimized to compress all file types as efficiently as possible. Even string matches as short as two octets are effectively compressed. The STAC-LZS compression algorithm supports both single compression history communication and multiple compression history communication.

Often, many streams of information are interleaved over the same link. Each virtual link will transmit data that is independent of other virtual links. Using multiple compression histories can improve the compression ratio of a communication link.

Multi-Link PPP

The main limitation of PPP is implicit in its name: Point-to-Point Protocol, meaning that it is limited to connecting two points over a single physical connection. Multi-Link PPP (MLPPP) extends the functionality of PPP by combining multiple PPP links into a single logical data pipeline, called a "bundle." Unlike standard PPP, MLPPP is not limited to individual links; both physical and virtual connections can be bundled.



Traditional vs. Multilink PPP

Multilink Modes of Operation

Multilink PPP supports combinations of both permanent and switched connections. This results in two possible modes of operation:

- permanent connection only
- switched connection only

Note

One important thing to remember when setting up multilinks is that all links to be bundled must exist on the same slot.

Permanent Connection Only

This mode allows multiple links to be joined into a single bundle. Permanent connections can be universal serial ports or fractional T1/E1 ports.

Switched Connection Only

This mode supports only switched connections. The only switched connections currently supported are ISDN calls. This allows multiple switched connections to be joined into a single bundle. In this mode, the first call is initiated as a demand connection, if a frame is available for the peer, or a backup connection, if the primary link becomes inactive, according to the configuration of the ISDN link.

◆ Note ◆

ISDN MLPPP bundles are limited to 2 B-channels

PPP Fragmentation Interleaving

The PPP Fragmentation/Interleaving functionality creates two prioritized virtual streams within a single PPP connection. The lower priority stream uses an MLPPP header to sequence the frames while the higher priority stream uses a standard PPP header without MLPPP sequence numbers. The lower priority stream is fragmented according to maximum delay parameters so that a higher priority frame can be injected in the middle of the low priority frame and not have to wait for the entire low priority frame to be transmitted.

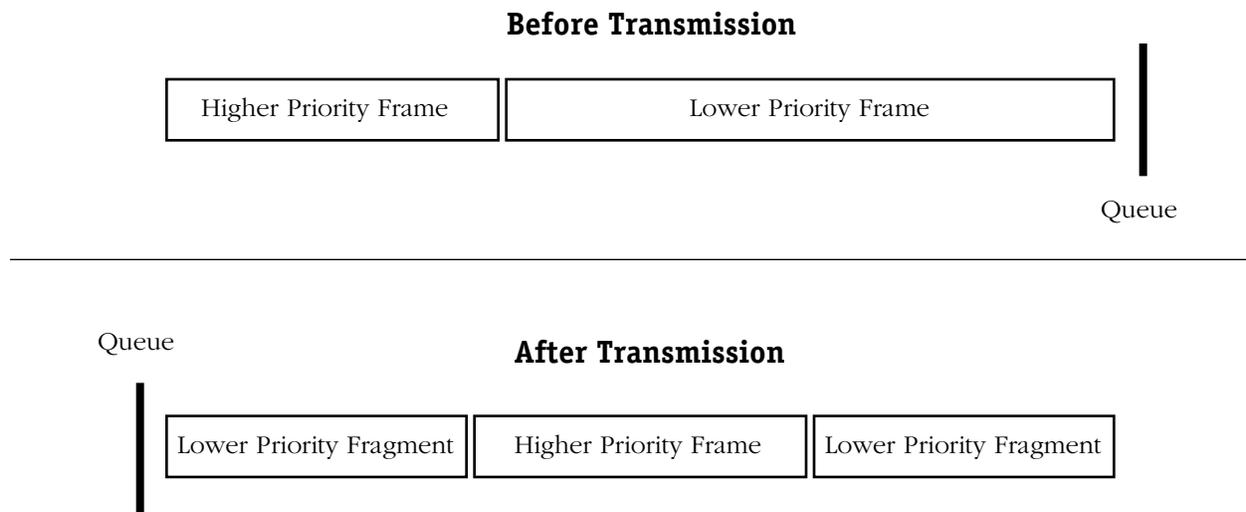
On the transmitting side, when low priority frames are being transmitted they are divided into multiple fragments. The size of each fragment is determined by the configured maximum delay parameter and the speed of the physical interface. The fragments are encapsulated with a standard MLPPP header, which contains a sequence number to identify lost fragments and beginning and ending flags to identify frame boundaries. When high priority frames are transmitted they are sent whole with standard PPP headers.

The delay of the high priority frame is the time it takes to finish transmitting the current frame or fragment plus the time it would take to transmit any other high priority frames in queue. On the OA-512, which has a hardware based high and low priority transmit queues, the high priority frame would be sent as soon as the current fragment/frame is finished. On the WSX, which has software based high and low priority transmit queues, it depends on how many frame/fragments have been committed to transmit buffer descriptors ahead of it. As part of the WSM transmit data flow improvements, the number of frames/fragments committed to buffer descriptors will be kept to a minimum, but because the queues are software based, will not be able to match the delays of the OA-512.

On the receiving side, as low priority frames are being received they will be put into the MLPPP reassembly queue, as supported by the existing software. As complete frames are received they will be forwarded to the normal PPP processing. When high priority frames are received, since they will always be sent complete, they will immediately be forwarded to the normal PPP processing.

The only configurable parameter that has been added is the maximum delay. The feature is enabled when this parameter is set to a non-zero value. A flag has been utilized to force a 16 fragment maximum for a fragmented frame to make this process compatible with Cisco products.

The following diagram illustrates this concept:



PPP Fragmentation Process

Overview of PPP Configuration Procedures

The configuration of a PPP connection on your switch is divided into three separate tasks. This three-phase strategy was chosen to allow PPP connections to be configured over *any* serial channel interface without requiring the use of multiple PPP configuration displays for each separate type of interface.

Step 1. Configure the Physical Interface to be Used for PPP

The information configured at the physical interface level includes the specification of the type of WSM interface and of any information that is specific to the given type of interface. The interfaces that can support PPP are ISDN, T1/E1, and the Universal Serial Port on all WSM boards.

An ISDN interface (WSM-BRI) requires the specification of the switch type, the local telephone number, and the Service Profile Identifiers (SPIDs) if appropriate for the switch type. The UI commands used to configure ISDN interfaces allow for modifying and viewing ISDN port's configuration and the display of its operational status. See Chapter 52 titled "Managing ISDN Ports" for detailed information on configuring an ISDN interface for PPP.

The configuration of a T1/E1 interface is described in Chapter 53 titled “Managing T1 and E1 Ports.”

The configuration of a universal serial port (USP) on a WSM-S board is described in Chapter 48 titled “Managing WAN Switching Modules.”

Step 2. Configure the Operation of PPP Itself

The information configured at the PPP level includes the remote and local user IDs and passwords, network protocol information, the use of data compression, and retry and delay information to be used during PPP connection establishment with LCP. The UI commands used to configure PPP connections (called “PPP Entities”) allow for the adding, modifying, and viewing of PPP connections and their operational status. This chapter describes the configuration of PPP Entities (connection configurations) using the **pppadd**, **pppmodify**, **pppdelete**, **pppview**, and **pppstatus** commands.

Step 3. Configure a Link Between the Physical Interface and PPP

As mentioned above, three kinds of physical interfaces can support PPP connections: Universal Serial Ports (on all WSM boards,), T1/E1 channels (on the WSM-FT1/E1 board), and ISDN lines (on the WSM-BRI board).

The “WAN Links” used to support PPP connections vary somewhat, depending upon which type of physical interface is being used for PPP. When the physical interface is a Universal Serial Port (USP) or a fractional T1/E1 channel (which are permanent channels), the port is dedicated to the PPP connection and the “WAN Link” simply identifies the physical interface in terms of the slot and port. When the physical interface being used is an ISDN interface (which provides dynamic, switched connections), the “WAN Link” identifies the numbering information that is to be used to establish the serial connection and the slot/port if necessary. The UI commands used to configure WAN Links allow for the adding, modifying, and viewing of the links, and the display of their operational status. See Chapter 51 titled “WAN Links” for detailed information on the commands used to configure WAN Links.

Multiple links can be configured when employing Multilink PPP, one for each link in the bundle. For Multilink PPP over ISDN, each link configured for a PPP entity is called every time the connection is attempted and Multilink PPP is successfully negotiated. For normal PPP over ISDN, when a connection with a PPP entity is attempted, each link is called until one is successful.

The PPP Submenu

The WAN menu contains a submenu, named **PPP**, containing commands specific to the Point-to-Point-Protocol (PPP).

To display the **PPP** menu, enter the following commands:

```
PPP
?
```

A screen similar to the following displays:

Command	PPP Menu
pppglobal	Add PPP Global configuration record
pppadd	Add PPP configuration record
pppmodify	Modify PPP configuration record
pppdelete	Delete PPP configuration record
pppview	View PPP configuration record(s)
pppstatus	Get Status of PPP configuration records and associated links

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

PPP Configuration Overview

Your first configuration step is to create a global PPP configuration record using the **pppglobal** command. This global record is used to provide default settings to be used for incoming calls. Then, you can add individual PPP configuration records (called “PPP Entities”) for each peer (i.e., for each remote site) with which you wish to be able to establish a point-to-point connection. You will need to know specific information about the remote peers with which you wish to connect in order to successfully configure the PPP Entity.

After you have configured at least one PPP Entity, you can use the other commands on the PPP Menu to modify, delete, view, and display its operational status. You can then add PPP Entities as you need them to support additional PPP connection requirements.

When a port is configured for PPP via the **wpm** command, a PPP entity and a WAN link entry are created automatically. For more information, see Chapter 48 titled “Managing WAN Switching Modules.”

Setting Global PPP Parameters

The **pppglobal** command is used to set global configuration parameters that are used by the PPP protocol. These parameters are termed “global” because they are the default settings used by the switch to establish connections with incoming calls. These global settings are not tied to a specific peer (i.e., a PPP Entity; see *Adding a PPP Entity* on page 50-9).

To set the global PPP parameters, enter the following command:

```
pppglobal
```

A screen similar to the following displays:

```
PPP Global Configuration:
```

- ```

1) Default Authentication Type PAP
 {(N)one, (P)AP, (C)HAP}
2) Global User ID sent to remote for Authentication. =
 {8 characters userid}
3) Global Password sent to remote for Authentication =
 {8 characters password}
4) Default Compression Type = STAC-LZS
 {(N)one, STAC-(L)ZS}
5) Default Bridge Config Admin Status = Disabled
 {(E)nable, (D)isable}
6) Default IP Config Admin Status..... = Enabled
 {(E)nable, (D)isable}
7) Default IPX Config Admin Status = Disabled
 {(E)nable, (D)isable}

```

```
(save/quit/cancel)
```

```
:
```

The fields on this screen have the following meanings:

### Default Authentication Type

Specifies the type of authentication that is to be expected on incoming calls. The options are **None**, **PAP**, and **CHAP**. Set this parameter to the type of authentication that you expect your callers to be using. If you enable either PAP or CHAP authentication, the next two parameters must also be set (user ID and password) or the caller’s connection requests will be refused. If you set this parameter to **None**, you must also set the Default Bridge, IP and IPX Configuration Administration Status parameters or the caller’s connection requests will be refused.

### Global User ID sent to remote for Authentication

Specifies the user ID that will be sent to a peer on incoming calls. Enter the text you will transmit on incoming calls. This parameter must contain a value if either PAP or CHAP authentication is being used. The User ID and password received from the peer will be checked against the list of peers (PPP Entities) to attempt to identify the remote peer.

### Global Password sent to remote for Authentication

Specifies the password that will be sent to a peer on incoming calls. Enter the text you will transmit on incoming calls. This parameter must contain a value if either PAP or CHAP authentication is being used.

### **Default Compression Type**

Specifies the type of compression that is to be expected on incoming calls. The options are **None** and **STAC-LZS**. If you set this parameter to **None** and your callers are using compression, the caller's connection request may be refused. See *Data Compression* on page 50-2 for a description of STAC-LZS data compression.

### **Default Bridge Config Admin Status**

Specifies whether the bridging function is to be negotiated for incoming calls. More information on the bridging function can be found in *Adding a PPP Entity* on page 50-9. If this parameter is disabled here, but disabled on the caller, the caller's connection request may be refused.

### **Default IP Config Admin Status**

Specifies whether the IP routing function is to be negotiated for incoming calls. More information on the IP routing function can be found in *Adding a PPP Entity* on page 50-9. If this parameter is disabled here, but disabled on the caller, the caller's connection request may be refused.

### **Default IPX Config Admin Status**

Specifies whether the IPX routing function is to be negotiated for incoming calls. More information on the IPX routing function can be found in *Adding a PPP Entity* on page 50-9. If this parameter is disabled here, but disabled on the caller, the caller's connection request may be refused.

## Adding a PPP Entity

The **pppadd** command is used to add a PPP Entity configuration record. The PPP Entities you create are identified by numbers called Peer IDs. When you enter the **pppadd** command, you may enter a Peer ID number with the command like this:

```
pppadd <ID number>
```

Alternatively, you can enter the command alone and you will be prompted for a Peer ID. The prompt will identify the next available, unique ID number.

After you enter the **pppadd** command as described above, a screen will be displayed that contains the configuration parameters that make up the PPP Entity. The steps that begin below will take you through the process of adding a PPP Entity.

After you have set the PPP Entity's configuration parameters, you must save them to actually create the PPP Entity. After saving, you will be prompted to add one or more links to be used with the PPP Entity. In other words, the software will automatically issue a **linkadd** command for you. This was designed to help you to quickly create working PPP Entities as they must be associated with at least one link in order to operate. The **linkadd** command, as well as the other commands on the Link menu, are described in Chapter 51 titled "WAN Links."

1. To add a PPP Entity, enter the following command:

```
pppadd
```

A screen similar to the following will display:

```
Add PPP configuration record. Please specify a unique
ID number to identify this record and the remote Peer to communicate with.
```

```
Peer ID (1):
```

This prompt is asking you to enter a Peer ID as well as indicating that the next available number is 1. If other Peers have already been configured, the number indicated will be different than is shown above.

2. To answer the prompt, for example, for Peer ID 1, you would enter the following command:

```
1
```

If you have enabled the verbose mode, you will see the following text immediately before the prompts:

```
To change a value, enter the corresponding number, an '=', and the new
value. For example to set a new description, use
: 2=My new Description
To clear an entry specify the value as '.' as in
2=.
When complete enter "save" to save all changes, or cancel or Ctrl-C to
cancel all changes. Enter ? to view the new configuration.
```

This text provides brief help on entering commands at the following screens. In the steps that follow below, this help text will *not* be shown.

A screen similar to the following will display:

```
Adding PPP configuration record for Peer ID: 1
Enter PPP parameters:

1) Description :
 {Enter text up to 30 characters}
2) Administrative Status Enabled
 {(E)nabled, (D)isable}
3) PPP Mode Normal
 {(N)ormal, (M)ultilink}
4) Compression Type None
 {(N)one, STAC-(L)ZS}
5) Bridging Group 1
 {1-65535 or 0 if no Bridging}
50) Bridge Config Admin Status Enabled
 {(E)nabled, (D)isable}
51) PPP Bridging Mode Ethernet Only
 {Bridge (A)ll, (E)thernet Only}
6) Routing Group 0
 {1-65535 or 0 if no Routing}
7) Authentication Type None
 {(N)one, (P)AP, (C)HAP}
8) Max Failure Count 3
 {1..65535}
9) Max Configure Count 3
 {1..65535}
10) Max Terminate Count 3
 {1..65535}
11) Retry Timeout Value 5
 {Retry Timeout in Second(s) 1..65535}
12) Fragmentation Interleaving No
 {Fragmentation Interleaving Yes or No}

(save/quit/cancel)
:
```

The prompts for Bridging, Routing, Authentication, and Fragmentation Interleaving (numbered 5, 6, 7, and 12 above), contain suboptions that are displayed only if you have enabled those features. These expanded menus are shown below in the relevant sections describing the UI fields.

3. When you have made the changes you need to the prompts on this screen, enter the following command to save the PPP Entity:

```
save
```

The following prompt will display:

```
Normal (non-multilink) PPP configuration record created.
Do you wish to define the link at this time y/n (y):
```

If you answer yes to this prompt, a **linkadd** command will be automatically executed for this PPP Entity. For complete details on using the **linkadd** command, see the relevant section in Chapter 51, entitled “WAN Links.”

If you answer No to this prompt, a message will appear indicating that the link was not added, but the PPP Entity itself was added.

### Note

You can add the link needed for a PPP Entity later if you decide not to do so now. The automatic execution of the **linkadd** command is done here only as a conve-

nience to you.

The fields on the **pppadd** configuration screen have the following meanings:

**Description**

A textual description for this PPP Entity. You can enter any text you like (up to 30 characters).

**Administrative Status**

Indicates the Administrative Status of this PPP Entity. **Enabled** will allow the PPP Entity to operate. **Disabled** will disable the PPP Entity without deleting it.

**PPP Mode**

Can be set to either **Multilink** or **Normal** (single PPP connection).

**Compression Type**

Controls whether this PPP Entity will perform compression. The one type of compression currently available is STAC-LZS. See *Data Compression* on page 50-2 for details on STAC-LZS compression.

**Bridging Group**

Indicates the VLAN Group to be used for PPP Bridging. A value of zero (0) indicates that this PPP Entity will not perform a bridging service and will discard all bridged format packets received or transmitted. The suboptions under this heading are:

***Bridge Config Admin Status***

Used to enable or disable the bridging function for this PPP Entity.

***PPP Bridging Mode***

Used to select the operational mode for bridging. The options are **Ethernet**, which will enable bridging on Ethernet interfaces only, or **All**, which enables it for all interfaces.

**Routing Group**

Indicates the VLAN Group to be used for PPP Routing of the IP and IPX protocols. A value of zero (0) indicates that this PPP Entity will not perform a routing service and will discard all routed format packets received or transmitted.

Enabling Routing expands the menu with the following suboptions:

- 6) **Routing Group** ..... 1  
 {1-65535 or 0 if no Routing}
- 60) **IP Config Admin Status** ..... Enabled  
 {(E)nabled, (D)isable}
- 61) **Remote IP Address (Only valid if IP is enabled)** ..... 0.0.0.0  
 {Valid IP address notation e.g., x.x.x.x}
- 62) **IPX Config Admin Status** ..... Enabled  
 {(E)nable, (D)isable}

The suboptions under this heading are:

### ***IP Config Admin Status***

Used to enable or disable the routing of IP packets over PPP. The options are **Enabled** and **Disabled**.

### ***Remote IP Address (Only valid if IP is enabled)***

Used to specify the Remote IP address of the PPP connection when IP routing is enabled. Valid IP address notation must be used. If this parameter is set to 0.0.0.0 and IP routing is enabled, the Remote IP address will be learned during Internet Protocol Control Protocol (IPCP) negotiation.

### ***IPX Config Admin Status***

Used to enable or disable routing of IPX packets over PPP. The options are **Enabled** and **Disabled**.

## **Authentication Type**

Indicates the type of authentication to be used by this PPP Entity. The options are **None**, **PAP**, and **CHAP**.

Enabling Authentication expands the menu with the following suboptions:

- 7) **Authentication Type** . . . . . **PAP**  
{(N)one, (P)AP, (C)HAP}
- 70) **User ID received from remote for Authentication** . . .  
{8 characters userid}
- 71) **Password received from remote for Authentication** .  
{8 characters password}
- 72) **User ID sent to remote for Authentication** . . . . .  
{8 characters userid}
- 73) **Password sent to remote for Authentication** . . . . .  
{8 characters password}

The suboptions under this heading are:

### ***User ID received from remote for Authentication***

Used to specify the User ID to be expected from the remote end during PAP or CHAP authentication.

### ***Password received from remote for Authentication***

Used to specify the password to be expected from the remote end during PAP or CHAP authentication.

### ***User ID sent to remote for Authentication***

Used to specify the User ID to be sent to the remote end during PAP or CHAP authentication. This parameter is used only for outgoing calls. Incoming calls use the global defaults (see *Setting Global PPP Parameters* on page 50-7 for details).

### ***Password sent to remote for Authentication***

Used to specify the password to be sent to the remote end during PAP or CHAP authentication. This parameter is used only for outgoing calls. Incoming calls use the global defaults (see *Setting Global PPP Parameters* on page 50-7 for details).

**Max Failure Counter**

The maximum number of times a CONFIGURATION\_REQUEST packet will be sent when the previous attempts received responses, but did not receive a CONFIGURATION\_ACK. This counter applies to all LCP and NCP negotiations.

**Max Configure Counter**

The maximum number of times a CONFIGURATION\_REQUEST packet will be sent when the previous attempts did not receive any responses. This counter applies to all LCP and NCP negotiations.

**Max Terminate Counter**

The maximum number of TERMINATE\_REQUEST packets that will be sent without receiving a TERMINATE\_ACK packet. This counter applies to all LCP and NCP negotiations.

**Retry Timeout Value**

Indicates the number of seconds to wait between CONFIGURATION\_REQUEST retries that do not receive a response. This timeout value applies to all LCP and NCP negotiations.

**Fragmentation Interleaving**

Fragmentation Interleaving allows you to break up lower priority packets into smaller pieces and insert higher priority packets inbetween. This is useful when sending time-critical information streams such as voice or video data.

Enabling Fragmentation Interleaving expands the menu with the following suboptions:

- 12) **Fragmentation Interleaving** ..... **No**  
     {Fragmentation Interleaving Yes or No
- 121) **Fragmentation Delay** ..... **0**  
         {Fragmentation Delay in milliseconds(ms)}
- 122) **Limit Maximum number of fragmentation to 16** ..... **No**  
         {(Y) meant cisco compatible. (N) meant native}

***Fragmentation Delay***

This field specifies a millisecond count for determining when to fragment a PPP packet. If higher priority data will remain in the queue for over the set amount of time, then the packet is fragmented.

***Limit Maximum number of fragments to 16***

This flag is set to make the interface compatible with Cisco products. When set to **Yes**, a PPP packet is never fragmented into more than 16 smaller packets.

## Modifying a PPP Entity

The **pppmodify** command is used to modify the parameters of an existing PPP Entity. To modify a specific PPP Entity, for example Peer ID 1, enter the following command:

```
pppmodify p1
```

A screen similar to the following displays:

```

Modify PPP for communication to Peer ID: 1
Enter PPP parameters:
1) Description :
 {Enter text up to 30 characters}
2) Administrative Status Enabled
 {(E)nable, (D)isable}
3) PPP Mode Normal
 {(N)ormal, (M)ultilink}
4) Compression Type None
 {(N)one, STAC-(L)ZS}
5) Bridging Group 1
 {1-65535 or 0 if no Bridging}
50) Bridge Config Admin Status Enabled
 {(E)nabled, (D)isable}
51) PPP Bridging Mode Ethernet Only
 {Bridge (A)ll, (E)thernet Only}
6) Routing Group 2
 {1-65535 or 0 if no Routing}
60) IP Config Admin Status Enabled
 {(E)nabled, (D)isable}
61) Remote IP Address 0.0.0.0
 {IP address or 0.0.0.0 = learn, if IP enabled}
62) IPX Config Admin Status Disabled
 {(E)nable, (D)isable}
7) Authentication Type PAP
 {(N)one, (P)AP, (C)HAP}
70) User ID received from remote for Authentication ...
 {0 (No ID) to 8 ASCII characters}
71) Password received from remote for Authentication .
 {0 (No Password) to 8 ASCII characters}
72) User ID sent to remote for Authentication
 {0 (No ID) to 8 ASCII characters}
73) Password sent to remote for Authentication
 {0 (No Password) to 8 ASCII characters}
8) Max Failure Count 3
 {1..65535}
9) Max Configure Count 3
 {1..65535}
10) Max Terminate Count 5
 {1..65535}
11) Retry Timeout Value 5
 {Retry Timeout in Second(s) 1..65535}
12) Fragmentation Interleaving No
 {Fragmentation Interleaving Yes or No}
121) Fragmentation Delay 0
 {Fragmentation Delay in milliseconds(ms)}
122) Limit Maximum number of fragmentation to 16 No
 {(Y) meant cisco compatible. (N) meant native}
:

```

The fields on this screen are the same as those produced by the **pppadd** command. See *Adding a PPP Entity* on page 50-9 for descriptions of each of these fields.

Make the desired changes to any of the parameters, then enter the **save** command to implement the changes. You will then be returned to the system prompt.

## Viewing PPP Entity Configurations

The `pppview` command is used to view the configuration parameters of existing PPP Entities.

### Displaying the Configuration of All PPP Entities

To view configuration information on all PPP Entities, enter the following command:

```
pppview
```

A screen similar to the following displays:

PPP Configuration for Chassis:

| Peer ID | Admin Status | Mode      | Authentication | Compression | Bridging Group | Routing Group |
|---------|--------------|-----------|----------------|-------------|----------------|---------------|
| 1       | UP           | Normal    | None           | None        | 1              | 0             |
| 2       | DN           | Multilink | PAP            | STAC-LZS    | 1              | 2             |
| 3       | UP           | Normal    | CHAP           | None        | 0              | 2             |

The fields on this screen have the following meanings:

#### Peer ID

The number assigned to this PPP Entity when it was added. Used to identify a specific PPP Entity that you want to examine with the `pppview` or `pppstatus` commands.

#### Admin Status

Indicates the Administrative Status of this PPP Entity. **UP** means that this entity is enabled, or operative. **DN** means that this entity is disabled, or inoperative.

#### Mode

Indicates whether **Normal** or **Multilink** operation is used by this PPP Entity. Multilink operation is described under the heading *Multi-Link PPP* on page 50-2.

#### Authentication

Indicates the type of authentication used by this PPP Entity. The options are **None**, **PAP** and **CHAP**. These are two well-established standards currently used for PPP authentication.

#### Compression

Indicates the type of data compression configured to operate with this PPP Entity. The options are **None** or **STAC-LZS**. See *Data Compression* on page 50-2 for information on STAC-LZS compression.

#### Bridging Group

Indicates the VLAN Group to be used for PPP Bridging. A value of zero (0) indicates that this PPP Entity will not perform a bridging service and will discard all bridged format packets received or transmitted.

### Routing Group

Indicates the VLAN Group to be used for PPP Routing of the IP and IPX protocols. A value of zero (0) indicates that this PPP Entity will not perform a routing service and will discard all routed format packets received or transmitted.

### Displaying the Configuration of a Specific PPP Entity

To view configuration information on a *specific* PPP Entity, you must enter a Peer ID number with the **pppview** command. For example, to examine Peer ID 1, you would enter the following command:

```
pppview p1
```

A screen similar to the following displays:

```
View PPP configuration record for communication to Peer ID: 1
1) Description : Entry Peer ID 1
2) Administrative Status Enabled
3) PPP Mode Normal
4) Compression Type Disabled
5) Bridging Group 1
 50) Bridge Config Admin Status Enabled
 51) PPP Bridging Mode Ethernet Only
6) Routing Group 1
 60) IP Config Admin Status Enabled
 61) Remote IP Address 0.0.0.0
 62) IPX Config Admin Status Disabled
7) Authentication Type PAP
 70) User ID received from remote for Authentication ...
 71) Password received from remote for Authentication .
 72) User ID sent to remote for Authentication
 73) Password sent to remote for Authentication
8) Max Failure Count 3
9) Max Configure Count 3
10) Max Terminate Count..... 3
11) Retry Timeout Value..... 5
12) Fragmentation Interleaving No
 {Fragmentation Interleaving Yes or No
 121) Fragmentation Delay 0
 {Fragmentation Delay in milliseconds(ms)}
 122) Limit Maximum number of fragmentation to 16 No
 {(Y) meant cisco compatible. (N) meant native}
```

The fields on this screen are similar to those produced by the **pppadd** command. A few differences are noted in the descriptions that are given below. Note that you cannot make changes to the parameters on this screen. To do so, you must use the **pppmodify** command instead (see *Modifying a PPP Entity* on page 50-14 for complete information).

## Displaying PPP Entity Status

The `pppstatus` command is used to view the operational status of one or more PPP Entities.

### Displaying the Status of All PPP Entities

To view the operational status of *all* PPP Entities, enter the following command:

```
pppstatus
```

A screen similar to the following displays:

| Peer ID | Admin State | Mode      | IP Oper State | IPX Oper State | BCP Oper State | CCP Oper State |
|---------|-------------|-----------|---------------|----------------|----------------|----------------|
| 1       | UP/UP       | Normal    | Open          | Close          | Open           | Open           |
| 2       | UP/UP       | Multilink | Open          | Open           | Open           | Open           |

The fields on this screen have the following meanings:

#### Peer ID

The number assigned to this PPP peer.

#### Admin State

Indicates the Administrative Status of this PPP Entity. **UP** means that this entity is enabled, or operative. **DN** means that this entity is disabled, or inoperative.

#### Mode

Indicates whether **Normal** or **Multilink** operation is used by this PPP Entity. Multilink operation is described under the heading *Multi-Link PPP* on page 50-2.

#### IP Oper State

Indicates the operational state of the IP Routing option. **Open** means that IP has successfully negotiated a connection and is able to pass IP packets. **Closed** means that IP has not yet reached the open state, and is therefore unable to pass IP packets. The reasons why the state may be closed are: 1) the call has been disconnected, 2) the protocol is in the process of making a connection, or 3) the IP Routing option was not configured.

#### IPX Oper State

Indicates the operational state of the IPX Routing option. **Open** means that IPX has successfully negotiated a connection and is able to pass IPX packets. **Closed** means that IPX has not yet reached the open state, and is therefore unable to pass IPX packets. The reasons why the state may be closed are: 1) the call has been disconnected, 2) the protocol is in the process of making a connection, or 3) the IPX Routing option was not configured.

### BCP Oper State

Indicates the operational state of the Bridging Control Protocol option. **Open** means that the bridging operation is active. **Closed** means that the bridging operation has not yet reached the open state. The reasons why the state may be closed are: 1) the call has been disconnected, 2) the protocol is in the process of making a connection, or 3) the Bridging option was not configured.

### CCP Oper State

The operational state of the compression control protocol option. **Open** means that compression is active. **Closed** means that compression has not reached the open state. The reasons why the state may be closed are: 1) the call has been disconnected, 2) the protocol is in the process of making a connection, or 3) the compression option was not configured.

## Displaying the Status of a Specific PPP Entity

To view both the operational status and the relevant statistics of a specific PPP Entity, for example, Peer ID 1, enter the following command:

```
pppstatus p1
```

A screen similar to the following displays:

```

PPP statistics for Peer ID: 2
Admin IP IPX BCP CCP
State Mode Oper Oper Oper Oper
===== =====
UP Normal Open Close Open Close

LCP Pkts IPCP Pkts IPCP Pkts BCP Pkts CCP Pkts
IN/OUT IN/OUT IN/OUT IN/OUT IN/OUT
===== =====
3/4 2/2 0/0 4/4 0/0

 Packets Packets Packets Octets Octets
 In Out In+Out In Out %In %Out
 ===== ===== ===== ===== ===== =====
Total 2232 1475 3707 91751 66034
Ethernet 0 146 146 0 13413 0 20
8025 0 0 0 0 0 0 0
FDDI 0 0 0 0 0 0 0
IP 79 158 237 7784 6952 8 10
IPX 0 0 0 0 0 0 0
BPDU 2153 1171 3324 83967 45669 91 69

STAC-LZS Compressed Compressed Uncompressed Compression
Compression Frames Octets Octets Ratio
 ===== ===== ===== =====
In 0 0 0 0.0:1
Out 0 0 0 0.0:1
IN+Out 0 0 0 0.0:1

```

The additional fields produced by the **pppstatus** command when a specific Peer ID is entered with the command are as follows:

### LCP Pkts IN/OUT

The total number of Link Control Protocol (LCP) packets received (**In**) and transmitted (**Out**) on this PPP connection.

**IPCP Pkts IN/OUT**

The total number of IP Control Protocol (IPCP) packets received (**In**) and transmitted (**Out**) on this PPP connection.

**IPCP Pkts IN/OUT**

The total number of IP Control Protocol (IPCP) packets received (**In**) and transmitted (**Out**) on this PPP connection.

**BCP Pkts IN/OUT**

The total number of BCP packets received (**In**) and transmitted (**Out**) for this PPP connection.

**CCP Pkts IN/OUT**

The total number of CCP packets received (**In**) and transmitted (**Out**) for this PPP connection.

Also shown on this screen are two tables of statistics. The first table shows various data transmission statistics shown both as a total and sorted by the type of frame encapsulation being used (**Total**, **Ethernet**, **8025**, **FDDI**, **IP**, **IPX**, and **BPDU**). The columns in the first table show the following information for each type of frame encapsulation: the number of packets received (**Packets In**), the number of packets transmitted (**Packets Out**), the sum of received and transmitted packets (**Packets In+Out**), the number of octets received (**Octets In**), the number of octets transmitted (**Octets Out**), and the percentages received (**%In**) and transmitted (**%Out**) for each type of frame encapsulation.

The second table shows statistics related to the performance of STAC-LZS compression sorted by **In**, **Out**, and **In+Out** categories. The column headings show the number of compressed frames and octets, the number of uncompressed frames and octets, and the overall compression ratio represented by the previous figures.

# Deleting a PPP Entity

The **pppdelete** command is used to delete an existing PPP Entity.

1. Before you can delete a PPP Entity, you must first delete all the links associated with it. You do so using the **linkdelete** command (see Chapter 51 titled “WAN Links”). If you try to delete a PPP Entity that still has links associated with it, the following message will be displayed:

```
Delete PPP Peer ID: 1 aborted because the following link(s) attach to it.
Link Index: 1, Description: Link Entry: 1, Peer ID: 1
```

2. To delete a specific PPP Entity (after deleting all links associated with it), enter the Peer ID number along with the **pppdelete** command. For example, to delete Peer ID 2, enter the following command:

```
pppdelete p2
```

A screen similar to the following displays:

```
This will delete the configuration for PPP Peer ID: 2
Continue ? {(Y)es, (N)o} : N
```

3. To delete this entity, enter **y** and press **Enter**. If you decide to cancel out of the deletion, press **Enter** to accept the default answer of No. The system prompt will reappear.

# 51 WAN Links

## Introduction

This chapter describes the procedures for configuring a “WAN link” between an already created PPP Entity (see Chapter 50, *Point-to-Point Protocol*) and the physical interface that will be used to carry PPP traffic. The procedures described in this chapter comprise the third and final step in the three-step process for configuring the operation of PPP on your OmniSwitch (the complete three-step process was also described in Chapter 50).

Here is a brief review of the PPP configuration process: the first step is to configure the physical interfaces that will carry PPP traffic. The second step is to configure the operation of PPP itself by creating “PPP Entities.” The third step is to configure the “link” between an existing PPP Entity and the physical interface that will be used to carry PPP traffic (hence the name “WAN Links”).

## Configuring WAN Interfaces

Three kinds of physical WAN interfaces can support PPP connections: serial ports (WSM-S), T1/E1 channels (WSM-FT1/E1), and ISDN lines (WSM-BRI). The “WAN Links” you create to support PPP connections vary somewhat, depending upon the type of physical interface being used. When the physical interface being used is a Universal Serial Port (USP) or a fractional T1/E1 channel (which are permanent channels), the port is dedicated to the PPP connection and the “WAN Link” simply identifies the physical interface in terms of the slot and port. When the physical interface being used is an ISDN interface (which provides dynamic, switched connections), the “WAN Link” identifies the numbering information that is to be used to establish the serial connection and the slot/port if necessary.

### Related Hardware Chapters

The configuration of an ISDN interface is described in Chapter 52, *Managing ISDN Ports*. The configuration of a T1/E1 interface is described in Chapter 53, *Managing T1 and E1 Ports*. The configuration of a universal serial port (USP) on a WSM-S board is described in Chapter 48, *Managing WAN Switching Modules*. The ISDN WSM board (WSM-BRI) also contains a USP; this port on the WSM-BRI board may be configured in a similar manner to the USP ports on the WSM-S board.

## The Link Submenu

The WAN menu contains a submenu named **link** which contains commands for creating the WAN Links needed to support the Point-to-Point Protocol (PPP) over various hardware interfaces. WAN links can either be “fixed” (i.e., configured for a serial port or T1/E1 port), or dial-based (i.e., configured for an ISDN port). The link UI commands also provide a means of modifying and viewing existing WAN Links and displaying their operational status.

To switch to, and to display, the **link** menu, enter the following commands:

```
link
?
```

A screen similar to the following displays:

| <b>Command</b>    | <b>Link Menu</b>                                   |
|-------------------|----------------------------------------------------|
| <b>linkadd</b>    | <b>Add a Link configuration entry</b>              |
| <b>linkmodify</b> | <b>Modify an existing Link configuration entry</b> |
| <b>linkdelete</b> | <b>Delete an existing Link configuration entry</b> |
| <b>linkview</b>   | <b>View configuration of WAN Link(s)</b>           |
| <b>linkstatus</b> | <b>Status of WAN Link(s)</b>                       |

|                  |                 |                |                 |                   |
|------------------|-----------------|----------------|-----------------|-------------------|
| <b>Main</b>      | <b>File</b>     | <b>Summary</b> | <b>VLAN</b>     | <b>Networking</b> |
| <b>Interface</b> | <b>Security</b> | <b>System</b>  | <b>Services</b> | <b>Help</b>       |

Each of the commands on this menu is described in the following sections.

## Adding a WAN Link

The **linkadd** command is used to add link configuration records, or “WAN Links” to the switch. This command defaults to a WSM physical port (serial or Fractional T1/E1). When the **linkadd** command is used to create links over WSM ports, all of the parameters needed to create the link are contained on one screen. However, when you select to create a link over an ISDN port, a second screen will be displayed after you enter and save the initial parameters on the first screen.

The first subheading (*Adding WSM Port Links*) below shows the sequence of screens when creating a link over a WSM port. The second subheading below (*Adding ISDN Call Links* on page 51-4) shows the sequence of screens when creating a link over an ISDN port.

### Adding WSM Port Links

1. To add a link over a WSM port, you must enter a Peer ID number (associated with a “PPP Entity”) with the command. See Chapter 50, *Point-to-Point Protocol*, for details on creating Peer IDs.

For example, to create a link for Peer ID 1, enter the following command (where **p1** is the Peer ID number):

```
linkadd p1
```

A screen similar to the following displays:

```
Adding Link for Peer ID 1, Link Index 1:
```

- ```

1) Description : Link Entry: 2, Peer ID: 1
   {Enter text up to 31 characters}
2) Administrative Status ..... = Enabled
   {(E)nabled, (D)isabled}
3) Link Type..... = WSM Port
   {(W)SM Port, (I)SDN call}
4) Link Slot..... = 0
   {Slot number or 0 if not tied to a slot}
5) Link Port ..... = 0
   {Port number or 0 if not tied to a port}

```

```
(save/quit/cancel)
```

```
:
```

To alter a parameter, enter the line number for the parameter, followed by an equal sign (=), then the new value. For example, to change the **Link Type** (line 3) from WSM Port to ISDN call, you would enter:

```
3=I
```

When you have completed configuring parameters, enter **save**. Your new values will be saved and you will exit this menu. If you want to exit this menu without saving changes, simply enter **quit** or **cancel**.

The fields on this screen have the following meanings:

Description

A textual description used to identify this WAN Link. The default text indicates the link entry number and the Peer ID number.

Administrative Status

Sets the Administrative Status of this WAN Link. The options are “**Enabled**,” which will enable this link and “**Disabled**,” which will disable the link but not delete it.

Link Type

Specifies the type of physical connection that will carry the link. The options are “**WSM Port**,” which means a serial or Fractional T1/E1 connection and “**ISDN**,” which means an ISDN call will be used to make the connection.

Link Slot

Specifies the switch slot number to be used by this WAN Link.

Link Port

Specifies the switch port number to be used by this WAN Link.

2. To make a change to the values for any of the fields on this screen, enter the field's line number followed by the desired value.
3. To add the link for a WSM port, you must specify which switch port and slot is to be used. To do so, you must make changes to the values for items 4 and 5. For example, if your WSM port is in slot 5, port 2, you would enter the following three commands:

```
: 4=5
: 5=2
: save
```

After entering the **save** command, you will be returned to the system prompt.

Adding ISDN Call Links

1. To create a link over ISDN, you must enter a Peer ID number (associated with a “PPP Entity”) with the command. See Chapter 50, *Point-to-Point Protocol*, for details on creating Peer IDs.

For example, to create a link for Peer ID 1, you would enter the following command (where **p1** is the Peer ID number):

```
linkadd p1
```

A screen similar to the following displays:

```
Adding Link for Peer ID 1, Link Index 1:
```

- 1) **Description : Link Entry: 2, Peer ID: 1**
{Enter text up to 31 characters}
- 2) **Administrative Status** = Enabled
{(E)nabled, (D)isabled}
- 3) **Link Type** = WSM Port
{(W)SM Port, (I)SDN call}
- 4) **Link Slot** = 0
{Slot number or 0 if not tied to a slot}
- 5) **Link Port** = 0
{Port number or 0 if not tied to a port}

```
(save/quit/cancel)
:
```

- You must now change the Link Type to ISDN. To do so, enter the following commands:

```
: 3=l
: ?
```

A screen similar to the following displays:

```
1) Link Description :
   {Enter text up to 31 characters}
2) Link Administrative Status ..... = Enabled
   {(E)nabled, (D)isabled}
3) Link Type..... = ISDN Call
   {(W)SM Port, (I)SDN call}
4) Link Slot..... =
   {Slot number or 0 if not tied to a slot}
5) Link Port ..... =
   {Port number or 0 if not tied to a port}

(save/quit/cancel)
:
```

- You must now enter the ISDN slot and port numbers that will be used by this WAN Link. For example, to use slot 4, port 2, you would enter the following commands:

```
: 4=4
: 5=2
```

Note

Incoming and backup ISDN calls may dynamically select and use any available slot and port. However, you *must* specify an ISDN slot and port for the link when you first create its WAN Link.

A screen similar to the following displays:

```
Modify ISDN call record configuration. Peer ID: 1 Link Index: 1
Type: ISDN Call Slot: 4 Port: 2

1) Link Description : Link Entry: 1, Peer ID: 1
   {Enter text up to 30 characters}
2) Link Administrative Status ..... = Enabled
   {(E)nabled, (D)isabled}
3) Inactivity Timer ..... = 0
   {1-9999 seconds or 0 if disabled}
4) Minimum call duration ..... = 0
   {1-9999 seconds or 0 if disabled}
5) Maximum call duration ..... = 0
   {1-9999 seconds or 0 if disabled}
6) Outgoing Calls ..... = Enabled
   {Enable, Disable}
   60) Call Originate Mode ..... = On-Demand
      {(O)n-Demand or (B)ackup}
   61) Carrier Delay Timeout ..... = 0
      {Call completion timeout 1-999 seconds}
   62) Maximum Call Retries ..... = 1
      {Retry call count, 0 if infinite}
   63) Retry Delay ..... = 0
      {Seconds between retry attempts, 0 = retry immediately}
   64) Failure Delay ..... = 0
      {Secs after max calls failed to retry,
       0 = don't retry after max calls failed}
   65) Remote Phone Number ..... =
      {digits 0 through 9}
   66) Desired Calling Speed ..... = 64000
      {56000, 64000}
7) Incoming calls ..... = Enabled
   {Enabled, Disabled}

(save/quit/cancel)
:
```

The fields on this screen have the following meanings:

Link Description

A textual description used to identify this WAN Link.

Link Administrative Status

Sets the Administrative Status of this WAN Link. The options are “**Enabled**,” which will allow the link to operate and “**Disabled**,” which will disable the link without deleting it.

Inactivity Timer

Sets the time period (in seconds) after which the connection will be terminated if it is not carrying useful data. “Useful data” refers to forwarding packets (routing information), but not to encapsulator maintenance frames. An entry of zero (0) specifies no disconnection due to inactivity. The Inactivity Timer is disabled for outgoing backup calls, and should be disabled by the user for incoming calls that are used to backup.

Minimum Call Duration

The minimum duration of a call, in seconds, starting from the time the call is connected until the call is disconnected. If you enable this field by entering a nonzero value, the Inactivity Timer will be disabled until the time set in the Minimum Call Duration field has passed.

Maximum Call Duration

The maximum call duration in seconds. An entry of zero (0) means “unlimited.”

Outgoing Calls

Sets whether outgoing calls can be made by this WAN Link. The option “**Enabled**” will allow the link to make outgoing calls while “**Disabled**” will not allow the link to make outgoing calls. These suboptions further specify the details of the outgoing calls:

Call Originate Mode

Specifies whether the call is to be initiated on demand or only when operating as a backup to another link.

Carrier Delay Timeout

The amount of time, in seconds, allowed for a call to be completed.

Maximum Call Retries

The number of calls to a non-responding address that may be made. An entry of zero (0) means there is no limit to the number of retries. The intent of this parameter is to limit the number of successive calls to an address which is inaccessible or which refuses those calls. Some countries regulate the number of call retries to a given peer that can be made.

Retry Delay

The time, in seconds, between call retries if a peer cannot be reached. An entry of zero (0) means that call retries may be done without any delay.

Failure Delay

The time, in seconds, after which call attempts are to be made again after a peer has been noticed to be unreachable (i.e., after the limit set in **Maximum Call Retries** has been reached). An entry of zero (0) means that a peer will not be called again after the maximum number of unsuccessful call attempts has been made.

Remote Phone Number

The phone number that is to be dialed in order to make the connection. Only one phone number can be associated with a single WAN Link. You can add other WAN Links if you want to use multiple phone numbers.

Desired Calling Speed

The desired calling speed. The options are 56000 and 64000 bits/second. You should set this parameter to the maximum speed supported by the telephone switch to which you will be connecting.

Incoming Calls

Sets whether incoming calls are to be accepted by this WAN Link. “**Enabled**” will allow the link to accept calls. “**Disabled**” will not allow the link to accept calls.

4. You must now enter a value in at least the **Remote Phone Number** field under **Outgoing Calls**. If you do not make an entry in this field, an error will be returned by the system when you attempt to save and exit the screen.

You can also make changes to any of the other fields on this screen if they are needed to provide ISDN call information this WAN Link. The default settings should suit many situations; however, you will need to determine what information will be needed to support your ISDN calls and make the appropriate entries in the fields on this screen.

5. Enter the **save** command when you are ready to create the WAN Link.
The system prompt will then reappear.

Modifying a WAN Link

The **linkmodify** command is used to modify the parameters of an existing WAN Link. Different parameters will be displayed by the command based on the type of link. The first subheading (*Modifying ISDN Links*) below shows the sequence of screens when modifying a link over a WSM port. The second subheading below (*Modifying WSM Links* on page 51-10) shows the sequence of screens when modifying a link over an ISDN port.

Note

The Slot and Port fields in an existing WAN Link record cannot be modified. To change them, you must delete the record then create a new record.

Modifying ISDN Links

- To modify a WAN Link, you must enter its Link Index with the command. For example, to modify Link Index 1 which uses ISDN, you would enter the following command:

```
linkmodify L1
```

A screen similar to the following displays:

```
Modify ISDN call record configuration. Peer ID: 1 Link Index: 1
Type: ISDN Call Slot: 5 Port: 1

1) Link Description : Link Entry: 1, Peer ID: 1
   {Enter text up to 30 characters}
2) Link Administrative Status ..... = Enabled
   {(E)nabled, (D)isabled}
3) Inactivity Timer ..... = 30
   {1-9999 seconds or 0 if disabled}
4) Minimum call duration ..... = 0
   {1-9999 seconds or 0 if disabled}
5) Maximum call duration ..... = 0
   {1-9999 seconds}
6) Outgoing Calls ..... = Enabled
   {Enable, Disable}
60) Call Originate Mode ..... = On-Demand
    (O)n-Demand or (B)ackup}
61) Carrier Delay Timeout ..... = 0
    {Call completion timeout 1-999 seconds}
62) Maximum Call Retries ..... = 0
    {Retry call count, 0 if infinite}
63) Retry Delay ..... = 0
    {Seconds between retry attempts, 0 = retry immediately}
64) Failure Delay ..... = 0
    {Secs after max calls failed to retry,
     0 = don't retry after max calls failed}
65) Remote Phone Number ..... =
    {digits 0 through 9}
66) Desired Calling Speed ..... = 64000
    {56000, 64000}
7) Incoming calls ..... = Enabled
   {Enabled, Disabled}

(save/quit/cancel)
:
```

The fields on this screen are the same as those produced by the **linkadd** command. See *Adding a WAN Link* on page 51-3 for descriptions of each of these fields.

2. Make the desired changes to each of the fields on this screen, then enter the **save** command to implement your changes.

The system prompt will then reappear.

Modifying WSM Links

1. To modify a WAN Link, you must enter its Link Index with the command. For example, to modify Link Index 2 which uses a WSM physical port (serial or Fractional T1/E1), you would enter the following command:

linkmodify L2

A screen similar to the following displays:

Modify Serial Port Link configuration. Peer ID: 2 Link Index: 2
Type: WSM port Slot: 5 Port: 1

- 1) **Link Description : Link Entry: 2, Peer ID: 2**
{Enter text up to 30 characters}
- 2) **Link Administrative Status = Enabled**
{(E)nabled, (D)isabled}

(save/quit/cancel)

:

The fields on this screen are the same as those produced by the **linkadd** command. See *Adding a WAN Link* on page 51-3 for descriptions of each of these fields.

2. Make the desired changes to the fields on this screen, then enter the **save** command to implement the changes.

The system prompt will then reappear.

Deleting WAN Links

The **linkdelete** command is used to delete one or more existing WAN Link records.

Note

Before you can delete a PPP Entity, you must first delete all WAN Links that have been associated with it. See *Deleting a PPP Entity* in Chapter 50 for complete information.

1. To delete an existing WAN Link, for example, Link Index 2, you would enter the following command:

```
linkdelete L2
```

A screen similar to the following displays:

```
This will delete the configuration for Link Peer ID: 3 Link Index: 2  
Continue ? {(Y)es, (N)o} : N
```

2. If you wish to delete this link, enter **y** and press **Enter**. If you wish to abort the deletion, just press **Enter** to accept the default answer of “No.”

The system prompt will then reappear.

Viewing WAN Links

The `linkview` command is used to view information on existing WAN Link records.

Displaying All Existing WAN Links

To view information on all existing WAN Links, enter the following command:

```
linkview
```

A screen similar to the following displays:

```
List of ISDN Port Type:
Peer Link  Link  Link  Link  Outgoing  Incoming  Peer  Inac.  Min/Max  Call
Id   Index Mode  Slot Port  Called Num. Caller Id.  Speed  Timer  Dur.    Retry
=====
   1    1  DEM   4    2    7145555555 8015551212 56000   0    0/0     0
   2    2  BKP   4    2    7145551212 8015555555 64000   0    0/0     0

List of WSM Port Type:
Peer Link  Link  Link
Id   Index Slot  Port
=====
   1    1    5    2
   2    2    5    4
```

The fields on this screen have the following meanings:

Peer ID

The number assigned to the PPP Entity that is related to this WAN Link. You assign this number when you create the PPP Entity (see Chapter 50, *Point-to-Point Protocol*, for more information on creating PPP Entities).

Link Index

The number assigned by the system to this WAN Link; used to identify the link in the table.

Link Mode

Indicates whether this WAN Link is on-demand (“DEM”) or back-up (“BKP”). On-demand links are brought up only when data is ready to be sent. Backup links are brought up when a primary link fails.

Link Slot

The number of the physical switch slot that is to be used for this connection.

Link Port

The number of the physical switch port that is to be used for this connection.

Outgoing Called Number

The phone number that is to be dialed in order to establish the connection.

Incoming Caller ID

The phone number reported by the Caller ID service, if available.

Peer Speed

The specified calling speed for this link. The options are 56000 and 64000 bits/second.

Inactivity Timer

Specifies the time period (in seconds) after which the connection will be terminated if it is not carrying useful data. "Useful data" refers to forwarding packets (routing information) but not encapsulator maintenance frames. Zero (0) specifies no disconnection due to inactivity.

Min/Max Duration

The minimum and maximum duration of a call, in seconds, starting from the time the call is connected until the call is disconnected. Zero (0) means "unlimited."

Call Retry

The number of calls that may be made to a non-responding address. A count of zero (0) means there is no limit to the number of call retries.

Displaying Information for a Specific WAN Link

To view detailed information on a *specific* WAN Link, you must enter its Link Index with the command. Different parameters will be displayed based on the type of link being used.

Example of an ISDN Link

To examine an ISDN link, for example, Link 1, you would enter following command:

```
linkview L1
```

A screen similar to the following displays:

```
View ISDN call record configuration. Peer ID: 1 Link Index: 1
Type: ISDN Call Slot: 5 Port: 2

1) Link Description :
2) Link Administrative Status ..... = Enabled
3) Inactivity Timer ..... = 30
4) Minimum call duration ..... = 0
5) Maximum call duration ..... = 0
6) Outgoing Calls ..... = Enabled
60) Call Originate Mode ..... = On-Demand
61) Carrier Delay Timeout ..... = 0
62) Maximum Call Retries ..... = 1
63) Retry Delay ..... = 0
64) Failure Delay ..... = 0
65) Remote Phone Number ..... = 7145551212
66) Desired Calling Speed ..... = 64000
7) Incoming calls ..... = Enabled
```

The fields on this screen provide the same information as those on the **linkadd** screen. See *Adding a WAN Link* on page 51-3 for descriptions of each of these fields.

Example of WSM Serial or T1/E1 Link

An example of a link over a WSM serial or Fractional T1/E1 port would look like this:

View ISDN Link configuration. Index: 2 Link Peer ID: 3
Type: WSM port Slot: 5 Port: 2

- 1) **Link Description : Link Entry: 1, Peer ID: 1**
{Enter text up to 31 characters}
- 2) **Link Administrative Status = Enabled**
{(E)nabled, (D)isabled}

The fields on this screen provide the same information as those on the **linkadd** screen. See *Adding a WAN Link* on page 51-3 for descriptions of each of these fields.

Displaying Link Status

The `linkstatus` command is used to display the operational status of WAN Links.

Displaying Status for All WAN Links

To view information on all WAN Links, enter the following command:

```
linkstatus
```

A screen similar to the following displays:

Link Idx	Peer Id	Slot/Port	Last Setup Time			
====	=====	=====	=====	=====	=====	=====
1	1	4/2	00:00:00	03/97		
2	2	4/2	00:00:00	03/97		

Active Session:						
Setup Time	Link Index	Peer Id	Peer Call Addr.	Conn. Time	Call St.	Call Org.
====	=====	=====	=====	=====	=====	=====
00:00	1	1	8188783500	00:00	CON	ANS
00:00	2	1	8188783500	00:00	CON	ANS

The fields on this screen have the following meanings:

Link Index

The number assigned to identify this WAN Link.

Peer ID

The number assigned to the PPP Entity that is related to a WAN Link (indicated by Link Index).

Slot/Port

The slot and port numbers associated with a given Link Index and Peer ID.

Last Setup Time

The value of "sysUpTime" (the time of day recorded by the switch) when the last call to this peer was started. For ISDN, this will be the time when the setup message was received from or sent to the network. This field will be updated whenever a call is started or answered.

Active Session

The following information is available for the active ISDN session, if one is in progress:

Setup Time

The value of "sysUpTime" (the time of day) when the call to this peer was started.

Peer Id

The Peer ID that is related to this active ISDN session.

Peer Call Address

The number to which this call is connected. Zero (0) means the number is not available.

Connection Time

The value of "sysUpTime" (the time of day) when the call was connected. Zero (0) means the call is not currently connected.

Call State

The current call state. The possible entries are **IDLE** (meaning there is no active call), **CONT** (meaning the call is in the process of connecting), **CONN** (meaning the call is connected), **ACTX** (meaning the call is active), **DISC** (meaning the call has been disconnected), and **UNKN** (meaning that the state is unknown).

Call Origination

The call origin. Possible entries are **OUTG** (meaning the call was outgoing) and **INCM** (meaning the call was incoming).

Displaying Status for a Specific WAN Link

To view detailed status information on a *specific* WAN Link, you must enter its Link Index with the command.

For example, to examine Link 1 (an ISDN link), you would enter following command:

```
linkstatus L1
```

A screen similar to the following displays:

```
Status for Link Index: 1
Connect Time ..... 0
Success Calls ..... 0
Failed Calls ..... 0
Accepted Calls ..... 0
Refused Calls ..... 0
Last Setup Time ..... 12:56:00 3/96
```

The fields on this screen have the following meanings:

Connect Time

Accumulated connect time to the peer since system start-up. This is the total connect time, i.e., the connect time for outgoing calls plus the time for incoming calls.

Success Calls

The number of completed calls to the Peer ID related to this WAN Link.

Failed Calls

The number of failed call attempts, or any reason, to the Peer ID related to this WAN Link since system start-up.

Accepted Calls

The number of calls from the Peer ID related to this WAN Link accepted since system start-up.

Refused Calls

The number of calls from the Peer ID that were refused, or any reason, since system start-up.

Last Setup Time

The value of “sysUpTime” (the time of day) when the last call to this peer was started. For ISDN, this will be the time when the setup message was received from or sent to the network. This field will be updated whenever a call is started or accepted.

52 Managing ISDN Ports

The WAN Switching Module for the Basic Rate Interface (WSM-BRI) supports 1 or 2 Universal Serial Ports (USP) and 1 or 2 ISDN Basic Rate Interfaces (BRI). The USPs can support Frame Relay or Point-to-Point Protocol (PPP). The BRI interface can support only PPP.

The Universal Serial Port on a WSM-BRI board is operationally identical to the USPs found on the 4- or 8-port WSM-S board. The ISDN BRI port is an RJ-45 connector. The BRI port can be configured either as a “U” interface for the North American market or as an “S/T” interface for international markets. The WSM-BRI board also supports hardware data compression via the STAC 9705 Data Compression Coprocessor.

The ISDN BRI interface supports switched connections, usually through a central office switch. Connections can be established when data is available for a remote peer, referred to as “demand” mode, or when a primary circuit is inactive, referred to as “backup” mode.

Overview of ISDN

Integrated Services Digital Network (ISDN) is a switched network that incorporates a digital connection to the central office (the local loop), instead of the current telephone network’s analog connection. Because the worldwide telephone network is becoming increasingly digital in the trunks between switching centers, the incorporation of ISDN allows for end-to-end switched digital connections. In general, there are three main goals for ISDN:

- provide end-to-end digital connectivity
- support a wide range of services, both voice and non-voice
- access the ISDN by a limited set of standard user-to-network interfaces

Basic Rate Interface (BRI) Versus Primary Rate Interface (PRI)

There are two methods defined for accessing ISDN. The Basic Rate Access (BRA) method, commonly known as the Basic Rate Interface (BRI), was intended for residential subscribers and small offices. The Primary Rate Access (PRA) method, commonly known as the Primary Rate Interface (PRI), was intended for users with greater data-transfer capacity requirements, such as offices with a digital PBX. The OmniSwitch WSM-BRI board supports only the BRI interface. Future products may be introduced that include support for PRI interfaces.

The WSM-BRI interface terminates at an ISDN-capable switch in the central telephone office. In order to perform properly, the WSM-BRI board must know to which type of telephone switch it is being connected. You must provide your OmniSwitch with this information during configuration of the WSM-BRI board. Also, depending upon the type of telephone switch you will be accessing, you may need to obtain from the telephone company a Service Profile Identification (SPID). The SPID is used in North America for DMS100, ATT 5ESS and Nation ISDN 1switch types.

“U”, “S/T”, and “R” Interfaces

The ISDN specification defines a limited set of user-to-network interfaces, including reference points for the BRI access method. The following are the main BRI reference points:

U Interface. The U interface is a two-wire (single pair) interface that supports full-duplex data transfer from the phone switch. Only a single device can be connected to a U interface. This device is called a Network Termination 1 (NT1) which converts the U interface to the S/T interface (described below). The U interface is used in North America. Elsewhere in the world, telephone companies supply the NT1 service, allowing customers the use of S/T interfaces.

S/T Interface. The S/T interface is a four-wire, bus interface on which multiple (up to eight) ISDN access devices can be attached to gain shared access to ISDN's data channels. The S/T interface is the most commonly-used interface in Europe.

R Interface. The R interface is a general reference point at which non-ISDN devices can gain access to an ISDN network through a device called a Terminal Adapter (TA). A Terminal Adapter typically converts various standard interfaces, such as RS232 and V.35, to the S/T bus.

The “B,” “D,” and “H” Channels

ISDN supports three types of data channels: the “B” channel, the “D” channel and the “H” channel. The line encoding and framing structure for each type of channel varies among the U, S/T, and R interfaces and for different access methods. A brief description of the three channels follows:

B Channel. The B channel is used for the transfer of information, which can be any type of data that the endpoints agree on, such as digitized voice, digitized video or packet data. The B channel operates at 64 kbps on both BRI and PRI interfaces, but is commonly rate-adapted to 56 kbps in North America to accommodate switching system limitations. A single BRI interface consists of one D channel operating at 16 kbps and two B channels operating at 64 kbps (or 56 kbps in North America).

D Channel. The D channel operates at 16 kbps on BRI (64 kbps on PRI) and is used for carrying common-channel signaling. The D channel is used both to establish and maintain circuit-switched calls on the B channels. The D channel can also be used to carry low-speed packet-switched data (the OmniSwitch does *not* support such usage).

H Channel. The H channel, supported *only* on PRI interfaces, is used to transfer information at higher bit rates by aggregating B channels. The four implementations of the H channel are: H0 (384 kbps, 6 B channels), H10 (1472 kbps, 23 B channels), H11 (1536 kbps, 24 B channels), and H12 (1920 kbps, 30 B channels). The use of the H channel is *not* supported by the OmniSwitch because this channel requires a PRI interface.

The ISDN Submenu

The WAN menu contains a submenu, **ISDN**, containing commands specific to WSM-BRI ISDN ports.

To switch to, and to display, the **ISDN** menu, enter the following commands:

```
ISDN
?
```

A screen similar to the following displays:

Command	ISDN Menu
isdnm	Modify an existing ISDN port's configuration
isdnd	Delete an existing ISDN configuration entry
isdnv	View an existing ISDN configuration entry
isdns	Status for the ISDN configuration entry
Main	File
Interface	Security
	Summary
	System
	VLAN
	Services
	Networking
	Help

Switch Configuration

This section describes how to configure the ISDN ports on WSM-BRI boards. You use the **isdnm** command to modify the configuration of an ISDN port. You must select the correct type of telephone switch to which you will be making your ISDN calls, as well as supply signalling calling addresses (phone numbers) and SPIDS, if required. Configuration is described in the next section, *Modifying an ISDN Configuration Entry* on page 52-4.

The other commands on the ISDN submenu are described in the remaining sections of this chapter.

Modifying an ISDN Configuration Entry

The **isdnm** command is used to modify the parameters for a selected ISDN port. These parameters are typically provided by the telephone carrier or other service provider at the time the ISDN line is installed.

1. To modify a specific port, for example in Slot 4, Port 1, enter the following command:

```
isdnm 4/1
```

A screen similar to the following displays:

```
1)  Switch Type ..... ETSI
    {5(ES)S, (D)MS100, (NI)1, (ET)SI}
2)  B1 Signalling Calling Address..... 8185551212
    {Phone Number}
3)  B1 Service Profile Identifier (SPID) ..... 123456789
    {9-20 Numeric characters}
4)  B2 Signalling Calling Address..... 7145551212
    {Phone Number}
5)  B2 Service Profile Identifier (SPID) ..... 123456789
    {9-20 Numeric characters}
```

```
(save/quit/cancel)
:
```

The fields on this screen have the following meanings:

Switch Type

Specifies the type of switch to which this ISDN port is to be connected. The options are: AT&T 5ESS (**5ESS**), Northern Telecom DMS100 (**DMS100**), National ISDN-1 Bellcore (**NI1**), and Euro-ISDN ETS 300/British Telecom NET3 (**ETSI**).

B1/B2 Signalling Calling Address

The number assigned to this channel by the carrier. If only one address is supplied by the carrier, assign it to channel B1, and leave channel B2 empty.

B1/B2 Service Profile Identifier (SPID)

The Service Profile Identifier assigned to this channel by the carrier. Normally, this value contains the calling address surrounded by some digits. If only one address is supplied by the carrier, assign it to channel B1, and leave channel B2 empty.

Important Note

When changing the **Switch Type** or adding/deleting **SPIDs**, reboot the switch to implement the changes.

Deleting an ISDN Configuration Entry

The **isdnd** command is used to delete one or more ISDN configuration entries. Deleting the configuration entry is equivalent to returning the ISDN port to its default settings. Although you cannot delete a physical ISDN port from the switch, you can remove the configuration entry that was recorded for a port.

1. To delete a specific ISDN entry, for example, for a board in slot/port 2/2, you would enter the following command:

```
isdnd 2/2
```

A screen similar to the following displays:

```
This will delete Slot 2, Port 2.  
Continue ? {(Y)es, (N)o} : N
```

2. To delete this entry, enter **y** and press **Enter**. To abort the deletion, press **Enter** to accept the default answer of “No.” The system prompt will then reappear.

Important Note

After deleting an ISDN configuration entry, you should reboot the switch to implement any configuration changes you make using the **isdnm** command.

Viewing an ISDN Configuration Entry

The `isdnv` command is used to view the configuration of existing ISDN configuration entries. You can either view a configuration summary for all ISDN ports on a specified slot, or display the configuration for a single ISDN port.

To view configuration information on all ISDN ports on a specific slot, for example, slot 4, enter the following command:

```
isdnv 4
```

A screen similar to the following displays:

```
View ISDN Configuration for Slot: 4, Port: 2.
1) Switch Type ..... ETSI
2) B1 Signalling Calling Address. ....
3) B1 Service Profile Identifier (SPID) .....
4) B2 Signalling Calling Address. ....
5) B2 Service Profile Identifier (SPID) .....

View ISDN Configuration for Slot: 4, Port: 4.
1) Switch Type ..... ETSI
2) B1 Signalling Calling Address. ....
3) B1 Service Profile Identifier (SPID) .....
4) B2 Signalling Calling Address. ....
5) B2 Service Profile Identifier (SPID) .....
```

To view information on a specific ISDN port and slot, for example, slot 4, port 4, enter the following command:

```
isdnv 4/4
```

A screen similar to the following displays:

```
View ISDN Configuration for Slot: 4, Port: 4.
1) Switch Type ..... ETSI
2) B1 Signalling Calling Address. ....
3) B1 Service Profile Identifier (SPID) .....
4) B2 Signalling Calling Address. ....
5) B2 Service Profile Identifier (SPID) .....
```

The fields on this screen are the same as those produced by the `isdnm` command:

Switch Type

Specifies the type of switch to which this ISDN port is to be connected. The options are: AT&T 5ESS (**5ESS**), Northern Telecom DMS100 (**DMS100**), National ISDN-1 Bellcore (**NI1**), and Euro-ISDN ETS 300/British Telecom NET3 (**ETSI**).

B1/B2 Signalling Calling Address

The number assigned to this channel by the carrier. If only one address is supplied by the carrier, it should be assigned to channel B1, and channel B2 should be left empty.

B1/B2 Service Profile Identifier (SPID)

The Service Profile Identifier assigned to this channel by the carrier. Normally, this value contains the calling address surrounded by some digits. If only one address is supplied by the carrier, it should be assigned to channel B1, and channel B2 should be left empty.

Displaying ISDN Configuration Entry Status

The `isdns` command is used to view the operational status of existing ISDN configuration entries. You can select to view the status of all ISDN ports, or select to display the status of a single ISDN port.

Displaying Status of All ISDN Ports

To view status information of the ISDN channels on all ISDN ports, enter the following command:

```
isdns
```

A screen similar to the following displays:

Slot/Port	Type	Oper Status	Call Address	Call Setup Time
=====	=====	=====	=====	=====
5/2(B1)	BRI-U	ACTIVE	7145555555	00:00:00 01/70
5/2(B2)	BRI-U	IDLE	7145555555	00:00:00 01/70
5/4(B1)	BRI-U	ACTIVE	7145555555	00:00:00 01/70
5/4(B2)	BRI-U	ACTIVE	7145555555	00:00:00 01/70

The fields on this screen have the following meanings:

Slot/Port

Identifies the ISDN port and slot numbers and the “B” channel number (in parentheses).

Type

Identifies the type of ISDN port (BRI-U or BRI-S/T). See *Overview of ISDN* on page 52-1.

Operational Status

Identifies the operational status of this port. The possible entries in the table are **Active**, meaning the call is currently in progress, or **Idle**, meaning the interface is currently idle.

Call Address

Identifies the current or last phone number that was called on this ISDN channel.

Call Setup Time

Identifies the value of “sysUpTime” (the time of day recorded by the switch) and the date (in *dd/yy* format) when the last call was established on this channel.

Displaying Status of a Specific ISDN Slot

To view status information on all ISDN channels on a specific ISDN slot, for example, slot 4, enter the following command:

```
isdns 4
```

A screen similar to the following displays:

```
Status for ISDN D channel on slot: 4, Port: 1:  
LAPD OperStatus: Layer 1: Active, Layer 2 DataLink: Established.
```

```
The number of incoming calls . . . . . 0  
The number of incoming calls which were actually connected . . . 0  
The number of outgoing calls . . . . . 0  
The number of outgoing calls which were actually connected . . . 0
```

	Oper Status	Peer Address	Call Origin	Call SetupTime
	=====	=====	=====	=====
B1	Idle	7144509154	Incoming	0:00:00 01/70
B2	Conn	7144509156	Outgoing	0:00:00 01/70

```
Status for ISDN D channel on slot: 4, Port: 2:  
LAPD OperStatus: Layer 1: Active, Layer 2 DataLink: Established.
```

```
The number of incoming calls . . . . . 0  
The number of incoming calls which were actually connected . . . 0  
The number of outgoing calls . . . . . 0  
The number of outgoing calls which were actually connected . . . 0
```

	Oper Status	Peer Address	Call Origin	Call Setup Time
	=====	=====	=====	=====
B1	Idle	7144509154	Incoming	0:00:00 01/70
B2	Conn	7144509156	Outgoing	0:00:00 01/70

The fields on this screen have the following meanings:

The number of incoming calls

Indicates the number of incoming calls received on this interface.

The number of incoming calls which were actually connected

Indicates the number of incoming calls which were actually connected on this interface. The difference between the previous field and this one is the number of calls that were refused.

The number of outgoing calls

Indicates the number of outgoing calls made on this interface.

The number of outgoing calls which were actually connected

Indicates the number of outgoing calls which were actually connected on this interface. The difference between the value of the previous entry and this one is the number of calls that failed.

Oper Status

Indicates the current call control state for this interface. The possible entries are:

- Idle** means the B Channel is idle: no call or call attempt is in progress.
- Connecting** means a connection attempt (outgoing call) is being made.
- Connected** means an incoming call is currently in the process of validation.
- Active** means a call is currently active.

Peer Address

Indicates the ISDN address to which the current or last call is or was connected. In some cases, the format of this information cannot be predicted since it largely depends on the type of switch or PBX to which the device is connected. The switch software supports the display of IA5 ASCII digits and the pound key (0-9 and #), but no space characters.

Call Origin

Indicates whether this call was answered on this channel (denoted as “**Incoming**”) or was originated by this channel (denoted as “**Outgoing**”).

Call Setup Time

Indicates the value of “sysUpTime” (the time of day recorded by the switch) when the ISDN setup message for the current or last call was sent or received. If, since system start-up, there has been no call on this interface, this field will display all zeros.

Displaying Status of a Specific ISDN Port

To view status information of the ISDN channels on a specific ISDN port, for example port 4, slot 1, enter the following command:

`isdns 4/1`

A screen similar to the following displays:

```

Status for ISDN D channel on slot: 4, Port: 1:
LAPD OperStatus: Layer 1: Active, Layer 2 DataLink: Established.

The number of incoming calls ..... 0
The number of incoming calls which were actually connected . . . 0
The number of outgoing calls ..... 0
The number of outgoing calls which were actually connected . . . 0

      Oper   Peer       Call       Call
      Status Address   Origin    SetupTime
      =====
B1 Idle   7144509154 Incoming  0:00:00 01/70
B2 Conn  7144509156 Outgoing  0:00:00 01/70
    
```

The fields on this screen were described earlier in this section (see *Displaying Status of a Specific ISDN Slot* on page 52-8).

53 Managing T1 and E1 Ports

T1 and E1 ports are supported on a variety of switching modules. In the OmniSwitch, T1 and E1 are used as standard WAN access ports, ATM cell switching ports, and circuit emulations ports. The following switching modules contain T1 or E1 ports:

- ASM-CE
- CSM-CE-T1/E1
- CSM-DS1/E1
- CSM-AB-IMA-DS1/E1
- WSM-FT1/E1
- WSX-FT1/E1

Ports on these modules share a common set on of physical level attributes and a common set of software configuration commands. T1/E1 configuration options include frame format, line coding, and Facility Datalink Protocol. T1/E1 ports can store up to 24 hours of performance statistics for local and remote ports. These software commands do not configure time slots.

Hardware descriptions of the ASM-CE can be found in Chapter 7, “OmniSwitch Switching Modules.” Hardware descriptions of the WSM-FT1/E1 can be found in Chapter 48, “Managing WAN Modules.” The CSM-CE-T1/E1 and the CSM-T1/E1 are adapter boards used in the CSM-U universal cell switching module; descriptions of these modules can be found in Chapter 40, “Cell Switching Modules.” And hardware descriptions of the WSX-FT1/E1 can be found in Chapter 3, “Omni Switch/Router Switching Modules.”

This chapter is divided into two parts. The first part provides an overview of T1/E1 digital services. The second part describes the configuration of physical T1 and E1 ports; this second part starts with the section, *The T1/E1 Menu* on page 53-3.

T1 and E1 Overview

Carrier digital services were designed primarily to support digitized voice over long distances. Digital services are the primary method for carrying voice between two endpoints using two pairs of copper wire. Digital wide-area data networking uses the same digital services that were originally designed for digitized voice.

Analog to Digital Conversion

To improve quality and reliability, long-distance phone networks upgraded their backbones from analog Frequency Division Multiplexing (FDM) to digital Time Division Multiplexing (TDM). In TDM, analog data is converted to digital data using a CODEC device that employs a method called Pulse Code Modulation (PCM).

In Pulse Code Modulation, the CODEC samples the analog signal 8,000 times a second and converts each sample to an 8-bit digital value. These 8,000 8-bit samples yield a total digital data rate of 64,000 BPS for one voice service. This service is also known as Digital Service Zero (DS0), which is the basis for T1 and E1 connections.

These 8,000 8-bits in time are also known as a *time slot*. A *channel* is a time slot that can carry voice or data. Using Time Division Multiplexing, 24 channels (for T1) or 32 channels (for E1) are multiplexed to create a service called Digital Service 1 (DS1). The more common name for DS1 is *T1* or *E1*.

T1 Framing

A T1 frame consists of 24, 8-bit time slots and a 1-bit synchronization and control bit. Twelve (12) T1 frames can be grouped into a *SuperFrame (SF/D4)*, or 24 T1 frames can be grouped into an *Extended SuperFrame*. In each SuperFrame, the 6th and 12th frame may contain “robbed bit” (A, B) signalling, which means the least significant bit is robbed from each time slot in the 6th and 12th frame and used for signalling. In Extended SuperFrames, this robbed-bit signalling (A, B, C, D) occurs in the 6th, 12th, 18th, and 24th frames.

E1 Framing

The E1 frame consists of 32, 8-bit time slots (two of these time slots are used for synchronization and multiframe signalling) for 256 bits per frame at 2.048 megabits per second. Sixteen (16) E1 frames are grouped into a multiframe. An E1 multiframe can use Channel Associated Signalling (CAS) contained in time slot 16. Timeslot 16 in multiframe 0 is used for multiframe synchronization and control. Timeslot 16 of multiframes 1 through 15 are used to carry A, B, C, and D signaling bits.

ATM Over T1/E1

When ATM is run over a T1 or E1 port, the same framing options are used. The only difference is that the payload is comprised of cells, rather than time slots.

The T1/E1 Menu

The commands for configuring and monitoring T1 and E1 ports are contained in the **te** submenu. This submenu displays as shown below and may be accessed (when in verbose mode) by entering **te** at a system prompt.

Command	T1/E1 Port Management Menu
tes	View status of a T1/E1 port configuration and statistics
temod	Modify a T1/E1 port configuration
tecls	Clear framer statistics of a T1/E1 port
telts	Display 24-hour period statistics of a local T1/E1 port
telcs	Display current 15-minute statistics of a local T1/E1 port
telis	Display 15-minute interval statistics of a local T1/E1 port
tercs	Display 24-hour period statistics of a remote T1/E1 port
tercs	Display current 15-minute statistics of a remote T1/E1 port
teris	Display 15-minute interval statistics of a remote T1/E1 port
tebcfg	Configure BERT test
tebs	Display BERT statistics
tebcls	Clear BERT statistics
tecfg	Configure T1/E1 port type

The commands in this menu are described in the following sections. The first command, **tes**, displays configuration information on ports. This configuration information is configured through the **temod** command. The remaining commands, listed after the **telts** command provide a variety of interval statistics for local and remote T1 and E1 connections.

◆ Note ◆

The **tebcfg**, **tebs**, **tebcls**, and **tecfg** commands apply only to the OmniAccess 408 and 512. For the OmniSwitch and Omni Switch/Router, these are nonfunctioning commands.

Configuring a T1 Port

The **temod** command configures a T1 port at the physical level and is generic to all such ports regardless of the logical level service, such as circuit emulation, that controls them.

To configure a T1 port, enter the following command

```
temod <slot>/<port>
```

where **<slot>** is the slot number where the board is located, and **<port>** is the T1 port number on the board that you want to modify. For example, to modify port number 2 on the board in switch slot 5, enter

```
temod 5/2
```

A screen similar to the following displays:

T1 Port Configuration for slot 5, port 2

1) Circuit Identifier { 30 chars max }	: Alcatel T1 Circuit
2) Frame Format { ESF (2), SF (3), unframed (8) }	: ESF
3) Line Build Out { short(1), long(2) }	: short
30) Line Length in meters (0-200)	: 30
4) Line Coding { B8ZS (2), AMI (5) }	: B8ZS
5) Facility Datalink { ANSI T1.403 (2), AT&T 54016 (4), T1.403-AT&T (6), none (8) }	: none
6) Facility Datalink Port Role { network (1), user (2) }	: network
7) Transmit Clock Source { loopTiming (1), localTiming (2) }	: localTiming
8) Loopback Mode { none (1), payload (2), line (3), inward (5) }	: inward
9) Signalling { none (1), CAS (2), CCS (3) }	: none
10) Trap Generation { enabled (1), disabled (2) }	: disabled
11) Yellow Alarm Detection { enabled (1), disabled (2) }	: enabled

Enter (option=value/save/cancel) :

1) Circuit Identifier

Enter a textual description of this T1 port, up to 30 characters. This text will be used in other screen displays to identify this T1 port.

2) Frame Format

Specify the frame format to be used on this port. The choices are Extended SuperFrame (**ESF**), SuperFrame or D4 (**SF**), or no special frame format (**unframed**). A T1 frame consists of 24 8-bit time slots and a 1-bit synchronization and control. Twelve (12) T1 frames can be grouped into a SuperFrame, and 24 T1 frames can be grouped into an Extended SuperFrame.

Normally, you should configure a T1 port as ESF (the default) since a T1 port configured as SuperFrame (SF) can produce false yellow alarms if a Layer 2 protocol like High-Level Data Link Control (HDLC) is being used. On ATM T1 ports, only option **2** (ESF) is supported since only the ESF format is compliant with the ATM Forum *DS1 Physical Layer Specification* (af-phy-0016.00). In addition, to support FDL and remote loopback activation/deactivation on the ATM UNI you *must* use the ESF format.

If you must set the port as SF, you can disable Yellow Alarm detection with the **Yellow Alarm Detection** option, which is described on page 53-7.

If you choose the **unframed** format, then the framer will not look for Channel Associated Signalling (CAS). Data is treated as a data stream. When used in a circuit emulation application, this option must be chosen when configuring an “unstructured” circuit emulation service.

Important Note

The unframed format is only valid on ASM and CSM circuit emulation modules. You *cannot* use it on WAN modules or on ASM and CSM T1 ports without circuit emulation.

3) Line Build Out

Indicate whether the T1 port supports short haul or long haul interfaces. Only T1 ports equipped with Line Interface Unit (LIU) support long haul. Long haul support is necessary if this T1 port is directly connected to a Central Office (CO) and the cable length is greater than 655 feet (200 meters). If this T1 port connects locally (i.e., it is not connected to an external CSV) using less than 655 feet (200 meters) of cable, short haul is adequate.

Note

All T1/E1 ports except those on the ASM-CE are equipped with a Line Interface Unit (LIU) chip.

An additional prompt displays for either the line length between this port and the T1 device (short haul configurations) or the attenuation of the cable attaching this port and the T1 device (long haul configurations). Each of these options is described below.

40) Line Length in meters

Displayed only when **short haul** is chosen as the **Line Build Out** option. Specify the distance, in meters, between this T1 port and the attached T1 device.

41) Attenuation

Displayed only when **long haul** is chosen as the **Line Build Out** option. Specify the attenuation of the line between this T1 port and the attached T1 device.

4) Line Coding

The type of physical encoding used on the connection. AMI (Alternate Mark Inversion) is more sensitive. B8ZS (Bipolar 8 Zero Substitution) should be used when possible. In most networks, B8ZS is recommended. If the port is running ATM traffic, B8ZS is *required*. In all cases, the Line Coding you select must match that provided by your service provider.

5) Facility Datalink

Facility Datalink (FDL) gathers performance statistics every second and stores them in the 24-hour local statistical database. It also sends local performance statistics to the remote T1 port depending on the type of FDL chosen and the “role” of the FDL (specified in the next field). In order to obtain far-end, or remote, performance statistics (viewed through the **terts**, **tercs**, and **teris** commands), you must enable an FDL protocol.

Note

Facility Datalink requires a T1 port and the frame type must be Extended SuperFrame.

You have the following choices:

- | | |
|------------------------|--|
| ANSI T1.403 | The FDL exchange recommended by ANSI. The FDL method sends Performance Report Messages (PRMs) to the far-end port every second, processes received PRMs, and stores them in a 24-hour far-end statistical database. |
| AT&T 54106 | The operation of this FDL protocol depends on the Facility DataLink Port Role setting (configured in the next field). The FDL protocol will either be active (network) or passive (user) in its sending of PRMs. |
| T1.403-AT&T | In this combination selection, the port supports both the ANSI (ANSI T1.403) and AT&T Extended Superframe (AT&T 54106) protocols at the same time. The port processes ANSI messages as described for the ANSI T1.403 option and responds to AT&T request messages. |
| none | The port does not use Facility Datalink. |

6) Facility Datalink Port Role

Indicates the role of this port in relation to the remote port. This setting only affects configurations where the Facility Datalink field is set to **AT&T 54016**. When set to **network**, far-end historical statistics are updated by periodically sending 24-hour and 1-hour performance statistics requests to the far-end port. When set to **user**, the FDL passively waits for messages from the far-end port.

7) Transmit Clock Source

The source of the transmit clock. Loop timing means the receive clock (recovered from receive data) is used as the transmit clock. Local timing indicates the local clock source (generated from PLLs) is used as the transmit clock.

The transmit clock source is related to the clocking mode used in circuit emulation services. In *synchronous* clocking mode, both sides of the T1 connection will use a local clock source. However, in *SRTS* and *adaptive* clocking, the T1 port receives the clock on one end (loop timing) and regenerates the clock locally (local timing) on the other end. In such a case, the T1 port receiving the clock from the network should be configured as **loop timing** and the other end of the link should be configured as **local timing**.

For more information on CSM timing, see Chapter 45, “Clocking ATM Networks.”

8) Loopback Mode

The loopback configuration for this port. Loopback configurations describe the relation between the device attached to a T1 port and the framing functionality within the T1 port. Framing functionality assembles T1 frames into SuperFrames and Extended SuperFrames, depending on how the port is configured. Possible values are as follows:

none	The port is not in a loopback state. This is the typical live network state for a T1 port.
payload	The received signal at this T1 port is looped out of the port after passing through the port's framing functionality. This state should only be used for debugging purposes.
line	The received signal at this T1 port does not go through the port's framing functionality, and is looped straight back out the port. This state should only be used for debugging purposes.
inward	The transmitted signal from the inward side of this port is looped back internally. The signal passes through the T1 framing functionality before looping back. This state should only be used for debugging purposes.

9) Signaling

The type of signaling used on this port. Only the **none** and **CAS** (Channel Associated Signaling) options are applicable to a circuit emulation service port. The **CCS** (Common Signal Channeling) option is used with external ISDN Primary Rate ports. If you select the **CAS** option, then you are enabling robbed-bit signalling.

Robbed-bit signalling can be used with SuperFrames or Extended SuperFrames. In each SuperFrame, the 6th and 12th frame may contain "robbed bit" (A, B) signalling, which means the least significant bit is robbed from each time slot in the 6th and 12th frame and used for signalling. In Extended SuperFrames, this robbed-bit signalling (A, B, C, D) occurs in the 6th, 12th, 18th, and 24th frames.

10) Trap Generation

Enables all of the SNMP-based traps related to T1 and E1 ports.

11) Yellow Alarm Detection

Specify the yellow alarm detection state for this port. A T1 port configured as SuperFrame (SF) can produce false yellow alarms if a Layer 2 protocol like High-Level Data Link Control (HDLC) is being used. Therefore, you can disable yellow alarm detection with this option. (A T1 port set to Extended SuperFrame (ESF) will not produce false yellow alarms.)

Configuring an E1 Port

The **temod** command configures an E1 port at the physical level and is generic to all such ports regardless of the logical level service, such as circuit emulation, that controls them. You configure the circuit emulation service that controls this port through the **cemodify** command.

To configure an E1 port, enter the following command

```
temod <slot>/<port>
```

where **<slot>** is the slot number where the board is located, and **<port>** is the T1 port number on the board that you want to modify. For example, to modify port number 2 on the board in switch slot 4, you would enter

```
temod 4/2
```

A screen similar to the following displays:

E1 Port Configuration for slot 4, port 2

1) Circuit Identifier { 30 chars max }	: Alcatel E1 Circuit
2) Frame Format { E1 (4), E1-CRC (5), E1-MF (6), E1-CRC-MF (7), unframed (9) }	: E1
3) Not FAS { enabled (1), disabled (2) }	: enabled
4) Line Build Out { short(1), long(2) }	: short
40) Cable Type { 75 Ohm (1), 120 Ohm (2) }	: 75 Ohm
5) Line Coding { HDB3 (3), AMI (5) }	: HDB3
6) Transmit Clock Source { loopTiming (1), localTiming (2) }	: localTiming
7) Loopback Mode { none (1), payload (2), line (3), inward (5) }	: none
8) Signalling { none (1), CAS (2), CCS (3) }	: none
9) Trap Generation { enabled (1), disabled (2) }	: disabled

Enter (option=value/save/cancel) :

1) Circuit Identifier

Enter a textual description of this E1 port, up to 30 characters. This text will be used in other screen displays to identify this E1 port.

2) Frame Format

Specify the E1 frame format to be used on this port. The choices are as follows:

- E1** Standard E1 frame format using the framing bits in time slot 0 for framing.
- E1-CRC** E1 frame using framing bits in both time slot 0 and CRC-4 multiframe for framing.
- E1-MF** E1 frame using framing bits in both time slot 0 and time slot 16 multiframe for framing.
- E1-CRC-MF** E1 frame using framing bits in time slot 0, time slot 16 multiframe, and CRC-4 multiframe for framing.
- unframed** The framing software will not look for framing bits to determine the start of a frame or multiframe. Data is treated as a data stream. When used in a circuit emulation application, this option should be chosen when configuring an “unstructured” circuit emulation service.

Important Note

The unframed format is only valid on ASM and CSM circuit emulation modules. You *cannot* use it on WAN modules or on ASM and CSM E1 port without circuit emulation.

3) Not FAS

Indicates whether you want to add an extra level of frame checking. E1 frames in time slot 0 are composed of alternating bits of FAS (Frame containing Frame Alignment Signal) and NFAS (Frame not containing Frame Alignment Signal). The **Not FAS** option tells the framer to check framing on FAS and NFAS bits. Normally, the framer checks only FAS bits, which contain the frame alignment signal pattern. If you enable **Not FAS**, then framing software will additionally also check NFAS bits, which include remote alarm indication information.

4) Line Build Out

The E1 port supports short haul or long haul interfaces. Only E1 ports equipped with a Line Interface Unit (LIU) chip support long haul. Long haul support is necessary if this E1 port is directly connected to a Central Office (i.e., not connected via an external CSU) and the cable length is greater than 655 feet (200 meters). If this E1 port connects locally using less than 665 feet (200 meters) of cable, then short haul is adequate.

Note

All T1/E1 ports except those on the ASM-CE are equipped with a Line Interface Unit (LIU) chip.

An additional prompt displays requesting the resistance type used for this port connection.

40) Cable Type

Indicate the cable resistance type used on the short or long haul interface. The cable resistance type can be 75 ohm or 120 ohm. The resistance is a set via a jumper on the E1 board; it is not configurable through software.

5) Line Coding

The type of physical encoding used on the connection. AMI (Alternate Mark Inversion) is more sensitive. HDB3 (High Density Bipolar 3) should be used when possible.

6) Transmit Clock Source

The source of the transmit clock. Loop timing means the receive clock (recovered from receive data) is used as the transmit clock. Local timing indicates the local clock source (generated from PLLs) is used as the transmit clock.

The transmit clock source is related to the clocking mode used in circuit emulation services. In synchronous clock mode, both sides of the E1 connection will use a local clock source. However, in SRTS and adaptive clocking, the E1 port receives the clock on one end (loop timing) and regenerates the clock locally (local timing) on the other end. In such a case, the E1 port receiving the clock from the network should be configured to **loop timing** and the other end of the link should be configured to **local timing**.

7) Loopback Mode

The loopback configuration for this port. Loopback configurations describe the relation between the device attached to an E1 port and the framing functionality within the E1 port. Framing functionality assembles E1 frames into multiframes, depending on how the port is configured. Possible values are as follows:

- | | |
|----------------|--|
| none | The port is not in a loopback state. This is the typical live network state for an E1 port. |
| payload | The received signal at this E1 port is looped out of the port after passing through the port's framing functionality. This state should only be used for debugging purposes. |
| line | The received signal at this E1 port does not go through the port's framing functionality, and is looped straight back out the port. This state should only be used for debugging purposes. |
| inward | The transmitted signal from the inward side of this port is looped back internally. The signal passes through the E1 framing functionality before looping back. This state should only be used for debugging purposes. |

8) Signalling

The type of signaling used on this port. Only the **none** and **CAS** (Channel Associated Signaling) options are applicable to a circuit emulation service port. The **CCS** (Common Signal Channeling) option is used with external ISDN ports. If you select the CAS option, then you are enabling Channel Associated Signaling, which is used with E1 multiframes. In Channel Associated Signaling, timeslot 16 in frame 0 of the multiframe is used for multiframe synchronization and control. Timeslot 16 of frames 1 through 15 are used to carry A, B, C, and D signaling bits.

9) Trap Generation

Enables all of the SNMP-based traps related to circuit emulation service ports.

Viewing T1/E1 Configuration and Alarm Information

You can view all current parameters and alarms for a T1 or E1 port using the **tes** command. These parameters will be either the default parameters or parameters you modified through the **temod** command or network management software.

You have a choice of viewing parameters at the chassis or port level. You receive different displays depending upon which level you choose. The sections below describe all ways to use the **tes** command.

Viewing Information for all T1/E1 Ports in the Switch

To view port parameters for all T1/E1 ports in a chassis, enter the following command

```
tes
```

A screen similar to following displays:

T1/E1 Chassis Status		
Slot/Port	Type	Active Alarms
4/2	E1	NoAlarm
4/3	E1	NoAlarm
5/2	T1	NoAlarm, Loopback
5/3	T1	NoAlarm, Loopback

Slot/Port. The T1 or E1 slot and port for which information is supplied. The slot is listed first, followed by a slash (/), followed by the port number.

Type. The port type. The port will either be a T1 or E1 port.

Active Alarms. Alarms that have occurred on this port. Possible alarms for each port are:

NoAlarm	The port is free of any alarms.
RcvYellow	This port is receiving a yellow alarm from the far-end port. A yellow alarm occurs in SuperFrames when bit 6 of all channels has been zero for at least 425 milliseconds. The yellow alarm will not occur if a Loss of Signal alarm has already occurred. In Extended SuperFrames, an alarm occurs if the yellow alarm pattern is found.
XmtYellow	The port is transmitting a yellow alarm <i>to</i> the far-end port. See the above definition of RcvYellow for a description of a yellow alarm.
RcvAIS	This port is receiving Alarm Indication Signal (AIS) from the far-end port. An AIS occurs when an unframed signal with a high density of 1s (99.9% density) is received for more than 1.5 seconds.
XmtAIS	This port is transmitting Alarm Indication Signal (AIS) <i>to</i> the far-end port. An AIS occurs when an unframed signal with a high density of 1s (99.9% density) is received for more than 1.5 seconds.
RedAlarm	The port is in red alarm state. A red alarm occurs when a T1 port has been in Out-of-Frame (OOF) condition for 2.55 seconds. The red alarm condition will be removed if the OOF condition has been absent for at least 16.6 seconds.

Viewing T1/E1 Configuration and Alarm Information

LossOfSignal	The port has experienced a Loss of Signal (LOS), or Loss of Carrier. An LOS event occurs after 175 contiguous pulse positions with no pulses (10 absent pulses on E1 ports). An LOS failure is cleared after the switch observes a single pulse.
RcvLOMF	This port is receiving loss of multiframe (LOMF) alarms from the far-end port. When a far-end E1 port detects an out-of-multiframe condition, it transmits a frame with the alarm indication bit set (in time slot 16) back to the local E1 port. This error is similar to a yellow alarm on T1 ports.
LocalUA	This port is not available possibly because a cable is not attached.
Loopback	The port is currently in loopback mode. Loopback mode can be configured through the temod command or dynamically activated through Facility Data Link (ANSI T1.403 and AT&T 54106) or through loopback control codes on a T1 port.

Viewing Information for T1/E1 Ports on One Module

To view port parameters, enter the following command

```
tes <slot>
```

where **<slot>** is the slot number where the on which you want to view information resides. For example, to view configuration parameters for the board in slot 5, enter

```
tes 5
```

A screen similar to following displays:

T1/E1 Port Status for slot 5		
Port	Type	Active Alarms
2	T1	NoAlarm, Loopback
3	T1	NoAlarm, Loopback

Explanations of the columns in this table are described in the section, *Viewing Information for all T1/E1 Ports in the Switch* on page 53-11.

Viewing Information For a T1 Port

To view T1 port parameters, enter the following command

```
tes <slot>/<port>
```

where **<slot>** is the slot number where the board is located, and **<port>** is the T1 port number on the board on which you want to view information. For example, to view information for Port 2 on the board in slot 5, enter

```
tes 5/2
```

A screen similar to following displays for a T1 port:

T1/E1 Port Status for slot 5, port 2

Circuit Identifier	: Alcatel T1 Circuit		
Frame Format	: ESF	Line Build Out	: 30 (SH)
Facility Datalink	: none	FDL Port Role	: network
Line Coding	: B8ZS	Signalling	: none
Transmit Clock Source	: localTiming	Trap Generation	: disabled
Status Change Time	: 0 days, 00:07:24.69		
Loopback Status	: LocalInwardLoop		
Line Status	: NoAlarm, Loopback		

Framer Statistics

Loss of Signal Events	: 0
Line Code Violation Events	: 431986
Out of Frame Events	: 0
Red Alarm Events	: 1
Squelch Alarm Events	: 0
Frame Bit Error Events	: 2
Alarm Indication Signal Events	: 0
Yellow Alarm Events	: 1
ESF CRC-6 Error Events	: 3

Circuit Identifier, Frame Format, Line Build Out, Facility Datalink, FDL Port Role, Line Coding, Signalling, Transmit Clock Source, Trap Generation. These parameters are described in the section, *Configuring a T1 Port* on page 53-4. Please refer to that section for descriptions.

Status Change Time. The system time when the last change in Line Status (i.e., alarm) parameter occurred.

Loopback Status. The type of loopback mode configured for this port through the **temod** command or activated remotely through FDL. Loopback modes are described in *Configuring a T1 Port* on page 53-4.

Line Status. A list of any alarms that have occurred on his port. The possible items in the list are the same as those for **Active Alarms** described in *Viewing Information for all T1/E1 Ports in the Switch* on page 53-11.

Loss of Signal Events. The total number of Loss of Signal (LOS) events that have been detected on this port. An LOS event occurs after 175 contiguous pulse positions with no pulses (10 absent pulses on E1 ports). An LOS failure is cleared after the switch observes a single pulse.

Line Code Violation Events. The occurrence of either a bipolar violation or an excessive zeros error. A bipolar violation is the occurrence of a pulse of the same polarity as the previous pulse. In B8ZS coded signals, a bipolar violation is a pulse of the same polarity as the previous without being part of the zero substitution code. An excessive zeros error is the occurrence of more than 15 contiguous zeros in an AMI-coded signal; in a B8ZS-coded signal, it is the occurrence of seven (7) or more contiguous zeros.

Out of Frame Events. The total number of out of frame events that have been detected on this port. An out of frame event occurs when two or more framing errors occur within a 3 microsecond period for Extended SuperFrame signals, or when two or more errors occur out of five or fewer consecutive framing bits. The signal will be back in frame when there have been fewer than two frame bit errors within a 3 microsecond period for Extended SuperFrame signals.

Red Alarm Events. The number of times this port has been in a red alarm state, which occurs when a T1 port has been in Out-of-Frame (OOF) condition for 2.55 seconds. The red alarm condition will be removed if the OOF condition has been absent for at least 16.6 seconds.

Squelch Alarm Events. The number of squelch alarm events that have been detected on this port. A squelch alarm occurs when the line signal level of the input pulse is below a threshold level. The threshold level on a T1 line is 0.5V.

Frame Bit Error Events. The number of framing bit error events that have been detected on this port. A frame bit error occurs when an error bit is detected during the framing process.

Alarm Indication Signal Events. The number of Alarm Indication Signal (AIS) events that have been detected on this port. An AIS occurs when an unframed signal with a high density of 1s (99.9% density) is received for more than 1.5 seconds.

Yellow Alarm Events. The total number of yellow alarm events that have occurred on this T1 port. A yellow alarm occurs in SuperFrames when bit 6 of all channels has been zero for at least 335 microseconds. The yellow alarm will not occur if a Loss of Signal alarm has already occurred. In Extended Superframes, an alarm occurs if the yellow alarm pattern is found.

Note

A T1 port that has been configured as a SuperFrame (SF) port can produce false yellow alarms. You can disable yellow alarm detection on a T1 port with the **temod** command, which is described in *Configuring a T1 Port* on page 53-4.

ESF CRC-6 Error Events. The number of times a CRC-6 error has been found in an Extended SuperFrame.

Viewing Information For an E1 Port

To view E1 port parameters, enter the following command

```
tes <slot>/<port>
```

where **<slot>** is the slot number where the board is located, and **<port>** is the E1 port number on the board for which you want to view information. For example, to view information for Port 2 on the board in slot 4, enter

```
tes 4/2
```

A screen similar to following displays for an E1 port:

T1/E1 Port Status for slot 4, port 2

```
Circuit Identifier      : Alcatel E1 Circuit
Frame Format            : E1                Line Build Out      : 120 Ohm (SH)
Line Coding             : HDB3             Signalling            : none
Transmit Clock Source  : localTiming      Trap Generation       : disabled
Status Change Time     : 0 days, 00:06:34.69
Loopback Status        : NoLoop
Line Status             : NoAlarm
```

Framer Statistics

```
Loss of Signal Events      :          1
Line Code Violation Events :          9
Out of Frame Events        :          2
Red Alarm Events           :          1
Squelch Alarm Events      :          1
Frame Bit Error Events     :          9
Alarm Indication Signal Events :          3
Out of Sub-multiframe Events :          0
Out of TS16 Multiframe Events :          0
Far End Frame Alarm Events :          2
Far End Multiframe Alarm Events :          0
Far End Block Error Events :          0
CRC-4 Error Events        :          0
```

Circuit Identifier, Frame Format, Line Build Out, Line Coding, Signaling, Transmit Clock Source, Trap Generation. These parameters are described in the section, *Configuring an E1 Port* on page 53-8. Please refer to that section for descriptions.

Status Change Time. The system time when the last change in Line Status (i.e., alarm) parameter occurred.

Loopback Status. The type of loopback mode configured for this port through the **temod** command. Loopback modes are described in *Configuring an E1 Port* on page 53-8.

Line Status. A list of any alarms that have occurred on his port. The possible items in the list are the same as those for **Active Alarms** described in *Viewing Information for all T1/E1 Ports in the Switch* on page 53-11.

Loss of Signal Events. The total number of Loss of Signal (LOS) events that have been detected on this port. An LOS event occurs after the port detects more than 10 consecutive zeros.

Line Code Violation Events. The occurrence of either a bipolar violation or excessive zeros error. A bipolar violation is the occurrence of a pulse of the same polarity as the previous pulse. In HDB3 coded signals, a bipolar violation is a pulse of the same polarity as the previous without being part of the zero substitution code. An excessive zeros error is the occurrence of more than 15 contiguous zeros in an AMI-coded signal; in an HDB3-coded signal, it is the occurrence of seven (7) or more contiguous zeros.

Out of Frame Events. The total number of out of frames events that have been detected on this port. An out of frame event occurs when three consecutive frame alignment signals have been received with an error. The signal will be back in frame when frame alignment signalling is normal for three consecutive frames.

Red Alarm Events. The number of times this port has been in a Red alarm state. A red alarm occurs when a T1 port has been in Out-of-Frame (OOF) condition for 2.55 seconds. The red alarm condition will be removed if the OOF condition has been absent for at least 16.6 seconds.

Squelch Alarm Events. The number of squelch alarm events that have been detected on this port. A squelch alarm occurs when the line signal level of the input pulse is below a threshold level.

Frame Bit Error Events. The number of framing bit error events that have been detected on this port. A frame bit error occurs when an error bit is detected during the framing process.

Alarm Indication Signal Events. The number of Alarm Indication Signal (AIS) events that have been detected on this port. An AIS occurs when an unframed signal with a high density of 1s (99.9% density) is received for more than 1.5 seconds.

Out of Sub-multiframe Events. The number of sub-multiframe events that have been detected on this E1 port. This error occurs when four (4) consecutive CRC-4 multiframe alignment signals have been received in error or when a frame alignment error has been lost.

Out of TS16 Multiframe Events. The number of TS16 multiframe events that have been detected on this E1 port. This error occurs when two (2) consecutive TS16 multiframe alignment signals have been received in error, or all bits in time slot 16 are logic 0 for one TS16 multiframe, or frame alignment has been lost.

Far End Frame Alarm Events. The number of times the remote end has detected an out-of-frame condition. When a far end E1 port detects an out-of-frame condition, it transmits a frame with the alarm indication bit set (in time slot 0) back to the local E1 port. This error is similar to a yellow alarm on T1 ports.

Far End Multiframe Alarm Events. The number of times the remote end has detected an out-of-multiframe condition. When a far-end E1 port detects an out-of-multiframe condition, it transmits a frame with the alarm indication bit set (in time slot 16) back to the local E1 port. This error is similar to a yellow alarm on T1 ports.

Far End Block Error Events. The number of times the remote end has received a frame with a bad CRC-4. When the far end E1 port detects a CRC-4 error in the incoming frame, it transmits the frame with the E bit cleared.

CRC-4 Error Events. The number times a frame has been received with a bad CRC-4.

Viewing T1/E1 Local Statistics

There are a number of commands available for viewing local T1 and E1 statistics. These commands provide statistics for the past 24 hours, the current 15-minute interval, or the past 96 15-minute intervals. The following sections describe these commands.

Viewing Total Local Statistics

You can view statistics occurring during the past 24 hours on a single port by entering the following command

```
telts <slot>/<port>
```

where **<slot>** is the slot number where the board is located, and **<port>** is the port number on the board for which you want to view statistics. For example, to view 24-hour statistics for Port 2 on the board in slot 5, enter

```
telts 5/2
```

A screen similar to the following displays:

```

Local 24-hour Period Statistics for port 2 on slot 5

Circuit Identifier      : Alcatel T1 Circuit
Valid Intervals        : 1 of 96      Elapsed Time           : 421 of 900

  ES   SES  BES   UAS  SEFS  LES  CSS  PCV  LCV
  ----  ---  ---  ----  ----  ---  ---  ---  ---
   3    1    1    0    1   313   0    2   313

```

Circuit Identifier. The textual description of this T1 or E1 port as configured through the **temod** command.

Valid Intervals. Indicates the number of 15-minute intervals for which valid statistics were gathered during the previous 24 hours. Statistics may be gathered for up to 96 15-minute intervals during a 24 hour period.

Elapsed Time. The number of seconds that have elapsed during this 15-minute interval of gathering statistics. This time will be reset to zero when a 15-minute session of statistics gathering is complete (and stored) and the next 15-minute interval begins.

ES. Errored Seconds. For T1-ESF and E1-CRC conditions, this is a second with one or more Path Code Violations, one or more out-of-frame defects, one or more controlled slip errors, or an AIS error.

SES. Severely Errored Seconds. For T1-ESF frames, this is a second with 320 or more Path Code Violation errors, one or more out-of-frame defects, or an AIS error. For E1-CRC conditions, this is a second with 832 or more Path Code Violation errors, or one or more out-of-frame defects. For E1-noCRC signals, this is a second with 2048 or more Line Code Violation errors. For D4/(SF) frames, this is a second with framing errors, an out-of-frame error, or a second with 1544 or more line code violation errors.

BES. Bursty Errored Seconds. The number of seconds with fewer than 320 but more than one (1) Path Code Violation error (see below for definition), no Severely Errored Frame errors, and no AIS errors.

UAS. Unavailable Seconds. The number of seconds this port was unavailable for transmitting or receiving data. In general, a port is unavailable after 10 consecutive Severely Errored Seconds or after a failure on the interface occurs.

Viewing T1/E1 Local Statistics

SEFS. Severe Errored Framing Second. A second with one or more out-of-frame errors or an AIS error.

LES. Line Errored Seconds. The number of seconds during which one or more Line Code Violation errors have occurred (see also the definition of Line Code Violation below).

CSS. Controlled Slip Seconds. A one-second interval with one or more controlled slip errors. Controlled slip errors are the replication or deletion of the payload bits on a frame. Such an error may occur when there is a difference between the timing of a synchronous receiving terminal and the received signal.

PCV. Path Code Violations. A frame synchronization bit error in EF/D4 and E1-noCRC frames, or a CRC or frame synchronization error in the T1-ESF (Extended Super Frame) and E1-CRC frames.

LCV. Line Code Violations. The occurrence of either a bipolar violation or excessive zeros error. A bipolar violation is the occurrence of a pulse of the same polarity as the previous pulse. In B8ZS and HDB3 coded signals, a bipolar violation is a pulse of the same polarity as the previous without being part of the zero substitution code. An excessive zeros error is the occurrence of more than 15 contiguous zeros in an AMI-coded signal; in a B8ZS-coded signal, it is the occurrence of seven (7) or more contiguous zeros.

Viewing Current Local Statistics

You can view statistics for the current 15-minute interval on a single port by entering the following command

```
telcs <slot>/<port>
```

where **<slot>** is the slot number where the board is located, and **<port>** is the port number on the board on which you want to view statistics. For example, to view 15-minute interval statistics for Port 2 on the board in slot 5, enter

```
telcs 5/2
```

A screen similar to the following displays:

```
Local Current 15-minute Measurement for port 2 on slot 5

Circuit Identifier      : Alcatel T1 Circuit
Valid Intervals        : 1 of 96      Elapsed Time          : 431 of 900

  ES   SES   BES   UAS   SEFS   LES   CSS   PCV   LCV
-----
  0    0    0    0    0    0    0    0    0
```

Definitions of the fields and columns in this display are the same as those used for the **telts** command. See *Viewing Total Local Statistics* on page 53-17 for an explanation of these statistics.

Viewing Local Historical Statistics

The **telis** command allows you to display historical statistics for the past 96 15-minute intervals. Enter the following command

```
telis <slot>/<port>
```

where **<slot>** is the slot number where the board is located, and **<port>** is the port number on the board on which you want to view statistics. For example, to view historical 15-minute interval statistics for Port 2 on the board in slot 5, enter

```
telis 5/2
```

A screen similar to the following displays:

Local 15-minute Interval Statistics for port 2 on slot 5

Circuit Identifier	: Alcatel T1 Circuit								
Valid Intervals	: 5 of 96			Elapsed Time			: 440 of 900		
Intv#	ES	SES	BES	UAS	SEFS	LES	CSS	PCV	LCV
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0

Definitions of the fields and columns in this display are the same as those used for the **telts** command. See *Viewing Total Local Statistics* on page 53-17 for an explanation of these statistics.

Viewing T1 Remote Statistics

To receive and monitor remote statistics on T1 ports you must enable the Facility Datalink (FDL) protocol through the **temod** command. These statistics will not be available if you do not enable FDL.

Note

Because there is no FDL standard for E1 configurations, remote statistics are not supported on E1 ports.

Viewing Total Remote Statistics

You can view remote statistics occurring during the past 24 hours on a single port by entering the following command

```
ters <slot>/<port>
```

where **<slot>** is the slot number where the board is located, and **<port>** is the port number on the board on which you want to view statistics. For example, to view remote 24-hour statistics for Port 2 on the board in slot 5, enter

```
ters 5/2
```

A screen similar to the following displays:

Remote 24-hour Period Statistics for port 2 on slot 5

```
Circuit Identifier      : Alcatel T1 Circuit
Valid Intervals       : 1 of 96      Elapsed Time           : 1 of 900

  ES  SES  BES  UAS  DM  SEFS  LES  CSS  PCV  LOFC
  ----  ---  ---  ---  ---  ---  ---  ---  ---  ---
    0    0    0    0    0    0    0    0    0    0
```

Most of the definitions of the fields and columns in this display are the same as those used for the **ters** command. See *Viewing Total Local Statistics* on page 53-17 for an explanation of these statistics. The remaining statistics are described below.

LOFC. Loss of Frame Count. A loss of frame count is the accumulation of the number of times a “Loss of Frame” is declared.

Viewing Current Remote Statistics

You can view remote statistics for the current 15-minute interval on a single port by entering the following command

```
tercs <slot>/<port>
```

where **<slot>** is the slot number where the board is located, and **<port>** is the port number on the board on which you want to view statistics. For example, to view remote 15-minute interval statistics for Port 2 on the board in slot 5, enter

```
tercs 5/2
```

A screen similar to the following displays:

Remote Current 15-minute Measurement for port 2 on slot 5

```
Circuit Identifier      : Alcatel T1 Circuit
Valid Intervals        : 1 of 96      Elapsed Time          : 1 of 900

  ES  SES  BES  UAS  DM  SEFS  LES  CSS  PCV  LOFC
=====
   0   0   0   0   0   0   0   0   0   0
```

Definitions of the fields and columns in this display are the same as those used for the **telts** command. See *Viewing Total Local Statistics* on page 53-17 for an explanation of these statistics.

Viewing Remote Historical Statistics

The **teris** command allows you to display remote historical statistics for the past 96 15-minute intervals. Enter the following command

```
teris <slot>/<port>
```

where **<slot>** is the slot number where the board is located, and **<port>** is the port number on the board on which you want to view statistics. For example, to view remote historical 15-minute interval statistics for Port 2 on the board in slot 5, enter

```
teris 5/2
```

A screen similar to the following displays:

Remote 15-minute Interval Statistics for port 2 on slot 5

```
Circuit Identifier      : Alcatel T1 Circuit
Valid Intervals        : 5 of 96      Elapsed Time          : 25 of 900

Intv#  ES  SES  BES  UAS  DM  SEFS  LES  CSS  PCV  LOFC
=====
   1   0   0   0   0   0   0   0   0   0   0
   2   0   0   0   0   0   0   0   0   0   0
   3   0   0   0   0   0   0   0   0   0   0
   4   0   0   0   0   0   0   0   0   0   0
   5   0   0   0   0   0   0   0   0   0   0
```

Definitions of the fields and columns in this display are the same as those used for the **telts** command. See *Viewing Total Local Statistics* on page 53-17 for an explanation of these statistics.

Clearing the Framer Statistics for a T1/E1 Port

The **tecls** command enables you to clear the accumulated physical-layer (Framer) statistics for a T1 or E1 port. To clear statistics, enter

```
tecls <slot>/<port>
```

where **<slot>** is the slot number where the board is located, and **<port>** is the port number on the board on which you want to clear statistics. For example, to statistics for Port 2 on the board in slot 5, enter

```
tecls 5/2
```

Once the statistics have been cleared, the following message will be displayed:

```
Statistics of port 5/2 have been cleared.
```

54 Managing DS3/E3 Modules

DS3/E3 Overview

DS3 and E3 are two interface types for running data across Wide Area Networks at clocking speeds of 44.736 and 34.368 Mbps, respectively. DS3, defined by ANSI standards, is used in North American networks. E3, defined by the ITU-T (formerly CCITT) standard, is used throughout the rest of the world.

These physical interfaces were originally designed to carry multiplexed digital data for voice services. Today, their use has been expanded to incorporate ATM services.

DS3 Framing

DS3 uses a framing structure of 4760 bits per “M-frame.” The M-Frame consists of 7 “M-subframes” each having 680 bits. Each M-subframe consists of 8 blocks of 85 bits, in which 84 of the 85 bits carry payload data. In the case of “legacy” DS3, the payload data consists of 28 T1 circuits. In the case of ATM DS3, the payload data bits consist of the ATM cells. The data is clocked at a bit rate of 44.736 Mbps. Control bits consist of X-bits, P-bits, and C-bits.

E3 Framing

The E3 module supports both the G.751 and G.832 protocols. G.751 E3 uses a frame of 1536 bits (192 octets), consisting of 24 bits of overhead and 1512 bits of payload data. G.832 E3 uses a framing structure of 4296 bits (537 octets) per frame, with 7 octets of overhead and 530 octets of payload data. In the case of “legacy” E3, the payload data consists of 16 E1 circuits. In the case of ATM DS3, the payload data bits consist of the ATM cells. The data is clocked at a bit rate of 34.368 Mbps. The G.751 control octet consists of frame alignment signal bits, an alarm indication bit, a national use bit, and justification service bits. The G.832 control octets consist of frame alignment signal (2 octets), error monitoring (1 octet), trail trace (1 octet), a maintenance and adaptation byte (1 octet that includes a 3-bit payload type), a network operator byte, and general-purpose communications channel (1 octet).

DS3/E3 Port Management Menu

The commands for configuring and monitoring DS3 and E3 ports are listed in the **ds3** submenu. To access this menu, enter **ds3**, followed by **<enter>**, at the system prompt. To display a summary of the DS3 menu commands, enter **?**, followed by **<enter>**. A screen similar to that shown below will be displayed:

Command	DS3 Port Management Menu
dss	View a DS3/E3 port configuration, status, and statistics
dsmod	Modify a DS3/E3 port configuration
dscls	Clear former statistics of a DS3/E3 port
dslts	Display 24-hour period statistics of a local DS3/E3 port
dslcs	Display current 15-minute statistics of a local DS3/E3 port
dslis	Display 15-minute interval statistics of a local DS3/E3 port
vps	View a DS3/E3 port status and statistics
vpis	View a DS3/E3 port interval statistics
cpis	Clear a DS3/E3 port interval statistics
dscfg	Configure DS3/E3 port type

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

The commands in this menu are described in the following sections. The first command, **dss**, displays configuration information on ports. This configuration information is configured through the **dsmod** command. The remaining commands, listed after the **dslts** command provide a variety of interval statistics for local and remote DS3 and E3 connections.

◆ Note ◆

The **dscfg** command only works for the OmniAccess 408 and 512. For the OmniSwitch and Omni Switch/Router, it is a nonfunctioning command.

Configuring a DS3 Port

The **dsmod** command configures a DS3 port at the physical level. It is generic to all such ports, regardless of the logical level service that controls them and regardless of the board type.

To configure a DS3 port, enter the following command, followed by **<enter>**

```
dsmod <slot>/<port>
```

in which **<slot>** is the slot number of the board on which the port is located and **<port>** is the port number on the board you want to modify. For example, to modify port number 2 on the switch slot 5, enter:

```
dsmod 5/2
```

A screen similar to the following displays:

```

DS3 Port Configuration for slot 5, port 2

1) Circuit Identifier (30 chars max)           : Alcatel DS3 Circuit
2) PL Scramble { False(1), True(2) }          : True
3) Timing Mode { Loop(1),Local(2) }           : Local
4) Loopback Config { NoLoop(1), InwardLoop(2),
    LineLoop(3), CellLoop(4),
    PayloadLoop(5) }                           : NoLoop
5) Line Type { CbitParity(1), M23(2) }        : CbitParity
6) Sublayer { PLCP(1), ADM(2) }               : PLCP
7) Trap Generation { enabled (1), disabled (2) } : disabled
8) Line Length (0-64000)                       : 50 meters

Enter (option=value/save/cancel) :

```

After you have entered the required values, be sure to save your configuration.

Field Descriptions

The following section explains the fields and their corresponding values.

1) Circuit Identifier

Enter a textual description of this DS3 port, up to 30 characters. This text will be used in other screen displays to identify this DS3 port.

2) PL Scramble

This field specifies whether Cell Payload Scramble is enabled. PL Scramble is a technique that enables framing to be maintained on certain medium-speed edge and trunk interfaces. Available values are **True(1)** (enabled) or **False(2)** (disabled).

3) Timing Mode

This field specifies the transmit clock timing source of the DS3 port. The possible values are **Loop(1)** and **Local(2)**. In loop timing, the transmit timing is recovered from the receive data stream and then the timing “looped” back onto the transmit data stream (NOTE: this is different from loop diagnostics modes (see below), in which the actual receive data stream is looped back to the transmit data stream). In local timing, the timing for the transmit data stream is generated internally, rather than using the clock recovered from the receive data stream of the DS3 port. For more details on timing, refer to Chapter 45, titled “Clocking ATM Networks.”

4) Loopback Config

This field is used for diagnostic purposes to set various receive-to-transmit data loops. Possible types are:

- NoLoop(1)** The port is not in a loopback state. This is the typical live network state for a DS3 port.
- InwardLoop(2)** The transmit function of the DS3 port is looped back internally to the receive function. This state should only be used for debugging purposes.
- LineLoop(3)** The received signal at this DS3 port does not go through the port’s framing functionality, and is instead looped straight back out the transmit function of the port. This state should only be used for debugging purposes.

CellLoop(4) The cells received (valid cells only) are looped back and sent out the transmit function of the port. This state should only be used for debugging purposes.

PayloadLoop(5) The received signal (bit level) at this DS3 port is looped through the port after passing through the port's framing functionality.

5) Line Type

Enter the physical format of the DS3 port. The possible line types for DS3 port are **CbitParity(1)** or **M23(2)**. The type must match the type as specified by your service provider.

6) Sublayer

Specify the sublayer type to be used for this port. The available values for a DS3 port are **PLCP(1)**, (Physical Layer Convergence Protocol) and **ADM(2)** (ATM Direct Mapping). The type must match the type as specified by your service provider.

7) Trap Generation

Specifies whether the SNMP-related status traps for this port are enabled. The possible values are **enabled(1)** and **disabled(2)**.

7) Line Length

The allowable range for line length is 0-64000 meters. The default setting is 50 meters.

Configuring an E3 Port

The **dsmod** command is also used to configure E3 ports at the physical level and is generic to all such ports regardless of the logical level service that controls them and regardless of the board type.

To configure an E3 port, enter the following command:

```
dsmod <slot>/<port>
```

in which **<slot>** is the slot number of the board on which the port is located, and **<port>** is the E3 port number on the board you want to modify. For example, to modify port number 2 on switch slot 4, enter:

```
dsmod 4/2
```

If this E3 port is configured for the G.751 line type, a screen similar to the following displays:

E3 Port Configuration for slot 4, port 2

1) Circuit Identifier (30 chars max)	: Alcatel E3 Circuit
2) PL Scramble { False(1), True(2) }	: True
3) Timing Mode { Loop(1),Local(2) }	: Local
4) Loopback Config { NoLoop(1), InwardLoop(2), LineLoop(3), CellLoop(4), PayloadLoop(5) }	: NoLoop
5) Line Type { G.751(1), G.832(2) }	: G.751
6) Sublayer { PLCP(1), ADM(2) }	: PLCP
7) Trap Generation { enabled (1), disabled (2) }	: disabled

Enter (option=value/save/cancel) :

Field Descriptions

The following section explains the fields and their corresponding values.

1) Circuit Identifier

Enter a textual description of this E3 port, up to 30 characters. This text will be used in other screen displays to identify this port.

2) PL Scramble

This field specifies whether Cell Payload Scramble is enabled. Possible values are **True(1)** (enabled) or **False(2)** (disabled).

3) Timing Mode

This field specifies the transmit clock timing source of the E3 port. The possible values are **Loop(1)** and **Local(2)**. In loop timing, the transmit timing is recovered from the receive data stream and then the timing “looped” back on the transmit data stream (NOTE: this is different than the loop diagnostic modes (see below), in which the actual receive data stream is looped back to the transmit data stream). In local timing, the timing for the transmit data stream is generated internally, rather than using the clock recovered from the receive data stream of the E3 port.

4) Loopback Config

This field is used for diagnostic purposes to set various Receive to Transmit data loops. Possible types are:

- NoLoop(1)** The port is not in a loopback state. This is the typical live network state for an E3 port.
- InwardLoop(2)** The transmit function of the E3 port is looped back internally to the receive function. This state should only be used for debugging purposes.
- LineLoop(3)** The received signal at this E3 port does not go through the port’s framing functionality, and is instead looped straight back out the transmit function of the port. This state should only be used for debugging purposes.
- CellLoop(4)** The cells received (valid cells only) are looped back and sent out the transmit function of the port. This state should only be used for debugging purposes.
- PayloadLoop(5)** The received signal (bit level) at this E3 port is looped through the port after passing through the port’s framing functionality.

5) Line Type

Enter the line type for the port. The possible line types for an E3 port are **G.751** and **G.832**. The type must match the type as specified by your service provider.

6) Sublayer

This field specifies the sublayer type used for this port. The available options for an E3 G.751 port are **PLCP(1)**, (Physical Layer Convergence Protocol) and **ADM(2)** (ATM Direct Mapping). For an E3 G.832 port, only **ADM(2)** is allowed. The type must match the type as specified by your service provider.

7) Trap Generation

This field specifies whether the SNMP-related status traps for this port are enabled. The available options are **enabled(1)** and **disabled(2)**.

If this port is configured for G.832, additional parameters (fields 8-11) are displayed, as shown in the example below:

1) Circuit Identifier (30 chars max)	: Alcatel E3 Circuit
2) PL Scramble { False(1), True(2) }	: True
3) Timing Mode { Loop(1),Local(2) }	: Local
4) Loopback Config { NoLoop(1), InwardLoop(2), LineLoop(3), CellLoop(4), PayloadLoop(5) }	: NoLoop
5) Line Type { G.751(1), G.832(2) }	: G.832
6) Sublayer { PLCP(1), ADM(2) }	: ADM
7) Trap Generation { enabled (1), disabled (2) }	: disabled
8) Transmitted Payload Type { Unequipped(1), ATM(2), Equipped,non-specific(3), SDH TU-12s(4) }	: Unequipped
9) Expected Payload Type { Unequipped(1), ATM(2), Equipped,non-specific(3), SDH TU-12s(4) }	: Unequipped
10)Transmitted Trail Trace ID { Allzeros(0), or 15 chars max}	: Allzeros
11)Expected Trail Trace ID { Allzeros(0), or 15 chars max}	: Allzeros

Enter (option=value/save/cancel) :

8) Transmitted Payload Type (E3-G.832 Only)

Specify the G.832 payload type used for transmit data. The possible values are:

Unequipped(1)
ATM(2)
Equipped, non-specific(3)
SDH-TU12s(4)

9) Expected Payload type(E3-G.832 only)

Specify the G.832 payload type expected to be used for receive data. The possible values are:

Unequipped(1)
ATM(2)
Equipped, non-specific(3)
SDH-TU12s(4)

10) Transmitted Trail Trace ID(E3-G.832 only)

Specify the data to be used for G.832 Trail Trace ID to be transmitted. The Trail Trace ID is a 16-octet field that contains 1 octet of CRC-7 (first octet) and 15 octets of data. The CRC field is automatically calculated by the system. The possible values are:

Allzeroes(0)
1 to 15 characters of text

11) Expected Trail Trace ID(E3-G.832 only)

Specify the G.832 Trail Trace ID expected to be received for receive data. The possible values are:

Allzeroes(0)
1 to 15 characters of text

Viewing DS3/E3 Configuration and Alarm Information

You can view all current parameters and alarms for a DS3 or E3 port using the **dss** command. The configurable parameters will be either the default parameters or parameters you modified through the **dsmod** command or network management software.

You have a choice of viewing status information and configurable parameters at the chassis, slot or port level. You will receive different displays, depending upon which level you choose. The following sections describe the various ways to use the **dss** command.

Viewing Information for all DS3/E3 Ports in the Switch

To view port parameters for all DS3/E3 boards and ports in a chassis, enter the following command, followed by **<enter>**:

```
dss <enter>
```

A screen similar to following displays:

```

                DS3/E3 Chassis Status
Slot/Port      Type  Active Alarms
=====
4/2            E3    NoAlarm
4/3            E3    NoAlarm
5/2            DS3    NoAlarm
5/3            DS3    NoAlarm

```

Field Descriptions

The following section explains the fields and their corresponding values.

Slot/Port

This field displays the DS3 or E3 slot and port for which information is supplied. The slot is listed first, followed by a slash (*/*), followed by the port number.

Type

The port type. The port type will be either a DS3 or E3 port.

Active Alarms

Indicates current active alarms on the given port. Possible alarms for each port are:

NoAlarm	The port is free of any alarms.
LossOfSignal	Loss of Signal alarm
RcvOOF	Out of Frame alarm
RcvAIS	Alarm Indication Signal alarm
RcvFerb	Far End Receive Failure alarm (Non-E3 G.751 cases)
RedAlarm	Red alarm

DS3/E3 Port Management Menu

RcvCLoss	Cell Loss alarm
RcvCOFA	Change of Frame Alignment alarm
RcvFEBE	Far End Block Error alarm
RcvPERR	Parity Error alarm

The following alarms are applicable only if the DS3 or E3 port is configured for PLCP timing. For E3 G.832, the only configurable sublayer is ADM (PLCP is not allowed). Therefore, these alarms are not applicable to E3 G.832:

RcvPlcpYellow	PLCP Yellow Alarm
RcvPlcpLOF	PLCP Loss of Frame Alarm
RcvPlcpOOF	PLCP Out of Frame Alarm
RcvPlcpFEBE	PLCP Far End Block Error Alarm
RcvPlcpFBE	PLCP Framing Error Alarm
RcvPlcpBPE	PLCP Bit interleaved Parity Error Alarm

The following alarms are applicable only for an E3 port configured with the G.832 line type:

RcvUneq	Unequipped Payload type Received Alarm
RcvTIM	Trail Trace ID Mismatch Alarm
RcvPLM	Rx Payload Mismatch Alarm

The following alarm is applicable only for an E3 port configured with the G.751 line type:

RcvRAI	Remote Alarm Indication Alarm
---------------	-------------------------------

Viewing Information for DS3/E3 Ports on a Board

To view port parameters for all ports on a board in a particular slot, enter the following command:

```
dss <slot>
```

in which **<slot>** is the slot number of the board containing the DS3 or E3 ports for which you want to view information. For example, to view configuration parameters for the board in slot 5, enter

```
dss 5
```

A screen similar to following is displayed:

```
DS3/E3 Port Status for slot 5
```

Port	Type	Active Alarms
2	DS3	NoAlarm
3	DS3	XmtYellow, RedAlarm, LossOfSignal

Explanations of the columns in this table are described in the section, *Viewing Information for all DS3/E3 Ports in the Switch* on page 54-7.

Viewing Information for a DS3 Port

To view DS3 port status and configurable parameters, enter the following command, followed by **<enter>**:

```
dss <slot>/<port>
```

in which **<slot>** is the slot number of the board containing the DS3 or E3 port, and **<port>** is the DS3 port number on the board on which you want to view information. For example, to view information for port 1 on slot 5, enter

```
dss 5/1
```

A screen similar to following displays:

```

DS3 Port Status for slot 5, port 1
Circuit Identifier      : Alcatel DS3 Circuit
Line Type              : CbitParity   Sublayer      : PLCP
Transmit Clock Source  : localTiming  Trap Generation : disabled
Line Length (meters)  : 50
Status Change Time    : 0 days, 00:00:00.00
Far End Alarm Code Rx : No Code
Cell Payload Scramble : True
Loopback Status       : NoLoopBack
Line Status           : NoAlarm

DS3 Port Statistics for slot 5, port 1
Loss of Signal        : 0           Alarm Indication Signal : 0
Out of Frame          : 0           Far End Receive Failure : 0
Framing Bit Errors    : 0           Change of Frame Alignment : 0
Line Coding Violations : 0         Red Alarms               : 0
Far End Block Errors  : 0           Path Parity Errors       : 0
Parity Errors         : 0           Cell Loss                 : 0

DS3 Port PLCP Statistics for slot 5, port 1
Out of Frame          : 0           Loss of Frame            : 0
Framing Errors        : 0           Yellow Alarms            : 0
Far End Block Errors  : 0           Bit Interlvd. Parity Errs : 0

```

Note: The above example shows PLCP Receive statistics. These statistics will only be displayed if the DS3 port is configured for PLCP timing.

Field Descriptions

The following section explains the fields and their corresponding values.

Circuit Identifier, Line Type, Line Length, and Cell Payload Scramble

These parameters are described in the section, *Configuring a DS3 Port* on page 54-2. Please refer to that section for descriptions.

Status Change Time

This field refers to the system time when the last change in line status occurred to this port.

Loopback Status

This field shows the type of loopback mode configured for this port through the **dsmod** command. The possible values are NoLoopBack, LocalPayloadLoop, LocalLineLoop, LocalInwardLoop, RemotePayloadLoop, RemoteLineLoop, and LocalOtherLoop (this will display when Cell loop or Inward loop is selected). These parameters are described in *Configuring a DS3 Port* on page 54-2.

Line Status

Indicates current active alarms on the given port. Possible alarms for each port are:

NoAlarm	The port is free of any alarms.
LossOfSignal	Loss of Signal alarm
RcvOOF	Out of Frame alarm
RcvAIS	Alarm Indication Signal alarm
RcvFerf	Far End Receive Failure alarm (Non-E3 G.751 cases)
RedAlarm	Red alarm.
RcvCLOSS	Cell Loss alarm
RcvCOFA	Change of Frame Alignment alarm
RcvFEBE	Far End Block Error alarm
RcvPERR	Parity Error alarm

The following alarms are applicable only if the DS3 port is configured for PLCP timing.

RcvPlcpYellow	PLCP Yellow Alarm
RcvPlcpLOF	PLCP Loss of Frame Alarm
RcvPlcpOOF	PLCP Out of Frame Alarm
RcvPlcpFEBE	PLCP Far End Block Error Alarm
RcvPlcpFBE	PLCP Framing Error Alarm
RcvPlcpBPE	PLCP Bit interleaved Parity Error Alarm

Viewing Information for an E3 Port

To view E3 port status and configurable parameters, enter the following command, followed by **<enter>**:

```
dss <slot>/<port>
```

in which **<slot>** is the slot number for the board containing the DS3 or E3 port, and **<port>** is the number of the DS3 or E3 port on that slot for which you want to view information. For example, to view information for port 2 on slot 5, enter:

```
dss 5/2
```

A screen similar to following displays:

E3 Port Status for slot 5, port 2

```

Circuit Identifier      : Alcatel E3 Circuit
Line Type              : G.751          Sublayer              : PLCP
Transmit Clock Source  : loopTiming   Trap Generation       : disabled
Status Change Time    : 0 days, 00:00:00.00
Cell Payload Scramble  : True
Loopback Status       : NoLoopBack
Line Status            : NoAlarm

```

E3 Port Statistics for slot 5, port 2

```

Loss of Signal         : 0          Alarm Indication Signal : 0
Out of Frame          : 0          Remote Alarm Indication : 0
Framing Bit Errors    : 0          Change of Frame Alignment : 0
Line Coding Violations : 0          Cell Loss                 : 0

```

E3 Port PLCP Statistics for slot 5, port 2

```

Out of Frame          : 0          Loss of Frame           : 0
Framing Errors        : 0          Yellow Alarms           : 0
Far End Block Errors  : 0          Bit Interlvd. Par. Errors : 0

```

Note: The above example shows PLCP receive statistics. These statistics will only be displayed if the E3 port is configured for PLCP timing.

If the port is an E3 G.832 port, a screen similar to the following displays:

E3 Port Status for slot 5, port 2

```

Circuit Identifier      : Alcatel E3 Circuit
Line Type              : G.832          Sublayer              : ADM
Transmit Clock Source  : localTiming   Trap Generation       : disabled
Status Change Time    : 0 days, 00:00:00.00
Cell Payload Scramble  : True
Loopback Status       : NoLoopBack
Line Status            : RcvTIM

```

	Trail Trace ID	Payload Type
Transmit	0xfd Abcdefghijklmno	Unequipped
Received	0x00 123456789012345	Unequipped
Expected	0xf8 123456789Abcdef	Unequipped
Status	Alarm	Ok

E3 Port Statistics for slot 4, port 1

```

Loss of Signal         : 0          Alarm Indication Signal : 0
Out of Frame          : 0          Far End Receive Failure : 0
Framing Bit Errors    : 0          Change of Frame Alignment : 0
Line Coding Violations : 0          Unequipped Payload Recvd : 0
Parity Errors         : 0          Payload Type Mismatch    : 0
Far End Block Errors  : 0          Trail Trace ID Mismatch  : 0
Cell Loss             : 0          Cell Loss                 : 0

```

Field Descriptions

The following section explains the fields and their corresponding values.

Circuit Identifier, Line Type, Sublayer, Transmit Clock Source, Trap Generation, Line Length.

These parameters are described in the section, *Configuring a DS3 Port* on page 54-2. Please refer to that section for descriptions.

Status Change Time

The system time when the last change in line status occurred to this E3 port.

Cell Payload Scramble

This field indicates whether Cell Payload Scramble is configured as **True** or **False**.

Loopback Status

This field displays the type of loopback mode configured for this port through the **dsmod** command. The possible values are NoLoopBack, LocalPayloadLoop, LocalLineLoop, LocalInwardLoop, RemotePayloadLoop, RemoteLineLoop, and LocalOtherLoop (This will display when Cell loop is selected). These parameters are described in *Configuring a DS3 Port* on page 54-2.

Line Status

Indicates current active alarms on the given port. Possible alarms for each port are:

NoAlarm	The port is free of any alarms.
LossOfSignal	Loss of Signal alarm
RcvOOF	Out of Frame alarm
RcvAIS	Alarm Indication Signal alarm
RcvFerf	Far End Receive Failure alarm (Non-E3 G.751 cases)
RedAlarm	Red alarm
RcvCloss	Cell Loss alarm
RcvCOFA	Change of Frame Alignment alarm
RcvFEBE	Far End Block Error alarm
RcvPERR	Parity Error alarm

The following alarms are applicable only if the E3 G.751-configured port is configured for PLCP timing:

RcvPlcpYellow	PLCP Yellow alarm
RcvPlcpLOF	PLCP Loss of Frame alarm
RcvPlcpOOF	PLCP Out of Frame alarm
RcvPlcpFEBE	PLCP Far End Block Error alarm

- RcvPlcpFBE** PLCP Framing Error alarm
- RcvPlcpBPE** PLCP Bit Interleaved Parity Error alarm

The following alarms are applicable only if the E3 port is configured as G.832:

- RcvFerb** Far End Receive Failure alarm
- RcvUneq** Unequipped Payload Type Received alarm
- RcvTIM** Trail Trace ID Mismatch alarm
- RcvPLM** Rx Payload Mismatch alarm

The following two line status alerts are status rather than alarms:

- RcvPlcpTIMEMK** Timing Marker Bit (bit 8 of the G.832 Maintenance and Adaptation byte) received. This string is displayed in the "line status" field of the "dss slot/port" command only.
- RcvNATUSE** National Use bit (bit 12 of the frame in E3 G.751 frame received. This string is displayed in the "line status" field of the "dss slot/port" command only.

Viewing DS3/E3 Local Statistics

There are a number of commands available for viewing local DS3 and E3 statistics. These commands provide statistics for the past 24 hours (**dslts**), the current 15-minute interval (**dslcs**), or any or all of the past 96, 15-minute intervals (**dsics**). The following sections describe these commands.

Viewing DS3/E3 Local Total Statistics

You can view the statistics totals for events occurring during the past 24 hours on a single DS3 or E3 port by entering the **dslts** command, as shown below:

dslts <slot>/<port>

in which **<slot>** is the slot number of the board the port is located on, and **<port>** is the port number on the board for which you want statistics. For example, to get statistics for port number 1 on switch slot 5, enter

dslts 5/1

A screen similar to the following displays:

```

Local 24-hour Period Statistics for port 1 on slot 5

Circuit Identifier : Alcatel DS3 Circuit
Valid Intervals   : 0 of 96      Elapsed Time : 504 of 900

PES  PSES SEFS UAS  LCV  PCV  LES  CCV  CES  CSES
=====
      0      0      0      0      0      0      0      0      0      0
    
```

Field Descriptions

The following section explains the fields and their corresponding values.

Circuit Identifier

The textual description of this DS3 or E3 port as configured through the **dsmod** command.

Valid Intervals

This field indicates the number of 15-minute intervals for which valid statistics were gathered over the last 24 hours. Statistics may be gathered and stored for up to 96, 15-minute intervals. The number of valid intervals will be 96 unless the interface was brought on-line within the last 24 hours.

Elapsed Time

This field indicates the number of seconds that have elapsed since the beginning of the current error-measurement 15 minute sample. This time will be reset to zero when a 15-minute session of statistics gathering is complete (and stored) and the next 15-minute interval begins.

Displayed Statistics

The statistics gathered and stored (as per the IETF RFC 1407 DS3 MIB standard) are:

PES - P-bit Errored Seconds

A P-bit Errored Second is a second with one or more P-bit Coding Violations, one or more Out Of Frame defects, or a detected incoming Alarm Indication Signal. This counter is not incremented when Unavailable Seconds statistics are counted.

PSES P-bit Severely Errored Seconds

A P-bit Severely Errored Second is a second with 44 or more P-bit Coding Violations, 44 or more Out Of Frame defects, or a detected incoming Alarm Indication Signal. This counter is not incremented when Unavailable Seconds statistics are counted.

SEFS Severely Errored Framing Seconds

A Severely Errored Framing Second is a second with one or more Out Of Frame defects or a detected incoming Alarm Indication Signal. This statistic is not incremented during unavailable seconds.

UAS Unavailable Seconds

Unavailable Seconds are calculated by counting the number of seconds that the interface is "unavailable". The DS3 or E3 interface is said to be unavailable from the onset of 10 contiguous P-bit Severely Errored Seconds, or the onset of the condition leading to a failure.

LCV Line Coding Violations

This statistic is a count of both Bipolar Violations and Excess Zeros occurring during the sample period.

PCV P-bit Coding Violations

A P-bit Coding violation error event is equivalent to P-bit Parity Error event. A P-bit Parity Error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally-calculated code.

LES Line Errored Seconds

A Line Errored Second is a second in which one or more Coding Violation occurred or one or more Loss Of Signal defects is detected.

CCV C-bit Coding Violations

For C-bit Parity and SYNTRAN DS3 applications, this is the count of coding violations reported via the C-bits. For C-bit Parity, it is a count of CP-bit parity errors occurring in the sample period. For SYNTRAN, it is a count of CRC-9 errors occurring in the sample period.

CES C-bit Errored Seconds

A C-bit Errored Second is a second with one or more C-bit coding violations, or one or more Out Of Frame defects occur, or a detected incoming Alarm Indication Signal. This count is applicable only to SYNTRAN and C-bit Parity DS3 applications. This statistic is not incremented when Unavailable Seconds statistics are counted

CSES C-bit Severely Errored Seconds

A C-bit Errored Second is a second with 44 or more C-bit coding violations, or 44 or more Out Of Frame defects occur, or a detected incoming Alarm Indication Signal. This count is applicable only to SYNTRAN and C-bit Parity DS3 applications. This statistic is not incremented when Unavailable Seconds statistics are counted.

Viewing DS3/E3 Local Current Statistics

To view the statistics totals for events occurring during the current 15-minute sample period on a single DS3 or E3 port, enter the **dslcs** command, followed by **<enter>**, as shown below:

```
dslcs <slot>/<port>
```

in which **<slot>** is the slot number of the board the port is located on, and **<port>** is the port number on the board you for which you want statistics. For example, to get statistics for port number 1 on switch slot 5, enter

```
dslcs 5/1
```

A screen similar to the following displays:

```

Local Current 15-minute Measurement for port 1 on slot 5

Circuit Identifier : Alcatel DS3 Circuit
Valid Intervals   : 0 of 96      Elapsed Time : 555 of 900

  PES  PSES  SEFS  UAS  LCV  PCV  LES  CCV  CES  CSES
  =====
    0    0    0  555 64981 45230 555 63221 0 0

```

Definitions of the fields and columns in this display are the same as those used for the **dslts** command. See *Viewing DS3/E3 Local Total Statistics* on page 54-13 for an explanation of these statistics.

Viewing DS3/E3 Local Interval (Historical) Statistics

You can view the statistics totals for events occurring during all currently stored 15-minute sample periods on a single DS3 or E3 port by entering the **dslis** command, as shown below:

dslis <slot>/<port>

in which **<slot>** is the slot number of the board the port is located on, and **<port>** is the port number on the board you want to get statistics on. For example to get statistics for port number 1 on switch slot 5, enter

dslis 5/1

A screen similar to the following displays:

Local 15-minute Interval Statistics for port 1 on slot 5

Circuit Identifier : Alcatel DS3 Circuit
Valid Intervals : 96 of 96 Elapsed Time : 47 of 900

Intv#	PES	PSES	SEFS	UAS	LCV	PCV	LES	CCV	CES	CSES
1	0	0	0	900	64636	19894	900	10288	0	0
2	0	0	0	394	28278	9725	394	4832	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0

More? [<SPACE> for next page, <enter> for next line, Quit]

If more than 15 sample periods are stored, a “More” prompt will be displayed. You can then step through the remaining samples either a line at a time pressing **<enter>** or a page at a time by pressing **<space>**.

Definitions of the fields and columns in this display are the same as those used for the **dslts** command. See “Viewing DS3/E3 Local Statistics” on page 31-13 for an explanation of these statistics.

Viewing ATM Physical Layer Statistics for DS3 (CbitParity PLCP Sublayer)

The **vps** command displays status and statistics for the specified DS3 or E3 port. If you have a DS3 interface configured with the CbitParity Type and PLCP Sublayer (via the **map** command), a screen similar to following displays for the **vps** command.

```

DS3 RX Line Status
Slot  Port  LOS  OOF  AIS  FERF  RED  Cell Loss  Loopback Status
=====
4     1     Ok   Ok   OK   Ok    Ok   Ok         NoLoopBack
4     2     Ok   Ok   OK   Ok    Ok   Ok         NoLoopBack

```

DS3 RX Line Status

```

Slot  Port  FEAC Code Rx
=====
4     1     No Code
4     2     No Code

```

DS3 RX Line Status

```

Slot  Port  PLCP  PLCP  PLCP
      Port  OOF   LOF   YEL
=====
4     1     Ok    Ok    OK
4     2     Ok    Ok    OK

```

DS3 RX Line Statistics

```

Slot  Port  LOS  OOF  FERF  RED  Cell Loss
=====
4     1     0    0    0     0    0
4     2     0    2    0     0    0

```

DS3 RX Line Statistics

```

Slot  Port  AIS  COFA  LCV  PERR  FERR
=====
4     1     0    0     0    0     0
4     2     0    1     3    7     96

```

DS3 RX Line Statistics

```

Slot  Port  FEBE  PPERR
=====
4     1     0     0
4     2     5     5

```

DS3 RX Line Statistics

```

Slot  Port  PLCP  PLCP  PLCP  PLCP  PLCP  PLCP
      Port  OOF   LOF   YEL   FOE   BPE   FEBE
=====
4     1     0     0     0     0     0     0
4     2     1     0     0     2     2     0

```

Physical layer statistics available only for DS3 and E3.

Status Definitions for DS3

The following section explains the status definition fields.

LOS	Loss of signal defect.
OOF	Out of frame defect.
AIS	Alarm Indication Signal.
FERF	Far end receive failure defect.
RED	Red defect indication. Result of a persistent LOS or OOF defect.
Cell Loss	Loss of cell delineation has occurred.
Loopback Status:	The current loopback status of this port. Loopback may be activated by local management or from the remote end through FEAC code. Possible values for this column are as follows: <i>NoLoopBack.</i> The port is not in loopback mode. <i>LocalPayloadLoop.</i> The port is in payload loopback. <i>LocalLineLoop.</i> The port is in line loopback. <i>LocalOtherLoop.</i> The port is in inward loopback. <i>RemotePayloadLoop.</i> The far-end port is in payload loopback. <i>RemoteLineLoop.</i> The far-end port is in line loopback.
FEAC Code Rx	The FEAC code being received at this DS3 interface. The possible values are as follows: <i>No Code.</i> No code is being received. <i>DS3 Eqpt. Failure (SA).</i> The remote DS3 equipment is in a failure state (service affecting) and requires immediate attention. <i>DS3 LOS.</i> The remote DS3 port is in loss of signal. <i>DS3 OOF.</i> The remote DS3 port is in loss of frame. <i>DS3 AIS Received.</i> The remote DS3 is receiving AIS. <i>DS3 IDLE Received.</i> The remote DS3 is receiving Idle code. <i>DS3 Eqpt. Failure (NSA).</i> The remote DS3 equipment is in a failure state (non-service affecting). This failure state could be suspended services, not activated, or not available for use. <i>Common Eqpt. Failure (NSA).</i> The remote DS3 equipment is in a failure state (non-service affecting). <i>Loopback Received.</i> The remote DS3 is sending loopback activation code. <i>Unsupported Code.</i> The DS3 interface is receiving unsupported code, such as DS1 loopback activation/deactivation code. <i>Unknown Code.</i> The DS3 interface is receiving unknown code.
PLCP OOF	PLCP out of frame defect.
PLCP LOF	PLCP loss of frame defect.
PLCP YEL	PLCP yellow alarm defect.

Statistics Definitions for DS3

The following section explains the statistics definition fields.

Note

The statistics tables indicate the number of times an alarm has occurred since start up.

LOS	Loss of frame defect count.
OOF	Out of frame defect count.
FERF	Far end receive failure defect count.
RED	RED alarm count.
Cell Loss	Number of times loss of cell delineation has occurred.
AIS	Alarm indication signal count.
COFA	Count of change of frame alignment occurrences.
LCV	Line code violation. This statistic is a count of Bipolar violations and Excessive zeros.
PERR	Parity bit errors. This statistic is the number of DS3 P-bit errors.
FERR	Framing bit errors. This statistic is the number of DS3 F-bit or M-bit errors.
FEBE	Far-end block error. This statistic is the number of times that DS3 frames with three C-bits of M-frame 4 are different from 111.
PPERR	Path Parity Bit Error. The number of DS3 path parity errors or C-bit parity errors.
PLCP OOF	PLCP out of frame defect count.
PLCP LOF	PLCP loss of frame defect count.
PLCP YEL	PLCP yellow alarm defect count.
PLCP FOE	PLCP framing octet error count.
PLCP BPE	PLCP bit interleaved parity error count.
PLCP FEBE	PLCP far end block error count.

Viewing ATM Physical Layer Statistics for DS3 (CbitParity ADM Sublayer)

If you have a DS3 interface configured with a CbitParity Type and ADM Sublayer (via the **map** command), a screen similar to following displays for the **vps** command.

DS3 RX Line Status

Slot	Port	LOS	OOF	AIS	FERF	RED	Cell Loss	Loopback Status
4	1	Ok	Ok	OK	Ok	Ok	Ok	NoLoopBack
4	2	Ok	Ok	OK	Ok	Ok	Ok	NoLoopBack

DS3 RX Line Status

Slot	Port	FEAC Code Rx
4	1	No Code
4	2	No Code

DS3 RX Line Statistics

Slot	Port	LOS	OOF	FERF	RED	Cell Loss
4	1	0	0	0	0	0
4	2	0	2	0	0	0

DS3 RX Line Statistics

Slot	Port	AIS	COFA	LCV	PERR	FERR
4	1	0	0	0	0	0
4	2	0	1	3	7	96

DS3 RX Line Statistics

Slot	Port	FEBE	PPERR
4	1	0	0
4	2	5	5

Physical layer statistics available only for DS3 and E3.

The statistics in this display are described in the section, *Viewing ATM Physical Layer Statistics for DS3 (CbitParity PLCP Sublayer)* on page 54-17.

Viewing ATM Physical Layer Statistics for DS3 (M23 Type PLCP Sublayer)

If you have a DS3 interface configured with an M23 Type and PLCP Sublayer (via the **map** command), a screen similar to following displays for the **vps** command.

DS3 RX Line Status

Slot	Port	LOS	OOF	AIS	FERF	RED	Cell Loss	Loopback Status
4	1	Ok	Ok	OK	Ok	Ok	Ok	NoLoopBack
4	2	Ok	Ok	OK	Ok	Ok	Ok	NoLoopBack

DS3 RX Line Status

Slot	Port	PLCP OOF	PLCP LOF	PLCP YEL
4	1	Ok	Ok	OK
4	2	Ok	Ok	OK

DS3 RX Line Statistics

Slot	Port	LOS	OOF	FERF	RED	Cell Loss
4	1	0	0	0	0	0
4	2	0	2	0	0	0

DS3 RX Line Statistics

Slot	Port	AIS	COFA	LCV	PERR	FERR
4	1	0	0	0	0	0
4	2	0	1	3	7	96

DS3 RX Line Statistics

Slot	Port	PLCP OOF	PLCP LOF	PLCP YEL	PLCP FOE	PLCP BPE	PLCP FEBE
4	1	0	0	0	0	0	0
4	2	1	0	0	2	2	0

Physical layer statistics available only for DS3 and E3.

The statistics in this display are described in the section, *Viewing ATM Physical Layer Statistics for DS3 (CbitParity PLCP Sublayer)* on page 54-17.

Viewing ATM Physical Layer Statistics for DS3 (M23 Type ADM Sublayer)

If you have a DS3 interface configured with an M23 Type and ADM Sublayer (via the **map** command), a screen similar to following displays for the **vps** command.

DS3 RX Line Status

Slot	Port	LOS	OOF	AIS	FERF	RED	Cell Loss	Loopback Status
4	1	Ok	Ok	OK	Ok	Ok	Ok	NoLoopBack
4	2	Ok	Ok	OK	Ok	Ok	Ok	NoLoopBack

DS3 RX Line Statistics

Slot	Port	LOS	OOF	FERF	RED	Cell Loss
4	1	0	0	0	0	0
4	2	0	2	0	0	0

DS3 RX Line Statistics

Slot	Port	AIS	COFA	LCV	PERR	FERR
4	1	0	0	0	0	0
4	2	0	1	3	7	96

Physical layer statistics available only for DS3 and E3.

The statistics in this display are described in the section, *Viewing ATM Physical Layer Statistics for DS3 (CbitParity PLCP Sublayer)* on page 54-17.

Viewing ATM Physical Layer Statistics for E3 (G.751 PLCP Sublayer)

If you have an E3 interface configured with a G.751 Type and PLCP Sublayer (via the **map** command), a screen similar to following displays for the **vps** command.

E3 RX Line Status

Slot	Port	LOS	OOF	AIS	Cell Loss	Loopback Status
====	====	=====	=====	=====	=====	=====
5	1	Ok	Ok	OK	Ok	NoLoopBack
5	2	Ok	Alarm	OK	Alarm	NoLoopBack

E3 RX Line Status

Slot	Port	PLCP OOF	PLCP LOF	PLCP YEL
====	====	=====	=====	=====
5	1	Ok	Ok	OK
5	2	Alarm	Alarm	OK

E3 RX Line Status

Slot	Port	RAI	Nat Use
====	====	=====	=====
5	1	Ok	Off
5	2	Ok	On

E3 RX Line Statistics

Slot	Port	LOS	OOF	FERR	LCV	Cell Loss
====	====	=====	=====	=====	=====	=====
5	1	0	0	0	0	0
5	2	0	142716	142716	11	1

E3 RX Line Statistics

Slot	Port	AIS	COFA	RAI
====	====	=====	=====	=====
5	1	0	0	0
5	2	0	0	0

E3 RX Line Statistics

Slot	Port	PLCP OOF	PLCP LOF	PLCP YEL	PLCP FOE	PLCP BPE	PLCP FEBE
====	====	=====	=====	=====	=====	=====	=====
5	1	0	0	0	0	0	0
5	2	142716	1	0	2	2	1

Physical layer statistics available only for DS3 and E3.

Status Definitions for E3 G.751 PLCP

The following section explains the status definition fields.

LOS	Loss of signal defect.
OOF	Out of frame defect.
AIS	Alarm Indication Signal.
Cell Loss	Loss of cell delineation has occurred.
Loopback Status	The current loopback status of this E3 port. Loopback may be activated by local management or the remote end through FEAC code. Possible values for this column are as follows: <i>NoLoopBack.</i> The port is not in loopback mode. <i>LocalPayloadLoop.</i> The port is in payload loopback. <i>LocalLineLoop.</i> The port is in line loopback. <i>LocalOtherLoop.</i> The port is in diagnostic loopback. <i>RemotePayloadLoop.</i> The far-end port is in payload loopback. <i>RemoteLineLoop.</i> The far-end port is in line loopback.
PLCP OOF	PLCP out of frame defect.
PLCP LOF	PLCP loss of frame defect.
PLCP YEL	PLCP yellow alarm defect.
RAI	Remote alarm indication.
Nat Use	National use. Reflects the state of the National use bit in the G.751 frame.

Statistics Definitions for E3, PLCP G.751

The following section explains the statistics definition fields.

Note

The statistics tables indicate the number of times an alarm has occurred since start up.

LOS	Loss of frame defect count.
OOF	Out of frame defect count.
FERR	Framing bit error count event.
LCV	Line code violation. This statistic is a count of Bipolar violations and Excessive zeros.
Cell Loss	Number of times loss of cell delineation has occurred.
AIS	Alarm indication signal count.
COFA	Count of change of frame alignment occurrences.
RAI	Remote Alarm Indicator count.

PLCP OOF	PLCP out of frame defect count.
PLCP LOF	PLCP loss of frame defect count.
PLCP YEL	PLCP yellow alarm defect count.
PLCP FOE	PLCP framing octet error count.
PLCP BPE	PLCP bit interleaved parity error count.
PLCP FEBE	PLCP far end block error count.

Viewing ATM Physical Layer Statistics for E3 (G.751 ADM Sublayer)

If you have an E3 interface configured with a G.751 Type and ADM Sublayer (via the **map** command), a screen similar to following displays for the **vps** command.

E3 RX Line Status

Slot	Port	LOS	OOF	AIS	Cell Loss	Loopback Status
====	====	=====	=====	=====	=====	=====
5	1	Ok	Ok	OK	Ok	NoLoopBack
5	2	Ok	Ok	OK	Alarm	NoLoopBack

E3 RX Line Status

Slot	Port	RAI	Nat Use
====	====	=====	=====
5	1	Ok	Off
5	2	Ok	On

E3 RX Line Statistics

Slot	Port	LOS	OOF	FERR	LCV	Cell Loss
====	====	=====	=====	=====	=====	=====
5	1	0	0	0	0	0
5	2	0	299895	299895	11	1

E3 RX Line Statistics

Slot	Port	AIS	COFA	RAI
====	====	=====	=====	=====
5	1	0	0	0
5	2	0	2	1

Physical layer statistics available only for DS3 and E3.

Statistics Definitions for E3, ADM G.751

The following section explains the statistics definition fields.

The statistics in this display are described in the section, *Viewing ATM Physical Layer Statistics for DS3 (CbitParity ADM Sublayer)* on page 54-20.

Viewing ATM Physical Layer Statistics for E3 (G.832 ADM Sublayer)

If you have an E3 interface configured with a G.832 Type and ADM Sublayer (via the `map` command), a screen similar to following displays for the `vps` command.

E3 RX Line Status

Slot	Port	LOS	OOF	AIS	Cell Loss	Loopback Status
5	1	Ok	Ok	OK	Ok	NoLoopBack
5	2	Ok	Ok	OK	Alarm	NoLoopBack

E3 RX Line Status

Slot	Port	FEBE	FERF	Time Marker	Payload Type
5	1	Ok	Ok	Off	0
5	2	Ok	Alarm	Off	0

E3 RX Line Statistics

Slot	Port	LOS	OOF	FERR	LCV	Cell Loss
5	1	0	0	0	0	0
5	2	0	307744	307744	11	0

E3 RX Line Statistics

Slot	Port	AIS	COFA	FERF	FEBE	PERR
5	1	0	0	0	0	0
5	2	0	3	2	8	9

E3 RX Line Statistics

Slot	Port	SLM	UNEQ	TIM
5	1	0	0	0
5	2	0	3	2

Status Definitions for G.832 ADM

The following section explains the status definition fields.

- LOS** Loss of signal defect.
- OOF** Out of frame defect.
- AIS** Alarm Indication Signal.
- Cell Loss** Loss of cell delineation has occurred.
- Loopback Status** The current loopback status of this port. Loopback may be activated by local management or the remote end through FEAC code. Possible values for this column are as follows:
 - NoLoopBack*. The port is not in loopback mode.
 - LocalPayloadLoop*. The port is in payload loopback.
 - LocalLineLoop*. The port is in line loopback.
 - LocalOtherLoop*. The port is in diagnostic loopback.

RemotePayloadLoop. The far-end port is in payload loopback.

RemoteLineLoop. The far-end port is in line loopback.

FEBE	Far end block error indication.
FERF	Far end receive failure indication.
Time Marker	Timing marker. Reflects the state of the Timing Marker bit in the G.832 frame.
Payload Type	Payload type. Reflects the state of the Payload Type bits in the G.832 frame.

Statistics definitions for E3, ADM G.832

The following section explains the statistics definition fields.

Note

The statistics tables indicate the number of times an alarm has occurred since start up.

LOS	Loss of frame defect count.
OOF	Out of frame defect count.
FERR	Framing bit error count event.
LCV	Line code violation. This statistic is a count of Bipolar violations and Excessive zeros.
Cell Loss	Number of times loss of cell delineation has occurred.
AIS	Alarm indication signal count.
COFA	Count of change of frame alignment occurrences.
FERF	Far end receive failure count.
FEBE	Far end block error count.
PERR	Bit interleaved parity event count. Number of times one or more BIP-8 (8-bit interleaved parity) errors have occurred.
SLM	Signal Label Mismatch Count. Number of payload type mismatch occurrences.
UNEQ	Unequipped Count. Number of unequipped payload received.
TIM	Trail Trace Id Mismatch Count.

Viewing ATM Physical Layer Interval Statistics for DS3 (CbitParity PLCP Sublayer)

You can view DS3 statistics over a certain time interval. The **vpis** command displays statistics similar to the **vps** command, but displays total values over a specified time.

If you have a DS3 interface configured with the CbitParity Type and PLCP Sublayer (via the **map** command), a screen similar to following displays for the **vpis** command.

DS3 RX Line Status						
Slot	Port	LOS	OOF	FERF	RED	Cell Loss
====	====	=====	=====	=====	=====	=====
4	1	0	0	0	0	0
4	2	0	0	0	0	0

DS3 RX Line Statistics						
Slot	Port	AIS	COFA	LCV	PERR	FERR
====	====	=====	=====	=====	=====	=====
4	1	0	0	0	0	0
4	2	0	0	0	0	0

DS3 RX Line Statistics			
Slot	Port	FEBE	PPERR
====	====	=====	=====
4	1	0	0
4	2	0	0

DS3 RX Line Statistics							
Slot	Port	PLCP OOF	PLCP LOF	PLCP YEL	PLCP FOE	PLCP BPE	PLCP FEBE
====	====	=====	=====	=====	=====	=====	=====
4	1	0	0	0	0	0	0
4	2	0	0	0	0	0	0

Slot	Port	Elapsed Time
====	====	=====
4	1	0 days, 00:00:01.63
4	2	0 days, 00:00:01.63

Physical layer statistics available only for DS3 and E3.

The statistics in this display are described in the section, *Viewing ATM Physical Layer Statistics for DS3 (CbitParity PLCP Sublayer)* on page 54-17.

The **Elapsed Time** column indicates the time interval over which these statistics were gathered. The format used for the time interval is as follows:

<xxx> days, <hours>:<minutes>:<seconds>.<tenths of second>

Viewing ATM Physical Layer Interval Statistics for DS3 (CbitParity ADM Sublayer)

The **vpis** command allows you to view DS3 statistics that have accumulated over time, either since the system was started, or since the **cpis** command (See "Clearing Interval Statistics" on page 31-33) was issued. The **vpis** command displays statistics similar to the **vps** command, but displays total values over the elapsed period of time.

If you have a DS3 interface configured with the CbitParity Type and ADM Sublayer (via the **map** command), a screen similar to following displays for the **vpis** command.

DS3 RX Line Status						
Slot	Port	LOS	OOF	FERF	RED	Cell Loss
====	====	=====	=====	=====	=====	=====
4	1	0	0	0	0	0
4	2	0	0	0	0	0

DS3 RX Line Statistics						
Slot	Port	AIS	COFA	LCV	PERR	FERR
====	====	=====	=====	=====	=====	=====
4	1	0	0	0	0	0
4	2	0	0	0	0	0

DS3 RX Line Statistics			
Slot	Port	FEBE	PPERR
====	====	=====	=====
4	1	0	0
4	2	0	0

Slot	Port	Elapsed Time
====	====	=====
4	1	0 days, 00:00:03.55
4	2	0 days, 00:00:03.55

Physical layer statistics available only for DS3 and E3.

The statistics in this display are described in the section, *Viewing ATM Physical Layer Statistics for DS3 (CbitParity ADM Sublayer)* on page 54-20.

The **Elapsed Time** column indicates the time interval over which these statistics were gathered. The format used for the time interval is as follows:

<xxx> days, <hours>:<minutes>:<seconds>.<tenths of second>

Viewing ATM Physical Layer Interval Statistics for DS3 (M23 Type PLCP Sublayer)

If you have a DS3 interface configured with the M23 Type and PLCP Sublayer (via the **map** command), a screen similar to following displays for the **vpis** command.

DS3 RX Line Status

Slot	Port	LOS	OOF	FERF	RED	Cell Loss
4	1	0	0	0	0	0
4	2	0	0	0	0	0

DS3 RX Line Statistics

Slot	Port	AIS	COFA	LCV	PERR	FERR
4	1	0	0	0	0	0
4	2	0	0	0	0	0

DS3 RX Line Statistics

Slot	Port	PLCP OOF	PLCP LOF	PLCP YEL	PLCP FOE	PLCP BPE	PLCP FEBE
4	1	0	0	0	0	0	0
4	2	0	0	0	0	0	0

Slot	Port	Elapsed Time
4	1	0 days, 00:00:02.43
4	2	0 days, 00:00:02.43

Physical layer statistics available only for DS3 and E3.

The statistics in this display are described in the section, *Statistics definitions for E3, ADM G.832* on page 54-27.

The **Elapsed Time** column indicates the time interval over which these statistics were gathered. The format used for the time interval is as follows:

<xxx> days, <hours>:<minutes>:<seconds>.<tenths of second>

Viewing ATM Physical Layer Interval Statistics for DS3 (M23 Type ADM Sublayer)

If you have a DS3 interface configured with the M23 Type and ADM Sublayer (via the **map** command), a screen similar to following displays for the **vpis** command.

```

DS3 RX Line Status

Slot  Port  LOS  OOF  FERF  RED  Cell Loss
====  ====  =====
4     1     0    0    0    0    0
4     2     0    0    0    0    0

DS3 RX Line Statistics

Slot  Port  AIS  COFA  LCV  PERR  FERR
====  ====  =====
4     1     0    0    0    0    0
4     2     0    0    0    0    0

Slot  Port  Elapsed Time
====  ====  =====
4     1     0 days, 00:00:02.99
4     2     0 days, 00:00:02.99

```

Physical layer statistics available only for DS3 and E3.

The statistics in this display are described in the section, *Viewing ATM Physical Layer Statistics for DS3 (CbitParity PLCP Sublayer)* on page 54-17.

The **Elapsed Time** column indicates the time interval over which these statistics were gathered. The format used for the time interval is as follows:

<xxx> days, <hours>:<minutes>:<seconds>.<tenths of second>

Viewing ATM Physical Layer Interval Statistics for E3 (G.832 PLCP Sublayer)

The **vpis** command allows you to view E3 statistics that have accumulated over time, either since the system was started, or since the **cpis** command (See “Clearing Interval Statistics” on page 31-33) was issued. The **vpis** command displays statistics similar to the **vps** command, but displays total values over the elapsed period of time.

For an E3 interface configured with a G.832 Type and PLCP Sublayer (via the **map** command), a screen similar to following displays for the **vps** command.

E3 RX Line Status						
Slot	Port	LOS	OOF	FERR	LCV	Cell Loss
5	1	0	0	0	0	0
5	2	0	30848	30848	0	0

E3 RX Line Statistics				
Slot	Port	AIS	COFA	RAI
5	1	0	0	0
5	2	0	0	0

E3 RX Line Statistics							
Slot	Port	PLCP OOF	PLCP LOF	PLCP YEL	PLCP FOE	PLCP BPE	PLCP FEBE
5	1	0	0	0	0	0	0
5	2	30848	0	0	0	0	0

Slot	Port	Elapsed Time
5	1	0 days, 00:00:05.51
5	2	0 days, 00:00:05.51

Physical layer statistics available only for DS3 and E3.

The statistics in this display are described in the section, *Statistics definitions for E3, ADM G.832* on page 54-27.

The **Elapsed Time** column indicates the time interval over which these statistics were gathered. The format used for the time interval is as follows:

<xxx> days, <hours>:<minutes>:<seconds>.<tenths of second>

Viewing ATM Physical Layer Interval Statistics for E3 (G.751 ADM Sublayer)

If you have an E3 interface configured with a G.751 Type and ADM Sublayer (via the **map** command), a screen similar to following displays for the **vps** command.

E3 RX Line Status

Slot	Port	LOS	OOF	FERR	LCV	Cell Loss
5	1	0	0	0	0	0
5	2	0	31354	31354	0	0

E3 RX Line Statistics

Slot	Port	AIS	COFA	RAI
5	1	0	0	0
5	2	0	0	0

E3 RX Line Statistics

Slot	Port	SLM	UNEQ	TIM
5	1	0	0	0
5	2	0	3	2

Slot	Port	Elapsed Time
5	1	0 days, 00:00:07.87
5	2	0 days, 00:00:07.87

Physical layer statistics available only for DS3 and E3.

The statistics in this display are described in the section, “Viewing ATM Physical Layer Statistics for E3 (G.751 PLCP Sublayer)” on page 23.

The **Elapsed Time** column indicates the time interval over which these statistics were gathered. The format used for the time interval is as follows:

<xxx> days, <hours>:<minutes>:<seconds>.<tenths of second>

Clearing Interval Statistics

You can clear interval statistics (viewed through the **vps** command) using the **cpis** command. You clear statistics on a port-by-port basis. The **Elapsed Time** variable and all statistics in **vps** displays are reset after you use the **cpis** command.

To clear statistics on a given DS3 or E3 port, enter the following command:

cpis <slot>/<port>

in which slot is the slot number for the ASM in the switch, and port is the port number on the ASM module for which you want to clear statistics. For example, to clear interval statistics on port 1 on the DS3 or E3 module in slot 5, enter:

cpis 5/1

A message similar to the following confirms the operation:

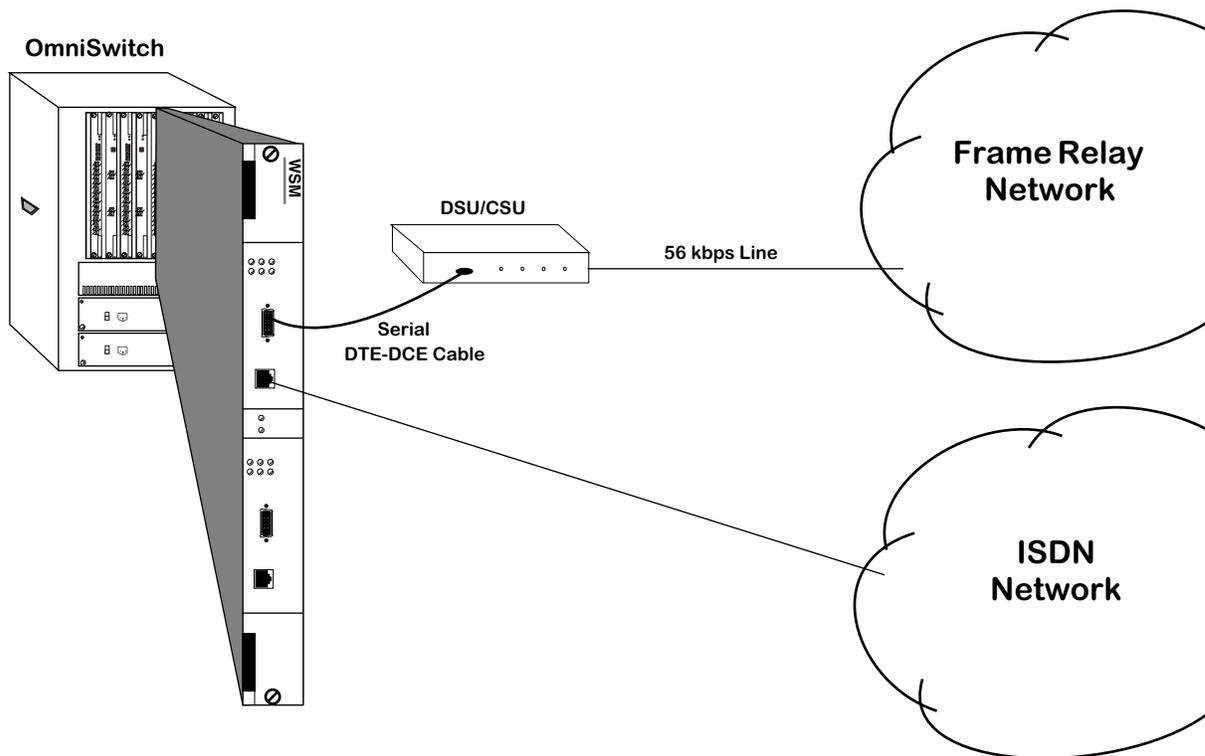
Physical layer interval statistics of port 5/1 has been cleared

55 Backup Services

Introduction

Backup Services are intended to be an integral part of a well-designed Wide Area Network (WAN). The purpose of a backup service is to provide an alternate route for data to take in the event of failure of the Primary port or Virtual Circuit. Initially, the primary entity may be either a physical port (any physical port type in the system), or a frame relay Private Virtual Circuit (PVC). The backup is via an ISDN BRI running Point-to-Point Protocol (PPP).

Backup services are configured by specifying information on the primary entity, the backup entity, and timers that control under what conditions the system will switch to backup mode. Both the primary and backup entities must be configured prior to accessing this menu. This menu also does no cross-checking to ensure that the primary being backed up is backed up by an “appropriate” backup entity. This is the responsibility of the user.



Frame Relay to ISDN Backup

Backup Services Commands

Backup services provides commands to view and configure your backup services. All commands start with “bs” for “Backup Service” followed by the function desired. All backup commands may be typed in full, or a three character abbreviation may be used (e.g. **bsadd** or **bsa** may be used to create a backup service).

Accessing the Backup Services Menu

The Backup Services menu is a submenu to the Interface menu. To access the Interface menu, enter **inter**, followed by **<return>**, as shown below.

```
/% inter <return>
```

To display a command summary for the Interface menu, enter **?**, followed by **<return>**:

```
/inter % ?
```

A screen similar to that shown below will display:

Command	Networking Menu
slipc	Configure SLIP (Serial Line IP) on a TTY Port
atm	Enter the atm Management submenu
eth100	Enter the 100BaseT submenu
10/100	Enter the 10/100BaseT submenu
wan	Enter the Wide Area Networking submenu
backup	Enter Backup networking command submenu

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

To enter the Backup menu, enter **backup**, followed by **<return>**, as shown below:

```
/Interface % backup <return>
```

To display a command summary for the Backup Services menu, enter **?**, followed by **<return>**.

```
/Interface/backup % ? <return>
```

A screen similar to that shown below will display:

Command	Networking Menu
bsadd	Add a Backup Service
bsmodify	Modify a Backup Service
bsview	View Backup Service(s)
bsdelete	Delete a Backup service
bsstatus	Display Backup service status
bsclear	Clear Backup service status

Main	File	Summary	VLAN	Networking
Interface	Security	System	Services	Help

Adding a Backup Service

With the **bsadd** command, you can:

- Add a backup for a physical port
- Back up a frame relay PVC

Adding a backup for a Physical Port

To add a backup service for a physical port:

1. Enter the **bsadd** command with no parameters, followed by **<return>**.

```
/Interface/backup % bsa <return>
```

A screen similar to that shown below will display:

```

Adding Backup Service Index          :1
1) Description                       : Backup 1
2) Admin Status { (E)nabled, (D)isabled } : Enabled
3) Primary Type { Physical Port (1),
   Frame Relay PVC DLCI (2) }       : Physical Port
   30) Slot                          :
   31) Port                          :
4) Backup Type { PPP Peer (1) }     : PPP Peer
   40) Peer ID                       :
5) Startup Timer Value { Time in Seconds after
   System Startup to wait
   for Primary to come up
   before activating
   Backup }                          : 300
6) Activate Timer Value { Time in Seconds after
   Primary Failure to
   activate Backup }                 : 30
7) Restore Timer Value { Time in Seconds after
   Primary restoral to
   disable Backup }                  : 30
(save/quit/cancel)
:
```

2. When you first enter the command, the next unique index is assigned automatically, a default description is created (**Backup** followed by the new index number), and defaults for primary type, backup type, and all backup timers are created (as shown above).
3. To back up a physical port, enter the numbers for the slot and port to be backed up and the PPP peer index (which defines ISDN call and PPP parameters). Optionally, you can modify the timer values (fields 5-7). Below is an example of backing up the port on slot 2, port 1 with PPP peer index 5.

```
      : 30=2
      : 31=1
      : 40=5
      : ?
1) Description: Backup 1
2) Admin Status { (E)nabled, (D)isabled }           : Enabled
3) Primary Type { Physical Port (1),
   Frame Relay PVC DLCI (2) }                       : Physical Port
   30) Slot                                           : 2
   31) Port                                           : 1
4) Backup Type { PPP Peer (1) }                     : PPP Peer
   40) Peer ID                                       : 5
5) Startup Timer Value { Time in Seconds after
   System Startup to wait
   for Primary to come up
   before activating
   Backup }                                           : 300
6) Activate Timer Value { Time in Seconds after
   Primary Failure to
   activate Backup }                                  : 10
7) Restore Timer Value { Time in Seconds after
   Primary restoral to
   disable Backup }                                  : 10
(save/quit/cancel)
:
```

4. Once you are satisfied with the values, enter the **save** command, followed by **<return>**.

```
: save <return>
```

The following will display:

```
Backup Service Index 1 created.
/Interface/backup %
```

Field Descriptions

The following section explains the fields and their corresponding values.

1) Description

Enter a description of the backup service in this field. Your description may consist of a maximum of 30 ASCII characters.

2) Admin Status

The available options for this field are **Enable** and **Disable**. **Enable** allows the backup service to operate. **Disable** will render the backup service inoperative without deleting it.

3) Primary Type

This field sets the type of entity that will be backed up in the case of network failure. The available options are **Physical Port** and **Frame Relay PVC DLCI**.

4) Backup Type

This field sets the entity type to be used as a backup in the event of primary failure. At this time, the only available backup type is **PPP**.

5) Startup Timer Value

This field sets the time after system startup to wait for the primary entity to come up. If the primary entity fails to come up within the defined time after system startup, the backup entity will be activated. Acceptable values are in the range of 0-65535 seconds. The default value is 300 seconds.

6) Activate Timer Value

This field sets the amount of time that the primary entity must remain in a failed state before the backup entity is activated. Acceptable values are in the range of 0-65535 seconds. The default value is 10 seconds.

7) Restore Timer Value

This field sets the amount of time the primary entity returns and remains in an operational state before the backup entity is deactivated. Acceptable values are in the range of 0-65535 seconds. The default value is 10 seconds.

Backing Up a Frame Relay PVC

Adding a backup service for a frame relay PVC is basically the same as for a physical port. The only differences are that you must specify Primary Type as **Frame Relay**, and you must specify a DLCI number. To add a backup service for a frame relay PVC:

1. Enter the **bsadd** command with no parameters, followed by **<return>**, as shown below:

```
/Interface/backup % bsa <return>
```

A screen similar to that shown below will be displayed:

```
Adding Backup Service Index           : 2
1) Description                       : Backup 2
2) Admin Status { (E)nabled, (D)isabled } : Enabled
3) Primary Type { Physical Port (1),
Frame Relay PVC (2) }                 : Physical Port
30) Slot                               :
31) Port                               :
4) Backup Type { PPP Peer (1) }       : PPP Peer
40) Peer ID                             :
5) Startup Timer Value { Time in Seconds after
System Startup to wait
for Primary to come up
before activating
Backup }                               : 300
6) Activate Timer Value { Time in Seconds after
Primary Failure to
activate Backup }                     : 10
7) Restore Timer Value { Time in Seconds after
Primary restoral to
disable Backup }                       : 10
(save/quit/cancel)
:
```

2. When you first enter the command, the next unique index is assigned automatically, a default description is created (“Backup” followed by the created index number), and defaults for primary type, backup type, and all backup timers are created (as shown above).

To backup a frame relay PVC, first change the primary type. Whenever the primary type is changed, the menu will be redisplayed, because different parameters are needed to define the primary type. An example is shown below:]

```

: 3=2
1) Description : Backup 2
2) Admin Status { (E)nabled, (D)isabled } : Enabled
3) Primary Type { Physical Port (1),
   Frame Relay PVC (2) } : Frame Relay PVC
   30) Slot :
   31) Port :
   32) DLCI :
4) Backup Type { PPP Peer (1) } : PPP Peer
   40) Peer ID :
5) Startup Timer Value { Time in Seconds after
   System Startup to wait
   for Primary to come up
   before activating
   Backup } : 300
6) Activate Timer Value { Time in Seconds after
   Primary Failure to
   activate Backup } : 10
7) Restore Timer Value { Time in Seconds after
   Primary restoral to
   disable Backup } : 10
(save/quit/cancel)
:

```

To backup a frame relay PVC, specify the slot (**30=x**), port (**31=x**) and DLCI number (**32=x**) of the PVC to be backed up. Next, enter the PPP peer index (which defines ISDN call parameters and PPP parameters). Optionally, you can modify the timer values. Below is an example of backing up the port on slot 3, port 3, PVC DLCI 32 with PPP peer index 1:

Backup Services Commands

```
      : 30=3
      : 31=3
      : 32=32
      : 40=1
      : ?
1) Description : Backup 2
2) Admin Status { (E)nabled, (D)isabled } : Enabled
3) Primary Type { Physical Port (1),
   Frame Relay PVC (2) } : Physical Port
   30) Slot : 3
   31) Port : 3
   32) DLCI : 32
4) Backup Type { PPP Peer (1) } : PPP Peer
   40) Peer ID : 1
5) Startup Timer Value { Time in Seconds after
   System Startup to wait
   for Primary to come up
   before activating
   Backup } : 300
6) Activate Timer Value { Time in Seconds after
   Primary Failure to
   activate Backup } : 10
7) Restore Timer Value { Time in Seconds after
   Primary restoral to
   disable Backup } : 10
(save/quit/cancel)
:
```

Once you are satisfied with the values, enter the **save** command, followed by **<return>**:

```
: save <return>
```

A screen similar to that shown below will display:

```
Backup Service Index 2 created.
/Interface/backup %
```

Modifying a Backup Service

With the **bsmodify** command, you can modify:

- A backup for a physical port
- A frame relay PVC.

Modifying a backup for a Physical Port

To modify a backup service for a physical port:

1. Enter the **bsmodify** command, followed by the index of the Backup service, followed by **<return>**. An example is shown below:

```
/Interface/backup % bsm 1 <return>
```

A screen similar to that shown below will display:

```
Modify configuration for Backup Service Index 1
1) Description                               : Backup 1
2) Admin Status { (E)nabled, (D)isabled }   : Enabled
   Primary Type                             : Physical Port
     Slot                                    : 2
     Port                                    : 1
   Backup Type                               : PPP Peer
   Peer ID                                   : 5
5) Startup Timer Value { Time in Seconds after
   System Startup to wait
   for Primary to come up
   before activating
   Backup }                                  : 300
6) Activate Timer Value { Time in Seconds after
   Primary Failure to
   activate Backup }                         : 10
7) Restore Timer Value { Time in Seconds after
   Primary restoral to
   disable Backup }                          : 10
(save/quit/cancel)
:
```

The command works in a manner similar to the **bsadd** command, except the parameters that define the backup service may not be changed. These parameters are the:

- index
- primary type
- primary type slot, port, and dlci
- backup type, and
- peer ID.

Only the description and startup, activate, and restore timer fields may be modified.

2. Once you are satisfied with the values, enter the **save** command, followed by **<return>**, as shown below:

```
: save <return>
```

A screen similar to that shown below will display:

```
Backup Service Index 1 modified.
/Interface/backup %
```

Modifying a Frame Relay PVC Backup Service

To modify a backup service for a frame relay PVC:

1. First, enter the **bsmodify** command, followed by the index of backup service, followed by **<return>**, as shown in the example below:

```
/Interface/backup % bsm b2 <return>
```

A screen similar to that shown below will display:

```
1) Description : Backup 1
2) Admin Status { (E)nabled, (D)isabled } : Enabled
   Primary Type : Frame Relay PVC
   Slot : 3
   Port : 3
   DLCI : 32
   Backup Type : PPP Peer
   Peer ID : 1
5) Startup Timer Value {Time in Seconds after
   System Startup to wait
   for Primary to come up
   before activating
   Backup } : 300
6) Activate Timer Value {Time in Seconds after
   Primary Failure to
   activate Backup } : 10
7) Restore Timer Value {Time in Seconds after
   Primary restoral to
   disable Backup } : 10
(save/quit/cancel)
:
```

The command functions in a manner similar to the **create** command, except the parameters that define the backup service may not be changed. These parameters are the:

- index
- primary type
- primary type subparameter
- backup type, and
- backup type subparameters.

Only the Description and Timer fields may be modified.

2. Once you are satisfied with the values, enter the **save** command, followed by **<return>** at the prompt, as shown below:

```
: save <return>
```

A screen similar to that shown below will display:

```
Backup Service Index 2 modified.
/Interface/backup %
```

Viewing Backup Service(s) Configurations

With the **bsview** command, you can view the configuration of either all backup services, or a single backup service.

Viewing the Configurations of All Backup Services

To view the configurations for all backup services, enter the following command, followed by **<return>**, at the prompt:

```
/Interface/backup % bsv <return>
```

A screen similar to that shown below will display:

Backup Table Entries

Idx	Description	Primary Type	Slot/Port/ DLCI	Bkup Type	Peer Id	Strup Time	Act. Time	Rest. Time
1	Backup 1	PHYPORT	2/1	PPP	5	300	10	10
2	Backup 2	FR PVC	3/3/32	PPP	1	300	10	10
3	Backup of PVC to Chicago	FR PVC	3/3/33	PPP	7	300	0	60

Viewing the Configuration of a Single Backup Service (bsview Command)

To view the configuration for a single backup service, enter the **bsview** command followed by the index number of the backup service, followed by **<return>**, as shown in the example below:

```
/Interface/backup % bsv 2 <return>
```

A screen similar to that shown below will display:

Backup Table Entries

Idx	Description	Primary Type	Slot/Port/ DLCI	Bkup Type	Peer Id	Strup Time	Act. Time	Rest. Time
1	Backup 1	Port	3/3/32	Peer	1	300	10	10

Deleting a Backup Service

Use the **bsdelete** command to delete a backup service. Deleting a backup service will delete the backup service configuration record. If a backup is enabled (e.g. due to the primary entity being down), the backup entity will be brought down (e.g., for ISDN the call will be disconnected).

To delete a backup service, enter the **bsdelete** command followed by the index number of the backup service, followed by **<return>**, as shown in the example below:

```
/ % bsdelete 2 <return>
```

A screen similar to that shown below will display.

```
This will bring down Backup (if up) and delete Backup Service Record
Index : 1
Description : Backup 1.
Continue? {(Y)es, (N)o} (N) :
```

Enter **<return>** or **N** (the default value) to cancel the command. Enter **Y** to delete the backup service

Viewing Backup Service Statistics

To view the statistics of a back service, enter the **bsstatus** command in the following manner:

```
bsstatus b<backupIndex>
```

where **b<backupIndex>** is the service index number assigned to the service when it was created. For example, to see the statistics for a backup service with an index number of 1, enter:

```
bsstatus b1
```

A screen similar the following displays:

```
Status for Backup Index: 1.
```

```
Current State                               :Primary Up
Number of Times Primary Port Disconnected  :0
Number of Times Backup Port Disconnected   :0
Number of Times Backup Port Initiated      :0
Number of Times Backup Port Connected      :0
Number of Times Primary Port Connected     :0
```

As a variation of this command, enter the **bsstatus** command without specifying the service index number. A screen displays showing all backup services on the switch, as shown:

Idx	Description	Slot/		Bkp	Peer	Current.
		Primary Port/	Dlci/			
1		Port	5/1/0	Peer	1	Primary Up

Current State. The current state of the backup service. The options for this are **Primary Up**, **Primary Down**, **Backup Up**, **Backup Down**, **Backup Initiated**.

Number of Times Primary Port Disconnected. The number of times the primary port has disconnected since the last clearing of statistics for this service.

Number of Times Backup Port Disconnected. The number of times the backup port has disconnected since the last clearing of statistics for this service.

Number of Times Backup Port Initiated. The number of times the backup port has been activated since the last clearing of statistics for this service.

Number of Times Backup Port Connected. The number of times the backup port has connected since the last clearing of statistics for this service.

Number of Times Primary Port Connected. The number of times the primary port has connected since the last clearing of statistics for this service.

Idx. The index number of the backup service.

Description. Enter a description of the backup service in this field. Your description may consist of a maximum of 30 ASCII characters.

Primary Type. This field shows the type of entity that will be backed up in the case of network failure. The available options are **Physical Port** and **Frame Relay PVC DLCI**.

Slot/Port/Dlci. The slot, port number, and DLCI number (if applicable) attached to this backup service.

Bkp Type. This field shows the entity type to be used as a backup in the event of primary failure. At this time, the only available backup type is **PPP**.

Peer Id. The identification number of the peer that has the backup port for this service.

Current State. The current state of the backup service. The options for this are **Primary Up**, **Primary Down**, **Backup Up**, **Backup Down**, **Backup Initiated**.

Clearing Backup Service Statistics

To clear the statistics for a backup service, enter the **bsclear** command as shown:

```
bsclear b<backupIndex>
```

where **b<backupIndex>** is the service index number assigned to the service when it was created. For example, to clear the statistics for a backup service with an index number of 1, enter:

```
bsstatus b1
```

A prompt similar the following displays:

```
This will reset the statistic for Backup Index: 1  
Continue ? {(Y)es, (N)o} (n) :
```

Enter **y** to clear the statistics.

56 Managing Channelized DS3 Modules

Introduction

Traffic patterns in the early days of the Internet were markedly different from those observed today. Early applications were text-based (FTP, telnet, email) and were mostly symmetrical in terms of traffic flow (i.e., client and server generally transmitted and received roughly equal amounts of data). The advent of the Web browser and graphical user interface for the Internet has simultaneously increased by an order of magnitude the number of users and servers on the Internet. This combined with advanced applications, such as video conferencing software, has upset both the symmetry and pattern of traffic flows, markedly reducing the overall throughput the average Internet user sees.

The channelized DS3 module (WSX-M013) addresses this problem by allowing customers to buy bandwidth based on their traffic needs. The channelized DS3 module uses channelized DS3 lines to split up the high performance capabilities of the line and divide it among several customers.

The channelized DS3 module is designed exclusively for high-density IP access and industrial strength routing, making it ideally suited to the task of providing and maintaining high-performance throughput with low delay. It easily fits into the Internet Provider landscape as a Point of Presence (PoP) at a national level (National Backbone Operator or NBO), a regional level (Regional Network Operator or RNO), and at local level (Internet Service Provider or ISP).

To achieve high-density IP access, the channelized DS3 module supports a channelized DS3 interface for Frame Relay and Point-to-Point Protocol (PPP) termination of DSOs, NxDSO bundles (or groups), DS1s and clear-channel DS3s (see the subsequent section for a description of these terms).

The channelized DS3 module is a daughtercard that plugs into the High Speed Switching Module. Each daughtercard has 2 DS3 ports. There can be two daughtercards per High Speed Switching Module, giving a total of 4 DS3 ports per chassis slot.

Each channelized DS3 is comprised of 28 DS1 channels, which in turn contain 24 DS0 time slots. Each time slot can be configured for 64kbs. DS0 time slots can be bundled together and assigned to logical ports (also known as groups), increasing the bandwidth capabilities of a group by $n \times 64\text{kbs}$, where n is the number of DS0s bundled into the logical port. A single daughtercard can support up to 512 logical channels, for a total of 1024 logical channels per chassis slot.

The channelized DS3 module can also run as a *clear channel*, which allows for the full use of the bandwidth of the DS3 connection (44.736Mbs).

Digital Signal Level X (DSX)

A Digital Signal Level X (DSX) is a term for the series of standard digital transmission rates or levels based on DS0, a transmission rate of 64 Kbps. Both the North American T-carrier system and the European E-carrier systems of transmission operate using the DS series as a base multiple. The digital signal is what is carried inside the carrier system.

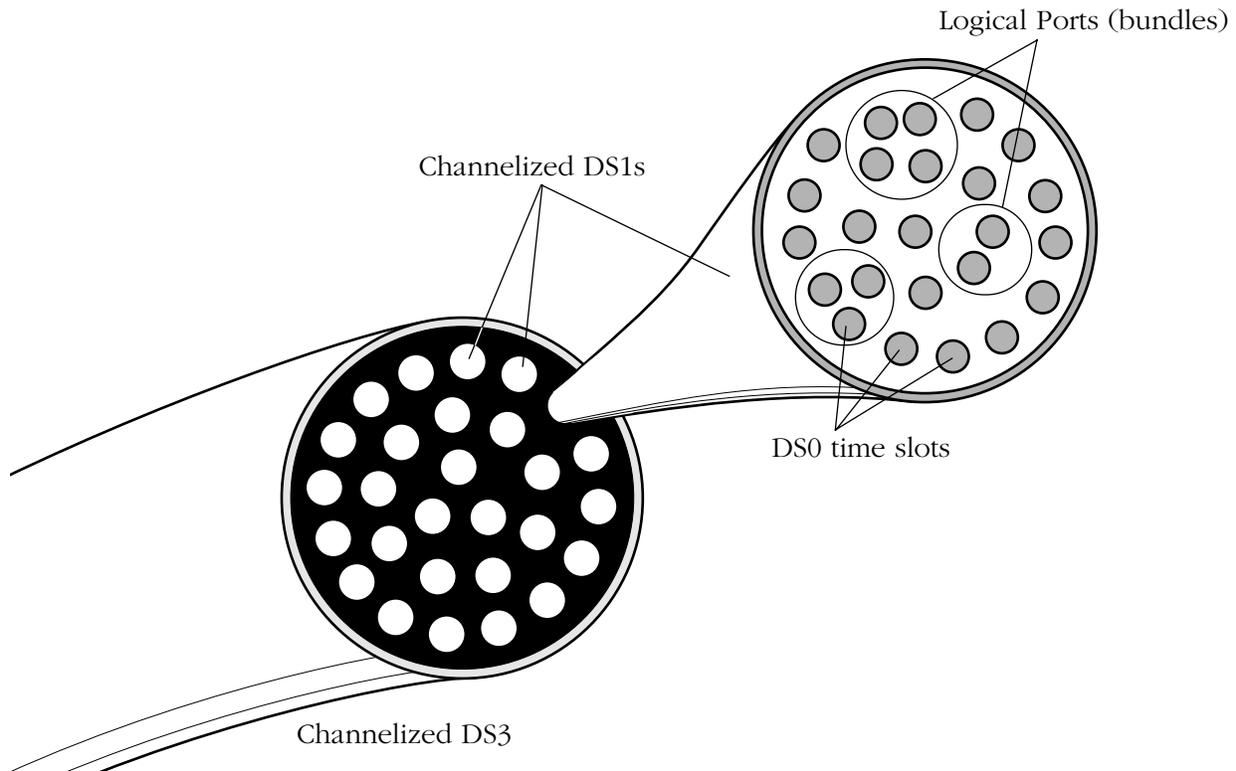
DS0 is the base for the digital signal X series. DS1, used as the signal in the T-1 carrier, is 24 DS0 (64 Kbps) signals transmitted using pulse-code modulation (PCM) and time-division multiplexing (TDM). DS2 is four DS1 signals multiplexed together to produce a rate of 6.312 Mbps. DS3, the signal in the T-3 carrier, carries a multiple of 28 DS1 signals or 672 DS0s or 44.736 Mbps.

The term “channelized” DS3 denotes the preservation within the DS3 of either the 28 DS1 signals (multiplexed DS1 to DS3, or “M13”) or the 672 DS0 and 28 DS1 signals (multiplexed DS0 to DS1 to DS3, or “M013”). (The diagram below illustrates this idea.) A “clear channel” DS3 denotes that the entire interface is treated as a single signal (no preservation of lower signals).

The channelized DS3 module supports channelized DS3 by preserving the 28 DS1 signals and 672 DS0s (24 time slots per DS1).

◆ Note ◆

The channelized DS3 module does not support the European E-carrier system.



Channelization of a DS3 and DS1

Supported Physical Interfaces

The channelized DS3 module uses a BNC physical interface (port) for data traffic, and a separate balanced T1 physical interface as an external clocking mechanism.

BNC

The BNC connectors on the channelized DS3 module daughtercard consist of two female ports, one for transmit (TX) and one for receive (RX). Both are used for a single DS3 connection and must attach to an RG-59 coaxial cable (75 ohms). Data is transmitted at a rate of 44.736MHz (+/- 20ppm) and received at a rate of 44.736MHz (+/- 50ppm).

The pinouts for transmitted and received signals of the BNC connectors are identical. Signals are transmitted and received on the center contact, while the outer shield is ground for the RG-59 (75 ohm) coaxial cable.

To reduce the effects of electromagnetic interference (EMI), it is strongly recommended that you use common-mode choke procedures. These are small ferrite sleeves that attach to the coaxial cable as close to the BNC connector as possible. It is also recommended that you attach the transmit and receive coaxial cables together along their entire length using heat activated shrink tubing or cable ties to further reduce the effects of EMI.

Balanced T1

The balanced T1 port is used exclusively as a link to an external clocking source, and will not transmit any other type of data. It uses an RJ-48C type cable.

◆ Note ◆

In order for external clocking to be employed, you must configure the channelized DS3 module to use external clocking at the DS1 channel level with the **ds1mod** command. See *Configuring a DS1 Channel* on page 56-24 for more information.

Supported Protocols

The channelized DS3 module supports both Frame Relay and synchronous Point-To-Point Protocol (PPP). For an overview of these protocols, see the “Managing Frame Relay” and “Point-to-Point Protocol” chapters of your switch manual. For information on selecting and configuring these protocols for use with logical ports, see *Adding a Logical Port Configuration* on page 56-33 and *Modify the Protocol Configuration of a Logical Port using PPP* on page 56-43 of this chapter.

Application Examples

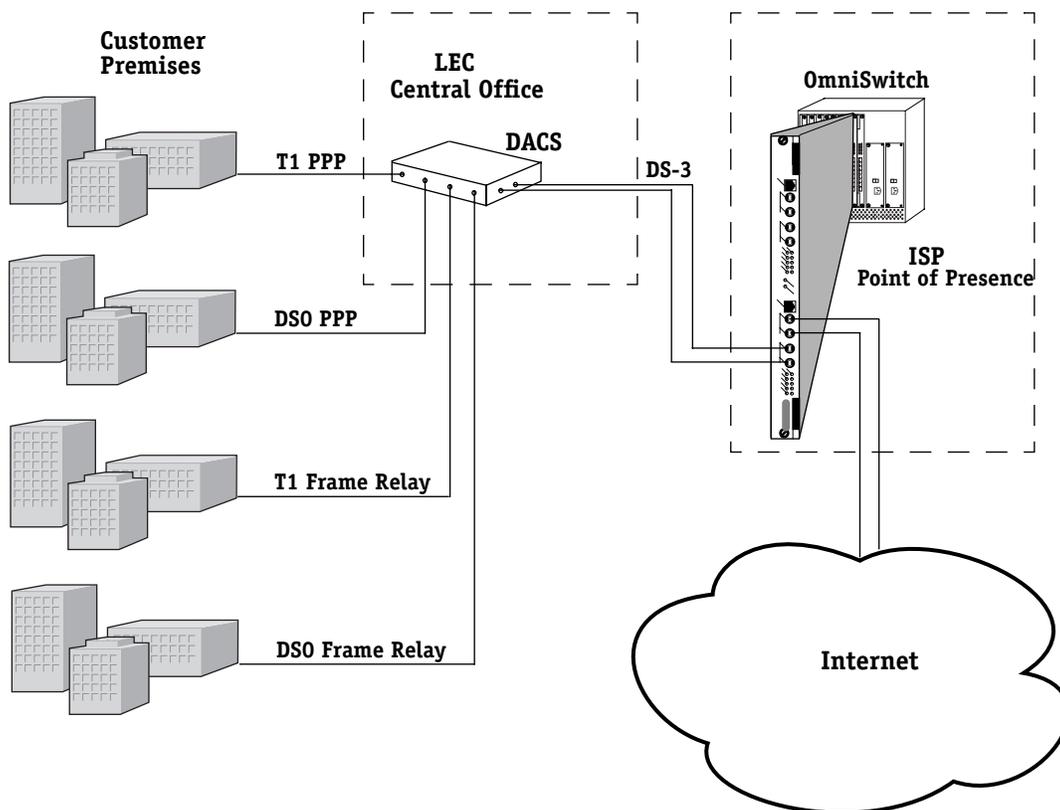
This section provides examples of the types of WAN networking possible using the channelized DS3 module.

Internet Services Provider Point-of-Presence

One ideal application for the channelized DS3 module is as an Internet Services Provider (ISP) Point of Presence (PoP). In this application, various customer access lines are combined into a single DS3 line through a Digital Access Cross-Connect System (DACS) at the Local Exchange Carrier's (LEC) central office.

The DS3 line is leased by the ISP and uses the channelized DS3 module to channelize the line into 28 DS1 channels, each with 24 DS0 time slots. Time slots are grouped together into logical ports (bundles) that can be assigned to accommodate the required bandwidth of the customer. As an ISP PoP, the channelized DS3 module terminates the layer 2 access protocol (Frame Relay or PPP) and then routes the traffic over the Internet.

The channelized DS3 module in this application could also be located at the LEC central office, depending upon the layout of the specific ISP service.

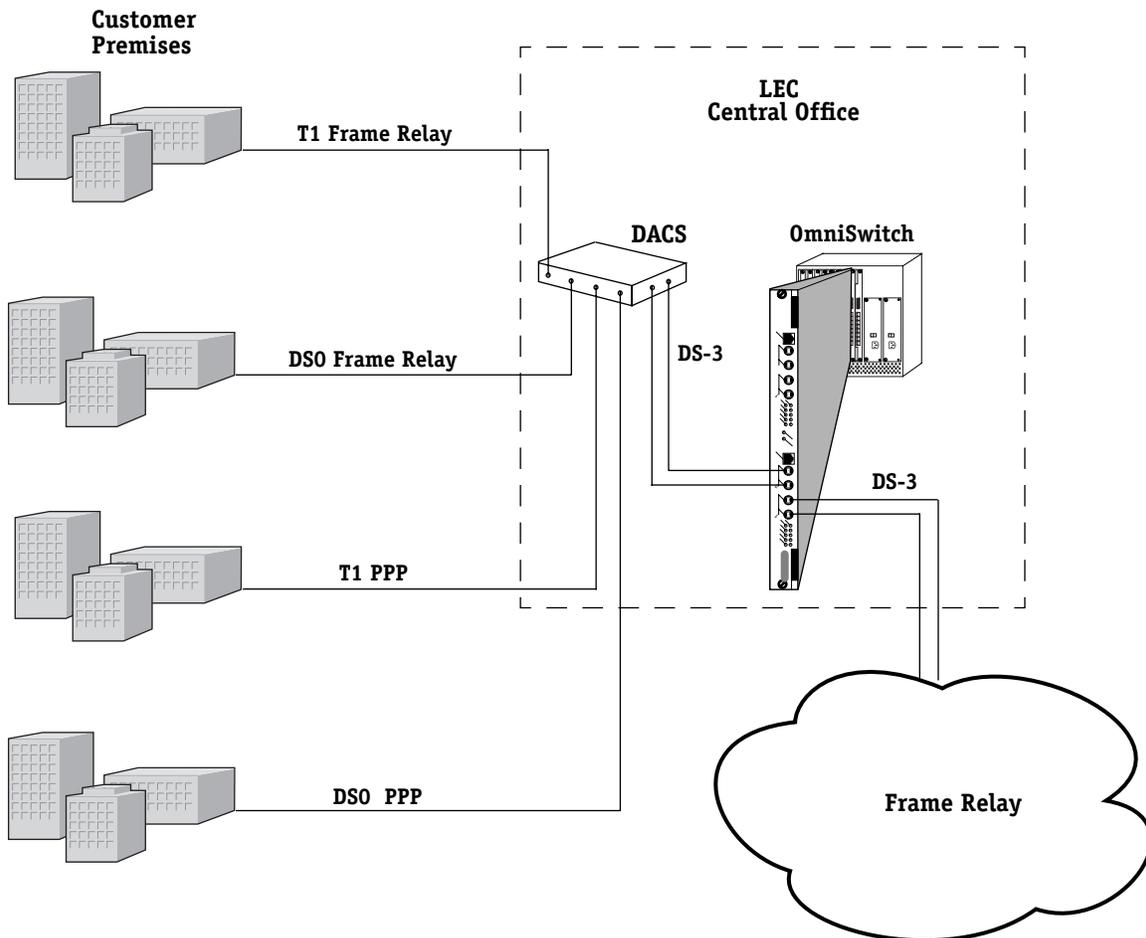


WSX Configuration with ISP Point-of-Presence

Local Exchange Carrier's Central Office

Another ideal application for the channelized DS3 module is as a layer 2 concentrator at the Local Exchange Carrier's (LECs) central office (CO). In this example, the channelized DS3 module functions primarily as a Frame Relay or PPP concentration point to trunk over an ATM backbone.

In this application, various customer lines are combined into a single DS3 line via a Digital Access Cross-connect System (DACS). The DS3 is then sent to the channelized DS3 module, where the module terminates DS3s of the LEC's DACS. The LEC can locally switch Frame Relay or PPP traffic (that is, switch from one access port to another access port) or trunk the traffic over ATM using either layer-two bridging or frame relay to ATM Interworking.



WSX Configuration From LEC Central Office

Channelized DS3 Module

The channelized DS3 module consists of a 2-port daughter card that plugs into the High Speed Switching Module. The ports are BNC DS3 connections and use RG-59 cables. These ports use either Point-to-Point Protocol (PPP) or Frame Relay.

You can configure physical port parameters through software commands. Configuration options include line type, line coding, and facility datalink. In addition, the switch can store up to 24 hours of traffic statistics in 15-minute intervals for DS3 ports, DS1 channels, and logical ports.

The WXS-M013 is actually a submodule, or daughtercard, that attaches to a High-Speed Switching Module. The High-Speed Switching Module contains memory and processing power for switching modules that operate at speeds greater than 10 Mbps. You plug cables into the channelized DS3 submodule, and the High-Speed Switching Module connects to the switch's backplane.

Channelized DS3 Module Technical Specifications	
Number of ports	2 DS3, 1 Balanced T1
Connector Type	BNC, T1 (external clocking)
Protocols Supported	Frame Relay and Point-to-Point (PPP)
Data Rates Supported	64Kbs to 44.736Mbs
Frame Formats	DS3: M23, C-bitparity DS1: D4 (Superframe), ESF (Extended Superframe)
Line Coding	DS3: B8ZS DS1: JBZS, B8ZS, HBD3, ZBTSI, AMI
DS0 time slots	1344
Logical Ports (bundles) Supported	512
Clocking	Internal, External, or Split (i.e., "loop timing")
Virtual Circuits Supported	Permanent Virtual Circuits (PVCs)
MAC Addresses Supported	OmniSwitch: 1,024; 2,048 with CAM upgrade option Switch/Router: 4096
Connections Supported	DS-3 and T1 (external clocking) Connections
Cable Supported	Coaxial RG-59 (75 ohms), Rj-48C
Maximum Cable Length	450 feet
FCC Rating	Class A, Class B

The module includes one column of LEDs for each port. The column number corresponds with the port number. If the module includes a total of four ports, then the module contains two sets of LEDs. The second set of LEDs displays next to the second set of ports.

T3EN (T3 Enabled). On when the DS3 connection is enabled and can transmit data.

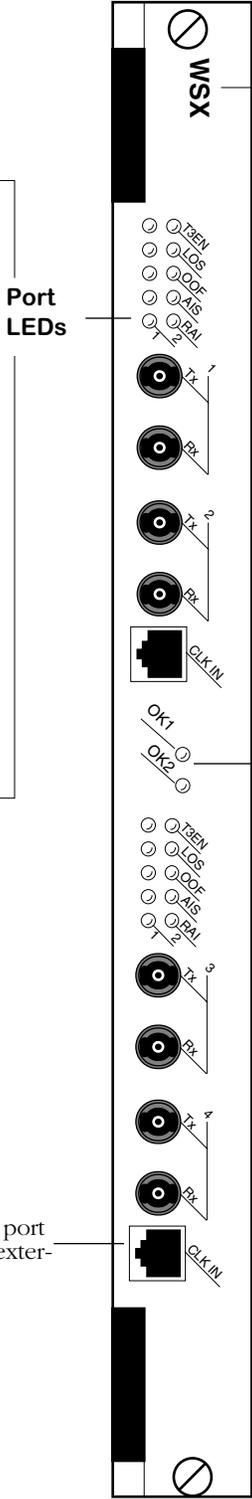
LOS (Loss of Signal). On when the WSX module observes 175 (+/- 75) contiguous pulse positions with no pulses of either positive or negative polarity from the incoming DS3 line.

OOF (Out Of Frame). On when any three or more errors within sixteen or fewer consecutive F-bits occurs within a DS3 M-frame.

AIS (Alarm Indication Signal). On when a maintenance signal is sent to the WSX by the network. If this LED is on, then there has been a change in the Alarm Indication Signal (AIS).

RAI (Remote Alarm Indication). On when an alarm signal is detected by the WSX module on the alarm channel.

CLK IN (Clocking Port). Balanced T1 port used when the module is set to use external clocking.



Module Label. This label indicates which platform the module is for

Port LEDs

Module LEDs

OK1 (Hardware Status). On Green when the module has passed diagnostic tests successfully. On Amber when the hardware has failed diagnostics or if the corresponding image file for the module is not in flash memory.

OK2 (Software Status). Blinking Green when the module software was downloaded successfully and the module is communicating with the MPM. Blinking Amber when the module is in a transitional state. On Solid Amber if the module failed to download software from the MPM.

Channelized DS3 Module With Four Ports

Channelized DS3 Module Configuration Overview

The channelized DS3 module uses DS3 lines to transmit data over a Frame Relay or PPP Wide Area Network. These DS3 lines can be run as clear channel lines (using the entire bandwidth of the connection) or channelized into 28 separate DS1 channels. Logical ports are assigned to these DS1 channels, which also may be run as clear channels or broken down further into DS0 time slots. Each DS1 has 24 DS0 time slots available, and a logical port can be assigned from 1-24 (the maximum) time slots. Time slots run at 64Kbps. There are 512 possible logical ports per channelized DS3 module daughtercard (2 DS3 physical ports).

When configuring the channelized DS3 module, the management menu is set up in a practical fashion to assist you in creating your WAN network.

◆ Note ◆

Many of the specifications for DS3, DS1, and logical ports will be decided by the specifications of the Frame Relay or PPP network provider.

When setting up the channelized DS3 module:

Step 1. Physical Configuration Of DS3 Ports

Initially, you will need to configure your DS3 ports on the physical level using the **ds3mod** command. This allows you to decide the clock source, line type, line length, and other physical parameters of your DS3 connection. See *Configuring a DS3 Port* on page 56-14 for specific procedures.

Step 2. Physical Configuration Of DS1 Channels

Next, if you are not running a DS3 clear channel, you will configure the physical aspects of the DS1 channels associated with the DS3 connection using the **ds1mod** command. Many of these parameters are similar to the DS3 parameters. See *Configuring a DS1 Channel* on page 56-24 for specific procedures.

Step 3. Creating Logical Ports

Once you have configured the DS3 ports, you can assign logical ports to these channels and configure them using the **lpadd** and **lpmod** commands. See *Adding a Logical Port Configuration* on page 56-33 and *Adding a Logical Port Configuration to a Clear Channel DS3 Port* on page 56-36 for details.

Step 4. Configuring Logical Port Protocols

Once logical ports are configured, you can modify the protocol configuration of each logical port (PPP or Frame Relay) with the **lppmod** command. See *Modify the Protocol Configuration of a Logical Port using PPP* on page 56-43 for instructions.

Step 5. Creating Virtual Circuits (Optional)

If you are using Frame Relay as your network protocol you can create virtual circuits with the **lfradd** command. See *Add Frame Relay DLCI on a Logical Port* on page 56-60 for procedures.

Step 6. Implementing Routing Options (Optional)

If your network uses IP routing, you can establish and modify router interfaces with the **riadd**, **ridel**, and **rimod** commands. For details, see *Adding a Router Interface* on page 56-62, and *Modifying a Router Interface Configuration* on page 56-63.

Step 7. Creating a Service (Optional)

If you need to create, modify, or delete a bridging or trunking service for a logical port, this is done with the **m013cas**, **m013das**, and **m013mas** commands. For details, see *Creating a Bridging or Trunking Service* on page 56-65,

When you have set up the channelized DS3 module, there are several commands that allow you to monitor the configuration and statistics of the DS3 ports, DS1 channels, clear channel logical port, and channelized logical ports.

The Channelized DS3 Module Management Menu

The user interface commands for configuring and monitoring the channelized DS3 module are listed in the **M013** submenu. This is located in the **Interface** menu of the main menu options. To access this submenu, enter

m013

followed by **<Enter>**, at the system prompt. If you are in verbose mode, a screen similar to the following is displayed. Otherwise, enter a question mark (?) to see the M013 menu commands:

	Command	M013 Port Management Menu
	m013	Enter M013 Port Management sub-menu
DS3 Commands	ds3mod	Modify M013 DS3 port configuration
	ds3dlts	Display 24-hour period statistics of a local DS3 port
	ds3dlcs	Display current 15-minute statistics of a local DS3 port
	ds3dlis	Display 15-minute interval statistics of a local DS3 port
	ds3clis	Clear interval statistics of a local DS3 port
	ds3dcs	Display DS3 port configuration and statistics
	ds3scs	Set DS1 statistics collection for DS3 port
DS1 Commands	ds1mod	Modify M013 DS1 port configuration
	ds1dlts	Display 24-hour period statistics of a local DS1 port
	ds1dlcs	Display current 15-minute statistics of a local DS1 port
	ds1dlis	Display 15-minute interval statistics of a local DS1 port
	ds1clis	Clear interval statistics of a local DS1 port
	ds1dcs	Display DS1 port configuration and statistics
Logical Port Commands	lpadd	Add logical port to M013 port configuration
	lpmod	Modify M013 logical port configuration
	lpdel	Delete logical port from M013 port configuration
	lpview	Display logical port configuration and statistics
	lpcls	Clear statistics of logical port
	lppmod	Modify protocol configuration of logical port
Virtual Circuit Commands	lppview	Display protocol configuration and statistics of logical port
	lppcls	Clear protocol statistics of logical port
	lpfradd	Add Frame Relay DLCI on a logical port
Routing Commands	lpfrdel	Delete Frame Relay DLCI on a logical port
	riadd	Add router interface
	rimod	Modify router interface
	ridel	Delete router interface
	riview	Display router interface
Service Commands	ricls	Clear statistics of router interface
	m013cas	Create bridging or trunking service on M013 port configuration
	m013das	Delete service from M013 port configuration
	m013vas	View service on M013 port configuration
	m013mas	Modify service on M013 port configuration
	m013cfgdel	Delete current M013 configuration
	Main Interface	File Security Summary System VLAN Services Networking Help

The following sections give a brief description of the above groups of commands.

Physical Configuration Commands

Physical configuration commands are provided to enable you to configure physical (i.e., DS3 & DS1) ports and to view and clear local statistics associated with these ports. They are comprised of DS3 commands and DS1 commands.

DS3 commands

DS3 commands, which include **ds3mod**, **ds3dlts**, **ds3dlcs**, **ds3dlis**, **ds3dcs**, **ds3scs**, and **ds3dms** allow you to configure and view statistics for any of the DS3 ports or clear channel DS3 in the channelized DS3 module. For configuration and statistics command details, see:

- *Configuring a DS3 Port* on page 56-14.
- *Viewing Cumulative Statistics and Errors of a Local DS3 Port* on page 56-17
- *Viewing Current 15-Minute Statistics and Errors of a Local DS3 Port* on page 56-19
- *Viewing 15-Minute Interval (Historical) Statistics and Errors of a Local DS3 Port* on page 56-20
- *Clearing Interval Statistics and Errors of a Local DS3 Port* on page 56-22,
- *Viewing Configuration and Statistical Parameters for a DS3 Port* on page 56-22.

DS1 commands

DS1 commands, which include **ds1mod**, **ds1dlts**, **ds1dlcs**, **ds1dlta**, and **ds1dcs**, allow you to configure and view statistics for any of the DS1 channels on a DS3 port.

For configuration and statistics command details, see:

- *Configuring a DS1 Channel* on page 56-24
- *Viewing Cumulative Statistics and Errors of a Local DS1 Channel* on page 56-26
- *Viewing Current 15-Minute Statistics of a Local DS1 Channel* on page 56-28
- *Viewing 15-Minute Interval Statistics and Errors of a Local DS1 Channel* on page 56-29,
- *Clearing Interval Statistics of a Local DS1 Channel* on page 56-31
- *Viewing Configuration and Statistical Parameters for a DS1 Channel* on page 56-32.

Logical Configuration Commands

Logical configuration commands are provided to enable you to configure logical ports and view and clear statistics associated with these ports.

A logical port uses HDLC encapsulation to carry Frame Relay or Point-to-Point traffic. It can have 1 or more DS0 time slots allocated, or it can run as a clear channel DS1 or DS3. The logical channel uses either PPP or Frame Relay to transmit data.

Further, you can create virtual circuits, router interfaces, and services for logical ports. They are comprised of logical port commands, virtual circuit commands, routing commands, and service commands.

Logical port commands

A logical port uses HDLC encapsulation to carry Frame Relay or Point-to-Point traffic. It can have 1 or more DS0 time slots allocated, or it can run as a clear channel DS1 or DS3. The logical channel will use either PPP or Frame Relay to transmit data. These commands, which include **lpadd**, **lpmo**, **lpdel**, **lpview**, **lpcls**, **lppmo**, **lppview**, and **lppcls**, allow you to create, modify, and delete logical ports, as well as modify and view statistics for the selected connection protocol (either PPP or Frame Relay).

For command details on creating, modifying, or deleting a logical port, see:

- *Adding a Logical Port Configuration* on page 56-33
- *Adding a Logical Port Configuration to a Clear Channel DS3 Port* on page 56-36
- *Deleting a Logical Port* on page 56-39.

For information on modifying or viewing the statistics of a logical port protocol configuration, see:

- *Modify the Protocol Configuration of a Logical Port using PPP* on page 56-43
- *Display Protocol Configuration and Statistics of a Logical Port using PPP* on page 56-50.

Virtual circuit commands

Virtual circuits are network connections that allow data traffic to be sent over Frame Relay. The virtual circuit commands, which include **lpfradd** and **lpfrdel**, allow you to create and delete virtual circuits from a logical port.

For command details on creating and deleting a virtual circuit, see:

- *Add Frame Relay DLCI on a Logical Port* on page 56-60
- *Delete Frame Relay DLCI on a Logical Port* on page 56-61

Routing commands

If your network uses IP routing, you will need to establish routing connections for the channelized DS3 module. The routing commands (which include **riadd**, **rimod**, **ridel**, **rview**, and **ricls**) allow you to create, delete, and view a router interface for the module.

For command details on creating, modifying, or deleting a router interface, see:

- *Adding a Router Interface* on page 56-62
- *Modifying a Router Interface Configuration* on page 56-63
- *Viewing Router Interfaces* on page 56-64

Service commands

If you want to use bridging or trunking on a logical port, you need to create a service for that logical port. This is done with the **m013cas**, **m013das**, and **m013mas** commands.

For details, see:

- *Creating a Bridging or Trunking Service* on page 56-65
- *Viewing Service Configurations* on page 56-67
- *Deleting Services* on page 56-67.

Configuring a DS3 Port

The **ds3mod** command configures a DS3 port at the physical level. It is generic to all such ports, regardless of the logical level service that controls them and regardless of the board type. To configure a DS3 port, enter the **ds3mod** command as follows:

```
ds3mod <slot>/<ds3port>
```

where **<slot>** is the slot number of the board on which the port is located and **<ds3port>** is the port number on the board you want to modify. For example, to modify port number 2 on switch slot 5, enter:

```
ds3mod 5/2
```

A screen similar to the following is displayed:

- 1) **Circuit Id (30 chars max) :**
- 2) **Framing Type { M23(1), C-bit(3) } :**
- 3) **Channelization { Channelized(1), Unchannelized(2) } :**
- 4) **Loopback Configuration {No Loop(1), Payload Loop(2), Line Loop(3) } :**
- 5) **DS3 Transmit Clock Source { Loop(1), Local(2) } :**
- 6) **DS1 Transmit Clock Source { Loop(1), Local (2), External (3) } :**
- 7) **Line Length {More than 255 feet(1), Less than 255 feet(2) } :**

Enter (option=value/save/cancel) :

You make changes to the options in this screen at the colon prompt (:). You do this by entering the line number of the option you want to change, an equal sign (=), and then the value for the new parameter.

For example, to set the **Line Type** to **M23**, you would enter **2** (the line number for **Framing Type**), and equals sign, and then **1** (the value that represents **M23**) as follows:

```
2=1
```

After you are finished, be sure to save your configuration changes by typing **save**.

Field Descriptions

The following section explains the fields in the **ds3mod** command and their corresponding values.

1) Circuit Identifier

Enter a textual description of the DS3 port, up to 30 characters. This text will be used in other screen displays to identify the port.

2) Line Type

Enter the physical format of the DS3 port. The line type chosen specifies the characteristics of the frame format. The possible line types for a DS3 port are:

M23(1)

Uses C-bits as stuff (null) bits to maintain the 7 rows by 8 column frame format.

C-bit(3)

Uses C-bits for specific uses (such as Far End Alarm and Control channels) rather than stuff bits.

3) Channelization

Specifies whether channelization is enabled or not. A channelized DS3 line maintains the distinctions of the 28 DS1 channels that account for the DS3's bandwidth. The possible values are **Channelized(1)** and **Unchannelized(2)**. If disabled, the DS3 line is a clear channel and the 28 DS1 channels are used together as a single line.

4) Loopback Configuration

This field is used for diagnostic purposes to set various receive-to-transmit data loops.

For both Frame Relay and PPP, loopback detection involves periodically transmitting a message and looking for that message to be received. When implementing Loopback Detection, it is important to keep two issues in mind: the message must not violate any standards; the message must be unique in such a way that it can be differentiated from a message sent by a remote node. For more on loopback detection, see Chapter 48, titled "Managing WAN Switching Modules (WSM)" of your switch manual.

Possible types are:

No Loop(1)

The port is not in a loopback state. This is the typical live network state for a DS3 port.

Payload Loop(2)

All 28 receive DS1s are looped back to the outgoing transmit DS1s. The received signal (bit level) at this DS3 port is looped through the port after passing through the port's framing functionality.

Line Loop(3)

The entire DS3 receive line is looped back to the outgoing DS3 transmit line. The received signal at this DS3 port does not go through the port's framing functionality, and is instead looped straight back out the transmit function of the port. This state should only be used for debugging purposes.

5) DS3 Transmit Clock Source

This field specifies the transmit clock timing source of the DS3 port. The possible values are:

Loop(1).

In loop timing, the transmit timing is recovered from the receive data stream and then the timing “looped” back onto the transmit data stream. This is different from loop diagnostics modes (see below), in which the actual receive data stream is looped back to the transmit data stream).

Local(2).

In local timing, the timing for the transmit data stream is generated internally, rather than using the clock recovered from the receive data stream of the DS3 port.

6) DS1 Transmit Clock Source

This field specifies the transmit clock timing source of the DS1 channel. The possible values are:

Loop(1).

In loop timing, the transmit timing is recovered from the receive data stream and then the timing “looped” back onto the transmit data stream. This is different from loop diagnostics modes (see below), in which the actual receive data stream is looped back to the transmit data stream).

Local(2).

In local timing, the timing for the transmit data stream is generated internally, rather than using the clock recovered from the receive data stream of the DS1 channel.

External (3)

In external timing, clocking is supplied from a reference clock such as a Stratum 1 or a GPS.

7) Line Length

Specify the line length of the cable to be used for this port. The available values for a DS3 port are **More than 255 feet(1)** or **Less than 255 feet(2)**. (255 feet is approximately 78 meters.)

Viewing Cumulative Statistics and Errors of a Local DS3 Port

The **ds3dlts** command allows you to view the statistics totals for events occurring during the past 24 hours on a single DS3 port. To view these statistics, enter the **ds3dlts** command as follows:

```
ds3dlts <slot>/<ds3port>/<option>
```

where **<slot>** is the slot number of the board the port is located on, **<ds3port>** is the port number on the board for which you want statistics, and **<option>** is the type of statistics you would like to display. Available options for this command are:

all. Both statistics and errors are shown in the command display.

stat. Only statistics are shown in the command display.

errors. Only errors are shown in the command display.

For example, to get the statistics for port number 3 on switch slot 2, enter:

```
ds3dlts 2/3/stat
```

A screen similar to the following is displayed:

```
Local Cumulative Total Statistics for DS-3 on Slot 2 /ds3port 3
Circuit Id: test
Valid intervals : 96 of 96, elapsed time (sec) : 504 of 900
  PES   PSES  SEFS   UAS   LES   CES   CSES
=====
      0     0     0     0     0     0     0
```

To get the errors for the same port, enter

```
ds3dlts 2/3/errors
```

A screen similar to the following is displayed;

```
Local Cumulative Total Errors for DS-3 on Slot 2/ds3port 3
Circuit Id: test
Valid intervals: 96 of 96, elapsed time (sec): 600 of 900
  LCV   PCV   CCV   REI
=====
      0     0     0     0
```

Using the option **all** with the **ds3dlts** command shows a combined display of both the statistics and the errors.

As a variation on this command, you can enter **ds3dlts <slot>/<option>**. This displays the statistics, errors, or both for all DS3 ports in a slot.

The following section explains the fields and their corresponding values.

Configuration Information

Circuit Identifier. The textual description of this DS3 port as configured through the `ds3mod` command.

Valid Intervals. This field indicates the number of 15-minute intervals for which valid statistics were gathered over the last 24 hours. Statistics may be gathered and stored for up to 96 15-minute intervals. The number of valid intervals displayed is 96, unless the interface was brought on-line within the last 24 hours.

Elapsed Time. This field indicates the number of seconds that have elapsed since the beginning of the current error-measurement 15-minute sample. This time will be reset to zero when a 15-minute session of statistics gathering is complete (and stored) and the next 15-minute interval begins.

Statistic and Errors Information

PES - P-bit Errored Seconds. A P-bit Errored Second is a second with one or more P-bit Coding Violations, one or more Out Of Frame defects, or a detected incoming Alarm Indication Signal. This counter is not incremented when Unavailable Seconds statistics are counted.

PSES - P-bit Severely Errored Seconds. A P-bit Severely Errored Second is a second with 44 or more P-bit Coding Violations, one or more Out Of Frame defects, or a detected incoming Alarm Indication Signal. This counter is not incremented when Unavailable Seconds statistics are counted.

SEFS - Severely Errored Framing Seconds. A Severely Errored Framing Second is a second with one or more Out Of Frame defects or a detected incoming Alarm Indication Signal. This statistic is not incremented during unavailable seconds.

UAS - Unavailable Seconds. Unavailable Seconds are calculated by counting the number of seconds that the interface is "unavailable". The DS3 interface is said to be unavailable from the onset of 10 contiguous P-bit Severely Errored Seconds, or the onset of the condition leading to a failure.

LES - Line Errored Seconds. A Line Errored Second is a second in which one or more Coding Violations occurred or one or more Loss Of Signal defects are detected.

CES - C-bit Errored Seconds. A C-bit Errored Second is a second with one or more C-bit coding violations, one or more Out Of Frame defects, or a detected incoming Alarm Indication Signal. This count is applicable only to SYNTRAN and C-bit Parity DS3 applications. This statistic is not incremented when Unavailable Seconds statistics are counted.

CSES - C-bit Severely Errored Seconds. A C-bit Severely Errored Second is a second with 44 or more C-bit coding violations, one or more Out Of Frame defects, or a detected incoming Alarm Indication Signal. This count is applicable only to SYNTRAN and C-bit Parity DS3 applications. This statistic is not incremented when Unavailable Seconds statistics are counted.

LCV - Line Coding Violations. This statistic is a count of both Bipolar Violations and Excess Zeros occurring during the sample period.

PCV - P-bit Coding Violations. A P-bit Coding violation error event is equivalent to P-bit Parity Error event. A P-bit Parity Error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally-calculated code.

CCV - C-bit Coding Violations. For C-bit Parity DS3 applications, this is the count of coding violations reported via the C-bits. Specifically, it is a count of CP-bit parity errors occurring in the sample period.

REI - Remote Error Indication. Also known as a Far End Block Error (FEBE). For C-bit parity applications, an indication that the far end equipment is receiving CCVs.

Viewing Current 15-Minute Statistics and Errors of a Local DS3 Port

The **ds3dlcs** command allows you to view the statistics totals for events occurring during the current 15-minute sample period on a single DS3 port. To view these statistics, enter the **ds3lcs** command as follows:

```
ds3dlcs <slot>/<ds3port>/<option>
```

where **<slot>** is the slot number of the board the port is located on, **<ds3port>** is the port number on the board for which you want statistics, and **<option>** is the type of statistics you would like to display. Available options for this command are:

all. Both statistics and errors are shown in the command display.

stat. Only statistics are shown in the command display.

errors. Only errors are shown in the command display.

For example, to get the statistics for port number 3 on switch slot 2, enter:

```
ds3dlcs 2/3/stat
```

A screen similar to the following is displayed:

```
Local Current 15-minute Statistics for DS-3 on Slot 2 /ds3port 3
Circuit Id: test
Valid intervals : 96 of 96, elapsed time (sec) : 504 of 900
  PES  PSES  SEFS  UAS  LES  CES  CSES
=====
      0      0      0      0      0      0      0
```

To view the errors for the same port, enter:

```
ds3dlcs 2/3/errors
```

A screen similar to the following is displayed:

```
Local Current 15-minute Errors for DS-3 on Slot 2/ds3port 3
Circuit Id: test
Valid intervals: 96 of 96, elapsed time (sec): 600 of 900
  LCV  PCV  CCV  REI
=====
      0      0      0      0
```

Using the option **all** with the **ds3dlcs** command shows a combined display of both the statistics and the errors.

As a variation to this command, you can enter **ds3dlcs <slot>/<option>**. This displays the statistics, errors, or both for all DS3 ports in a slot.

Definitions of the fields and columns in this display are the same as those used for the **ds3dlts** command. See *Viewing Cumulative Statistics and Errors of a Local DS3 Port* on page 56-17 for an explanation of these statistics.

Viewing 15-Minute Interval (Historical) Statistics and Errors of a Local DS3 Port

The **ds3dlis** command allows you to view the statistics totals for events occurring during all currently stored 15-minute sample periods on a single DS3 port. To view these statistics, enter the **ds3dlis** command as follows:

```
ds3dlis <slot>/<ds3port>/<option>
```

where **<slot>** is the slot number of the board on which the port is located, **<ds3port>** is the port number on the board for which you want to get statistics, and **<option>** is the type of statistics you would like to display. Available options for this command are:

all. Both statistics and errors are shown in the command display.

stat. Only statistics are shown in the command display.

errors. Only errors are shown in the command display.

For example, to get statistics for port number 3 on switch slot 2, enter:

```
ds3dlis 2/3/stat
```

A screen similar to the following is displayed:

```
Local 15-minute Interval Statistics for DS-3 on Slot 2/ds3port 3
Circuit Id: Alcatel DS3 Circuit
Valid Intervals : 96 of 96, elapsed time (sec): 47 of 900
# PES PSES SEFS UAS LEV CES CSES
== =====
 1 0 0 0 900 64636 19894 900
 2 0 0 0 900 64636 19894 900
 3 0 0 0 900 64636 19894 900
 4 0 0 0 900 64636 19894 900
 5 0 0 0 900 64636 19894 900
 6 0 0 0 900 64636 19894 900
 7 0 0 0 900 64636 19894 900
 8 0 0 0 900 64636 19894 900
 9 0 0 0 900 64636 19894 900
10 0 0 0 900 64636 19894 900
11 0 0 0 900 64636 19894 900
12 0 0 0 900 64636 19894 900
13 0 0 0 900 64636 19894 900
14 0 0 0 900 64636 19894 900
15 0 0 0 900 64636 19894 900
16 0 0 0 900 64636 19894 900
```

If more than 16 sample periods are stored, the following prompt will be displayed:

```
More? [<SPACE> for next page, <RETURN> for next line, Quit]
```

You can then step through the remaining samples either a line at a time by pressing **<Enter>**, or a page at a time by pressing **<space>**.

To view the errors for the same port, enter:

```
ds3dlis 2/3/errors
```

A screen similar to the following is displayed:

```

Local 15-minute Interval Errors for DS-3 on Slot 2/ds3port 3
Circuit Id: Alcatel DS3 Circuit
Valid Intervals : 96 of 96, elapsed time (sec): 47 of 900
#   LCV   PCV   CCV   REI
==  =====
 1     0     0     0    900
 2     0     0     0    900
 3     0     0     0    900
 4     0     0     0    900
 5     0     0     0    900
 6     0     0     0    900
 7     0     0     0    900
 8     0     0     0    900
 9     0     0     0    900
10     0     0     0    900
11     0     0     0    900
12     0     0     0    900
13     0     0     0    900
14     0     0     0    900
15     0     0     0    900
16     0     0     0    900

```

If more than 16 sample periods are stored, the following prompt will be displayed:

More? [`<SPACE>` for next page, `<RETURN>` for next line, Quit]

You can then step through the remaining samples either a line at a time by pressing `<Enter>`, or a page at a time by pressing `<space>`.

Using the option **all** with the **ds3dlis** command shows a combined display of both the statistics and the errors.

As a variation to this command, you can enter **ds3dlis <slot>/<option>**. This displays the statistics, errors, or both for all DS3 ports in a slot.

Definitions of the fields and columns in this display are the same as those used for the **ds3dlts** command. See *Viewing Cumulative Statistics and Errors of a Local DS3 Port* on page 56-17 for an explanation of these statistics.

Clearing Interval Statistics and Errors of a Local DS3 Port

The **ds3clis** command allows you to clear interval statistics on a port-by-port basis. (The **Elapsed Time** variable and all statistics in the displays are reset after you use the command.) To clear statistics on a given DS3 port:

1. Enter the **ds3clis** command as follows:

```
ds3clis <slot>/<ds3port>
```

where **<slot>** is the slot number of the board on which the port is located, and **<ds3port>** is the port number on the board for which you want to clear statistics. For example, to clear interval statistics on port 1 in switch slot 3, enter:

```
ds3clis 3/1
```

2. When you have done this and hit return, the following prompt is displayed:

```
Confirm to clear interval statistics of local DS3 port
```

```
Enter (option=yes/no)
```

3. Once you have confirmed your choice, a message similar to the following confirms the operation:

```
Port 3/1 interval statistics cleared
```

Viewing Configuration and Statistical Parameters for a DS3 Port

The **ds3dcs** command allows you to view configuration and statistical parameters for a DS3 port. To view these parameters, enter the **ds3dcs** command, as follows:

```
ds3dcs <slot>/<ds3port>
```

where **<slot>** is the slot number of the board on which the port is located and **<ds3port>** is the port number on the board for which you want to view configuration and statistical parameters. For example, to view configuration and statistical parameters for port 1 on the board in switch slot 3, enter:

```
ds3dcs 3/1
```

A screen similar to the following is displayed:

Configuration for DS-3 on Slot 3/ds3port 1:

```

-----
Circuit Id: test
Framing Type:          C-bit
Channelization:       Channelized
Loopback Configuration: NoLoop
Transmit Clock Source: Local
Line Length:          > 255 feet
Line Status Trap Generation: Enabled
Line Coding:
Valid intervals:      96 of 96
Elapsed time(sec):    600 of 900
Invalid intervals:    20
Line Status:          RcvRAIFailure
Line Status Changed:  0 days, 00:33:40.05
Loopback status:      NearEndPayloadLoopback

```

Local Current 15-minute Statistics and Errors:

```

-----
PES PSES SEFS UAS LEC CES CSES LCV PCV CCV REI
=====
0 0 0 0 0 0 0 0 0 0 0

```

Local Cumulative Total Statistics and Errors:

```

-----
PES PSES SEFS UAS LEC CES CSES LCV PCV CCV REI
=====
0 0 0 0 0 0 0 0 0 0 0

```

There are two variations to this command. You can view configuration and statistical parameters for all DS3 ports in a slot by entering **ds3dcs <slot>** followed by **<Enter>**, or you can view configuration parameters for an entire switch by entering the **ds3dcs** command by itself.

The following section explains the fields and their corresponding values.

Most of the definitions of the fields in this display are the same as those used for the **ds3mod** and **ds3dlts** commands. See *Configuring a DS3 Port* on page 56-14 and *Viewing Cumulative Statistics and Errors of a Local DS3 Port* on page 56-17 for an explanation of these fields and statistics.

Fields not described in those two sections are described below.

Invalid Intervals. Indicates the number of statistics intervals that were invalid due to errors or interruption.

Line Status. Indicates the current active alarms for the DS3 port. Possible alarms for a port are:

- **No Alarms.** No alarm is present.
- **RAI.** Remote alarm indication (RAI).
- **AIS.** Alarm indication signal (AIS) failure state.
- **OOF.** Out of frame (LOF) failure state.
- **LOS.** Loss of signal (LOS) failure state.

Configuring a DS1 Channel

The **ds1mod** command configures a DS1 channel as part of a DS3 line at the physical level. (It is generic to all such ports, regardless of the logical level service that controls them.)

To configure a DS1 port, enter the **ds1mod** command as follows:

```
ds1mod <slot>/<ds3port>/<ds1>
```

where **<slot>** is the slot number of the board on which the port is located, **<ds3port>** is the port number on the board you want to modify, and **<ds1>** is the DS1 channel number for the selected DS3 port. Since a channelized DS3 is comprised of 28 DS1 channels, the value for the DS1 channel must be 1-28. For example, to modify DS1 channel 14 for port number 2 on switch slot 5, enter:

```
ds1mod 5/2/14
```

A screen similar to the following is displayed:

- 1) Circuit Id (30 chars max):
- 2) Framing {ESF(1),D4(2)}
- 3) Loopback Config {No Loopback(1), Payload Loopback(2),
Line Loopback(3)} :
- 4) Send Code (ESF framing only) { No Code(1),
Line Code(2), Payload Code(3), Reset Code(4)}:

Enter (option=value/save/cancel) :

You make changes to the options in this screen at the colon prompt (:). You do this by entering the line number of the option you want to change, an equal sign (=), and then the value for the new parameter.

For example, to set the **Loopback Config** to **PayloadLoop** you would enter **3** (the line number for **Loopback Config**), an equals sign, and then **2** (the value that represents **PayloadLoop**).

After you have entered the required values, be sure to save your configuration.

As a variation of this command, you can enter **ds1mod <slot>/<ds3port>** at the system prompt without a specific DS1 channel number. Using the **ds1mod** command in this manner changes the settings for all 28 DS1 channels in a DS3 port.

Field Descriptions

The following section explains the fields and their corresponding values.

1) Circuit Identifier

Enter a textual description of this DS1 port, up to 30 characters. This text will be used in other screen displays to identify this DS1 port.

2) Line Type

Specify the frame format to be used on this port. The choices are Extended SuperFrame (**ESF**), or SuperFrame (**D4**). A T1 frame consists of 24 8-bit time slots and a 1-bit synchronization and control. Twelve (12) T1 frames can be grouped into a SuperFrame, and twenty-four (24) T1 frames can be grouped into an Extended SuperFrame.

The possible line types for a DS1 port are **ESF (1)** (Extended Superframe) and **D4 (2)** (Superframe).

3) Loopback Config

This field is used for diagnostic purposes to set various receive-to-transmit data loops. Possible types are:

No Loopback(1)

The port is not in a loopback state. This is the typical live network state for a DS1 port.

Payload Loopback(2)

Loopback all 24 receive DS0s on the DS1 to the outgoing transmit DS0 on the DS1 interface. The received signal (bit level) at this DS1 port is looped through the port after passing through the port's framing functionality.

Line Loopback(3)

Loopback the entire receive DS1 to the outgoing transmit DS1s. The received signal at this DS1 port does not go through the port's framing functionality, and is instead looped straight back out the transmit function of the port. This state should only be used for debugging purposes.

4) Send Code

Send codes are loopback commands sent in the Extended Superframe data link. If the remote device is configured to accept these commands, it will begin a loopback mode upon receiving them. The options specify what type of code is being sent across the DS1 interface by the device. Possible types are:

No Code(1)

Sending looped or normal data. No ESF datalink code is sent.

Line Code(2)

Sending a request for a DS1 line loopback. The received signal at this DS1 port does not go through the port's framing functionality, and is instead looped straight back out the transmit function of the port. This state should only be used for debugging purposes.

Payload Code(3)

Sending a request for a payload loopback (i.e., all DS1s in a DS3 frame). Loopback all 24 receive DS0s on the DS1 to the outgoing transmit DS0 on the DS1 interface. The received signal (bit level) at this DS1 port is looped through the port after passing through the port's framing functionality.

Reset Code(4)

Sending a request for loopback deactivation. It cancels a previous command for any of the three options above.

Setting DS1 Collection Statistics for a DS3 Port

In the interests of saving memory and enhancing performance, it is possible to determine which DS1 channels in a DS3 port are to be polled for statistics. To choose what specific DS1 channels are to be polled for statistics, enter the **ds3scs** command as follows:

```
ds3scs <slot>/<ds3port>
```

where **<slot>** is the slot number of the board on which the port is located and **<ds3port>** is the port number on the board for which you want to set DS1 channel collection statistics. For example, to set DS1 channel collection statistics for DS3 port 2 on slot 3, you would enter:

```
ds3scs 3/2
```

The following screen is displayed:

```
DS1 statistics collection for DS3 port 2/1
As the result of configuration change DS1 statistics may be reset

1) DS1 ports collecting statistics:
{1,2,3,4,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28}
DS1 ports not collecting statistics:
{5,6,7,8}
(Usage: "+/-<port|all>" add/remove ds1 port. For example,
"1=+10+12-9" to add ds1 port 10 & 12 and remove ds1 port 9.
"1=+all" add all ds1 ports. "1=-all" remove all ds1 ports)

Enter (option=value/save/cancel)
```

◆ Note ◆

Collecting statistics for more than six DS1 channels at one time will negatively affect the performance of the module.

Viewing Cumulative Statistics and Errors of a Local DS1 Channel

The **ds1dlts** command allows you to view statistics for events occurring during the past 24 hours on a single port. To view these statistics, enter the **ds1dlts** command as follows:

```
ds1dlts <slot>/<ds3port>/<ds1>/<option>
```

where **<slot>** is the slot number of the board on which the port is located, **<ds3port>** is the port number on the board, **<ds1>** is the DS1 channel for which you want to view statistics or errors, and **<option>** is the type of statistics you would like to display. Available options for this command are:

all. Both statistics and errors are shown in the command display.

stat. Only statistics are shown in the command display.

errors. Only errors are shown in the command display.

For example, to get statistics for DS1 channel 2 on port number 1 on switch slot 3, enter:

```
ds1dlts 3/1/2/stat
```

A screen similar to the following is displayed:

```
Local Cumulative Total Statistics for DS-1 #2 on Slot 3/ds3port 1
Circuit Id: test
Valid Intervals : 96 of 96, elapsed time (sec): 421 of 900
   ES   BES   SES   SEFS   DM   UAS
=====
   1111  1112  1113  1114  1115  1116
```

To view the errors for the same port, enter:

```
ds3dlts 3/1/2/errors
```

A screen similar to the following is displayed:

```
Local Cumulative Total Errors for DS-1 #2 on Slot 3/ds3port 1
Circuit Id: test
Valid Intervals : 96 of 96, elapsed time (sec): 421 of 900
   PCV
=====
   1111
```

Using the option **all** with the **ds1dlts** command shows a combined display of both the statistics and the errors.

As a variation of this command, you can enter **ds1dlts <slot>/<ds3port>/<option>** to display all of the DS1 channels configured for a single DS3 port.

Field Descriptions

The following section explains the fields and their corresponding values.

Configuration information

Circuit Identifier. The textual description of this DS1 port as configured through the **ds1mod** command.

Valid Intervals. Indicates the number of 15-minute intervals for which valid statistics were gathered during the previous 24 hours. Statistics may be gathered for up to 96 15-minute intervals during a 24-hour period.

Elapsed Time. The number of seconds that have elapsed during this 15-minute interval of gathering statistics. This time will be reset to zero when a 15-minute session of statistics gathering is complete (and stored) and the next 15-minute interval begins.

Statistics information

ES - Errored Seconds. For T1-ESF and E1-CRC conditions, this is a second with one or more Path Code Violations, one or more out-of-frame defects, one or more controlled slip errors, or an AIS error.

BES - Bursty Errored Seconds. The number of seconds with fewer than 320 but more than one (1) Path Code Violation error (see below for definition), no Severely Errored Frame errors, and no AIS errors.

SES - Severely Errored Seconds. For T1-ESF frames, this is a second with 320 or more Path Code Violation errors, one or more out-of-frame defects, or an AIS error. For E1-CRC conditions, this is a second with 832 or more Path Code Violation errors, or one or more out-of-frame defects. For E1-noCRC signals, this is a second with 2048 or more Line Code Violation errors. For D4/(SF) frames, this is a second with framing errors, an out-of-frame error, or a second with 1544 or more line code violation errors.

SEFS - Severe Errored Framing Second. A second with one or more out-of-frame errors or an AIS error.

DM - Degraded Minutes. The number of minutes in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.

UAS - Unavailable Seconds. The number of seconds this port was unavailable for transmitting or receiving data. In general, a port is unavailable after 10 consecutive Severely Errored Seconds or after a failure on the interface occurs.

PCV - Path Code Violations. A frame synchronization bit error in EF/D4 and E1-noCRC frames, or a CRC or frame synchronization error in the T1-ESF (Extended Super Frame) and E1-CRC frames.

Viewing Current 15-Minute Statistics of a Local DS1 Channel

The **ds1dlcs** command allows you to view the statistics totals for events occurring during the current 15-minute sample period on a single DS1 port. To view these statistics, enter the **ds1dlcs** command as follows:

```
ds1dlcs <slot>/<ds3port>/<ds1>/<option>
```

where **<slot>** is the slot number of the board the port is located on, **<ds3port>** is the port number on the board, **<ds1>** is the DS1 channel for which you want to view statistics, and **<option>** is the type of statistics you would like to display. Available options for this command are:

all. Both statistics and errors are shown in the command display.

stat. Only statistics are shown in the command display.

errors. Only errors are shown in the command display.

For example, to get statistics for DS1 channel 2 on port number 1 of switch slot 3, enter

```
ds1dlcs 3/1/2/stat
```

A screen similar to the following is displayed:

```
Local Current 15-minute Statistics for DS-1 #2 on Slot 3/ds3port 1
Circuit Id: test
Valid Intervals : 96 of 96, elapsed time (sec): 421 of 900
  ES   BES   SES   SEFS   DM   UAS
=====
 1111  1112  1113  1114  1115  1116
```

To view the errors for the same channel, enter

```
ds3dlcs 3/1/2/errors
```

A screen similar to the following is displayed:

```

Local Cumulative Total Errors for DS-1 #1 on Slot 2/ds3port 1
Circuit Id: test
Valid Intervals : 96 of 96, elapsed time (sec): 421 of 900
PCV
=====
1111

```

Using the option **all** with the **ds1dlcs** command shows a combined display of both the statistics and the errors.

As a variation of this command, you can enter **ds1dlcs <slot>/<ds3port>/<option>** to display all of the DS1 channels configured for a single DS3 port.

Definitions of the fields and statistics columns in this display are the same as those used for the **ds1dlts** command. See *Viewing Cumulative Statistics and Errors of a Local DS1 Channel* on page 56-26 for an explanation of these statistics.

Viewing 15-Minute Interval Statistics and Errors of a Local DS1 Channel

The **ds1dlis** command allows you to view the statistics and errors totals for events occurring during all currently stored 15-minute sample periods on a single DS1. To view these statistics, enter the **ds1dlis** command as follows:

```
ds1dlis <slot>/<port>/<ds1>/<option>
```

where **<slot>** is the slot number of the board on which the port is located, **<port>** is the port number on the board, **<ds1>** is the channel for which you want to view statistics, and **<option>** is the type of statistics you would like to display. Available options for this command are:

all. Both statistics and errors are shown in the command display.

stat. Only statistics are shown in the command display.

errors. Only errors are shown in the command display.

For example, to get statistics for channel 3 on port 1 on the board in switch slot 2, enter:

```
ds1dlis 2/1/3/stat
```

Configuring a DS1 Channel

A screen similar to the following is displayed:

```
Local 15-minute Interval Statistics for DS-1 #3, on Slot 2/ds3port 1
Circuit Id: test
Valid Intervals: 96 of 96, elapsed time (sec): 600 of 900
#   ES   BES   SES   SEFS   DM   UAS
==  =====
 1   0     0     0    900 64636 19894
 2   0     0     0    900 64636 19894
 3   0     0     0    900 64636 19894
 4   0     0     0    900 64636 19894
 5   0     0     0    900 64636 19894
 6   0     0     0    900 64636 19894
 7   0     0     0    900 64636 19894
 8   0     0     0    900 64636 19894
 9   0     0     0    900 64636 19894
10   0     0     0    900 64636 19894
11   0     0     0    900 64636 19894
12   0     0     0    900 64636 19894
13   0     0     0    900 64636 19894
14   0     0     0    900 64636 19894
15   0     0     0    900 64636 19894
16   0     0     0    900 64636 19894
```

If more than 16 sample periods are stored, the following prompt will be displayed:

```
More? [<SPACE> for next page, <RETURN> for next line, Quit]
```

You can then step through the remaining samples either a line at a time pressing **<Enter>** or a page at a time by pressing **<space>**.

To view the errors for the same channel, enter:

```
ds1dlis <slot>/<ds3port>/<ds1>/errors
```

This displays a screen similar to the following:

```
Local 15-minute Interval Errors for DS-1 #3, on Slot 2/ds3port 1
Circuit Id: test
Valid Intervals: 96 of 96, elapsed time (sec): 600 of 900
#   PCV
==  =====
 1   0
 2   0
 3   0
 4   0
 5   0
 6   0
 7   0
 8   0
 9   0
10   0
11   0
12   0
13   0
14   0
15   0
16   0
```

If more than 16 sample periods are stored, the following prompt will be displayed:

```
More? [<SPACE> for next page, <RETURN> for next line, Quit]
```

You can then step through the remaining samples either a line at a time by pressing **<Enter>**, or a page at a time by pressing **<space>**.

Definitions of these fields and statistics columns in this display are the same as those used for the **ds1dlts** command. See *Viewing Cumulative Statistics and Errors of a Local DS1 Channel* on page 56-26 for an explanation of these statistics.

Clearing Interval Statistics of a Local DS1 Channel

The **ds1clis** command allows you to clear interval statistics on a port-by-port, DS1 channel-by-channel basis. (The **Elapsed Time** variable and all statistics in displays are reset after you use the command.) To clear statistics on a given DS1 port:

1. enter the **ds1clis** command as follows:

```
ds1clis <slot>/<ds3port>/<ds1>
```

where **<slot>** is the slot number of the board on which the port is located, **<ds3port>** is the port number on the board, and **<ds1>** is the DS1 channel for which you want to clear statistics. For example, to clear interval statistics for channel 1 on port 1 in switch slot 3, enter:

```
ds1clis 3/1/1
```

2. When you have done this and hit return, the following prompt is displayed:

```
Confirm to clear interval statistics of local DS1 port
```

```
Enter (option=yes/no)
```

3. When you have confirmed your choice to clear the statistics, a message similar to the following confirms the operation:

```
Port 3/1/1 interval statistics cleared
```

Viewing Configuration and Statistical Parameters for a DS1 Channel

The **ds1dcs** command allows you to view configuration and statistical parameters for a DS1 port. To view these parameters, enter the **ds1dcs** command as follows:

```
ds1dcs <slot>/<ds3port>/<ds1>
```

where **<slot>** is the slot number of the board on which the port is located, **<ds3port>** is the port number on the board, and **<ds1>** is the DS1 channel for which you want to view configuration and statistical parameters. For example, to view configuration and statistical parameters for DS1 channel 1 for DS3 port1 on the board in switch slot 3, enter:

```
ds1dcs 3/1/1
```

A screen similar to the following is displayed:

Configuration for DS-1 #2 on Slot 3/ds3port 1:

```
-----
Circuit Id: test                Loopback Config: NoLoop
Framing:                        ESF                Send Code: SendNoCode
Valid intervals:                96 of 96        Trap Generation: enabled
Elapsed Time (sec):            600 of 900
Invalid intervals:              20
Line status:                    RcvRAIFailure,
Line Status Changed:            0 days, 00:33:40.05
Loopback status:                NearEndPayloadLoopback
```

Local Current 15-minute Statistics and Errors:

```
-----
      ES   BES   SES   SEFS   DM   UAS   PCV
-----
    1111  1112  1113  1114  1115  1116  1117
```

Local Cumulative Total Statistics and Errors:

```
-----
      ES   BES   SES   SEFS   DM   UAS   PCV
-----
    1111  1112  1113  1114  1115  1116  1117
```

There are two variations of this command. You can enter **ds1dcs <slot>/<ds3port>** to view configuration and statistical parameters for all DS1 channels on a DS3 port, or you can enter **ds1dcs <slot>** and view configuration and statistical parameters for all DS1 channels on an entire channelized DS3 module.

All of the definitions for fields in this display are the same as those used for the **ds1mod** and **ds1dlts** commands. See *Configuring a DS1 Channel* on page 56-24 and *Viewing Cumulative Statistics and Errors of a Local DS1 Channel* on page 56-26 for an explanation of these fields and statistics.

Adding a Logical Port Configuration

The **lpadd** command allows you to create a logical port. A logical port is an HDLC channel used to transmit data, and can be assigned up to 24 time slots from a DS1.

To add a logical port, perform the following steps:

1. Enter the **lpadd** command as follows:

```
lpadd <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the HDLC channel or logical port number that identifies the new logical port. If you want to assign the next available logical port number, you can type an asterisk (*) instead of a specific logical port number. For example, to add a logical port number 1 to physical port 2 in switch slot 3, enter:

```
lpadd 3/2/1
```

A screen similar to the following is displayed:

```
Adding logical port: slot 3, ds3port 1, logical port 1
1) ds1 channel {1-28} : 0
2) Protocol {PPP(0), FR(1)} : PPP
3) Change channel mask (0x000000 - 0xFFFFF) : 0x000000
 31) Add starting ds0 channel of the group (1-24) : 0
 32) Add number of ds0 channels in the group (1-24): 0
 33) Group add to mask (1) or clear in the mask (2)
 34) ds0 channels (time slots) used {}
      channels available: {9,10,11,12,13,14}
(Usage: "+/-<ts/all)" add/remove time slot. For example,
"5=+10+12-9" to add time slot 10 and 12 and remove time slot 9.
"5=+all" to add all time slots. "5=-all" remove all time slots)
```

```
Enter (option=value/save/cancel) :
```

2. Make changes to the options in this screen at the colon prompt (:) by entering the line number of the option you want to change, an equal sign (=), and then the value for the new parameter.

For example, to change the logical port protocol to Frame Relay, you would enter 2 (the line number for protocol), and equals sign, and then a 1 (the value for Frame Relay) as follows:

2=1

3. After you have entered the required values, be sure to save your configuration.

◆ Note ◆

When creating a logical port, either by assigning it a specific number or selecting the next available number, it is important to keep a record of this as it uniquely identifies the logical port and is required when using other logical port commands. Logical port numbers cannot be duplicated on the same module.

Field Descriptions

The following section explains the fields and their corresponding values.

1) ds1channel {1-28}

The logical port must be assigned to one of the 28 DS1 channels of a DS3 line. Since a channelized DS3 consists of 28 DS1 channels, this number must be between 1 and 28.

◆ Note ◆

More than one logical port can be assigned to a DS1 as long as the two logical ports are not assigned to use the same set of DS0 time slots.

2) Protocol {PPP(0), FR(1)}

The protocol this logical port will use to transmit data, either Point-to-Point Protocol (**PPP (0)**) or Frame Relay (**FR (1)**).

3) Change channel mask (0x000000 - 0xFFFFFFFF)

A hexadecimal number assigned to this logical port indicating which DS0s have been assigned to the logical port.

31) Add starting ds0 channel of the group (1-24)

Select the first DS0 time slot number the logical port will use for data traffic. Since there are 24 time slots in a DS1 channel, this number must be between 1 and 24. For example, if you wish to have this logical port begin with time slot 5, you would enter that number for this parameter.

32) Add number of ds0 channels in the group (1-24)

Select the number of DS0 time slots to add to the starting DS0 time slot. Using the above example, if you wanted to have this logical port use 4 time slots total, you would enter 3 for this parameter. This logical port would now use DS0 time slots 5, 6, 7, and 8 of this DS1 channel.

33) Group add to mask (1) or clear in the mask (2)

Decide whether the DS0 group is added to the logical port mask or if it will be clear in the mask.

◆ Note ◆

Once a DS0 time slot is assigned to a logical port, it cannot be used in another logical port unless it is first removed from the initial assignment.

34) ds0 channels (time slots) used

Displays a list of the specific DS0 time slots being used by this logical port.

Adding a Logical Port Configuration to a Clear Channel DS3 Port

If a DS3 port is configured to be a clear channel port, it is still possible to add a logical port that encompasses the entire clear channel.

To add a logical port to a clear channel DS3:

1. Using the **ds3mod** command, configure the DS3 port as described in *Configuring a DS3 Port* on page 56-14. Change the **Channelization** option to **Unchannelized** by entering a **3** (the line number for **Channelization**), an equal sign (=), and a **2** (the value for **Unchannelized**) at the system prompt, as shown:

```
3=2
```

This setting allows the DS3 to run as a single line using its full bandwidth. Remember to save your configuration.

2. Use the **lpadd** command as described in *Adding a Logical Port Configuration* on page 56-33. Instead of the regular **lpadd** screen, an abbreviated version appears, as shown:

```
Adding clear channel logical port: slot 2. ds3port 1, logical port 511
1) Protocol {PPP(0), FR(1)}: PPP
```

```
Enter (option=value/save/cancel) :
```

Choose either Point-to-Point Protocol or Frame Relay as your transmission protocol at the system prompt. For example, to select Frame Relay you would enter **1** (the line number), and equal sign (=), and **1** (the value for Frame Relay), as shown:

```
1=1
```

3. Remember to save your configuration when you are finished.

Modifying a Logical Port Configuration

The **lpmod** command allows you to modify a logical port to the M013 configuration. To modify the configuration of a logical port, perform the following steps:

1. Enter the **lpmod** command as follows:

```
lpmod <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port as designated when the port was created. For example, to modify logical port number 1 for physical port 2 on slot 3, enter:

```
lpmod 3/2/1
```

A screen similar to the following is displayed:

```

Logical port configuration:
slot 3, ds3port 2, ds1channel 10, logical port 1
operState Enabled, ds0 channel mask 0x000000
1) Logical port descriptor (30 chars max)      :
2) Protocol {PPP(0), FR(1)}                   : PPP
3) Administrative state {enabled(1), disabled(2)}: Enabled
4) ds0 channels (time slots) used: {}
      channels available: { 1,2,3,4,5,6,7,8,9,10,11,12,
                          13,14,15,16}
(Usage: "+/-<ts/all)" add/remove time slot. For example,
"5=+10+12-9" to add time slot 10 and 12 and remove time slot 9.
"5=+all" to add all time slots. "5=-all" remove all time slots)
    
```

Enter (option=value/save/cancel) :

2. Make changes to the options in this screen at the colon prompt (:). You do this by entering the line number of the option you want to change, an equal sign (=), and then the value for the new parameter.

For example, if you wanted to change the **Administrative state** to **disabled**, you would enter 3 (the line number for **Administrative state**), an equal sign, and then 2 (the number for **disabled**), as follows:

```
3=2
```

3. After you have entered the required values, be sure to save your configuration.

◆ **Note** ◆

Once you have created a logical port and assigned it to a DS3 port and DS1 channel, it remembers this information. Thus you will not need to enter those parameters when using this and other logical port commands.

Field Descriptions

The following section explains the fields and their corresponding values.

1) Logical port descriptor (30 chars max)

A textual description of the logical port. This is how the logical port will be identified in other UI screens. It can be up to thirty (30) characters long.

2) Protocol {PPP(0), FR(1)}

The protocol this logical port will use to transmit data, either Point-to-Point Protocol (**PPP (0)**) or Frame Relay (**FR (1)**).

3) Administrative state {enabled(1), disabled(2)}

This field indicates the Administrative State of the logical port, which can be either Enabled or Disabled. If **enabled**, the logical port has been enabled and can transmit data as long as its Operational State is also **enabled**. If the Admin Status is **disabled**, the port will not pass data.

4) ds0 channels (time slots) used

Displays a list of the specific DS0 time slots being used by this logical port.

Deleting a Logical Port

The **lpdel** command allows you to delete a logical port from the M013 configuration. To delete a logical port, perform the following steps:

1. Enter the **lpdel** command as follows:

```
lpdel <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port as designated when the port was created. For example, to delete a logical port number 1 for physical port 2 on slot 3, enter:

```
lpdel 3/2/1
```

A screen similar to the following is displayed:

```
Confirm to delete logical port 1, ds3port 2 on slot 3
```

```
Enter (option=yes/no) :
```

2. Confirm deletion by entering **yes** at the colon prompt (:) followed by **<Enter>**. The following message should be displayed:

```
Changing configuration ...
```

```
Logical port 1 for ds3port 2 on slot 3 deleted
```

Viewing Logical Port Configuration and Statistics

The **ipview** command allows you to view logical port configuration and statistics.

To view logical port configuration and statistics, enter the **ipview** as follows:

```
ipview <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port as designated when the port was created. For example, to view the statistics for logical port 27 for port 3 on slot 2, enter:

```
ipview 2/3/27
```

A screen similar to the following is displayed:

```
Configuration of logical port 27 2/3/27
DS1 channel:3           Descriptor:
DS0 channels (time slots) used: {}
DS0 channel mask: 0x000000 Protocol: Frame Relay
Daughter card: 1       Speed: 0
Administrative state: Enabled Status change time: 0 days, 00:00:00.00
Operational state: Enabled

Statistics of logical port 27 on slot 2
TxOctetCount:          1      RxOctetCount:           7
TxUniCount:            22     RxUniCount:            88
TxMcCount:             333    RxMcCount:             999
TxBcCount:            4444    RxBcCount:            1111
TxBufDiscard:         55555   RxBufDiscard:         22222
TxErrorDiscard:      666666   RxErrorDiscard:      333333
DelayExceedDiscard:   4       VseDiscardTxFull:     55
MtuExceedDiscard:    666     FloodLimitDiscard:   999999
VlanFiltered:         7777    PortFiltered:         88888
UnknownProtos:       1111111  OutQLen:              5518
```

There are three variations of this command. You can enter **ipview <slot>/<ds3port>** to show the statistics of all logical ports for the selected port, **ipview <slot>** to show the statistics for all logical ports on the selected slot, and **ipview** alone to show the statistics for all logical ports in the switch. To see the next set of logical port statistics, press the space bar.

Field Descriptions

The following section explains the fields and their corresponding values.

Configuration information

DS 1 channel. The DS1 channel number for this logical port.

DS 0 channels (time slots) used. A list of the DS0 timeslots used in this logical port.

Descriptor. This field is a textual description of the configured logical port (up to a maximum of thirty characters) as created with the **lpmo**d command.

DSO Channel Mask. This field is a hexadecimal number used to mask the channel number for security purposes.

Protocol. This field indicates the Protocol Type, which can be either Frame Relay or Point-to-Point Protocol (PPP).

Daughter Card. This field indicates which daughtercard of the channelized DS3 module the logical port uses.

Speed. This column indicates the speed of the logical port, expressed in bits per second (bps).

Administrative State. This field indicates the Administrative State of the logical port, which can be either Enabled or Disabled. If **Enabled**, the logical port has been enabled and can transmit data as long as its Operational State is also **enabled**. If the Admin Status is **Disabled**, the port will not pass data.

Operational State. This field indicates the Operational State of the logical port, which can either be enabled or disabled. If **enabled**, the port is capable of passing data as long as it has been logically enabled at the Administrative level. If **disabled**, the port cannot pass data because the port is administratively down. If the Operational State displays **LB**, the port is currently in Loopback (test) mode.

Status Change Time. This field refers to the system time when the last change in line status occurred to this logical port.

Statistics information

TxOctetCount. The total number of octets, or bytes, transmitted from this logical port since the last time the switch was initialized.

RxOctetCount. The total number of octets, or bytes, received on this logical port since the last time the switch was initialized. This statistic includes the data and Frame Relay header fields, but does not include CRC or flag characters.

TxUniCount. The number of unicast frames transmitted on this logical port to a higher layer protocol since the last time the switch was initialized.

RxUniCount. The number of unicast frames received by this logical port from a higher level protocol since the last time the switch was initialized.

TxMcCount. The number of multicast frames transmitted on this logical port to a higher layer protocol since the last time the switch was initialized.

RxMcCount. The number of multicast frames received by this logical port from a higher level protocol since the last time the switch was initialized.

TxBcCount. The number of broadcast frames transmitted on this logical port to a higher layer protocol since the last time the switch was initialized.

RxBcCount. The number of broadcast frames received by this logical port from a higher level protocol since the last time the switch was initialized.

TxBufDiscard. For transmissions from this logical port, the number of frames discarded due to a lack of buffer space.

RxBufDiscard. For data received by this logical port, the number of frames discarded due to a lack of buffer space.

TxErrorDiscard. For transmissions from this logical port, the number of frames discarded due to errors.

RxErrorDiscard. For data received by this logical port, the number of frames discarded due to errors.

DelayExceedDiscard. Number of frames that were delayed, usually due to collisions, but were ultimately transmitted.

VseDiscardTxFull. The number of frames that were discarded due to a lack of VSE transmit buffer space.

MtuExceedDiscard. The number of frames that have been discarded because they exceeded the maximum transmission unit (MTU) size. See *Adding a Logical Port Configuration to a Clear Channel DS3 Port* on page 56-36 for information on setting the MTU size.

FloodLimitDiscard. The number of frames discarded due to exceeding the flood limit of this logical port. Flooding occurs when the frame's destination is not known, so it is sent out to all devices in a VLAN or segment ring.

VlanFiltered. The number of frames discarded due to not being able to find a matching VLAN.

PortFiltered. The number of frames discarded due to not being able to find a matching virtual port.

UnknownProtos. The number of unknown protocols encountered by this logical port.

OutQLen. The number of packets in the output packet queue.

Clear Statistics for a Logical Port

The **lpcls** command allows you to clear statistics associated with a logical port. To clear statistics:

1. Enter the **lpcls** command as follows:

```
lpcls <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port as designated when the port was created. For example, to clear the statistics for logical port 27 on port 3 of slot 2, enter:

```
lpcls 2/3/27
```

The following message will be displayed:

```
Confirm to clear statistics of logical port
```

```
Enter (option=yes/no):
```

2. Enter **yes** and hit **<Enter>** to clear the statistics. A message similar to the one below will appear to verify the operation:

```
Statistics of logical port 27 on port 3 for slot 2 cleared
```

3. There are three variations of this command. Enter **lpcls <slot>/<ds3port>** to clear the statistics for all logical ports on the selected port, **lpcls <slot>** to clear the statistics of all logical ports for the selected slot, or **lpcls** to clear the statistics for all logical ports in the switch.

Modify the Protocol Configuration of a Logical Port using PPP

The **lppmod** command allows you to modify the configuration of a logical port protocol (either PPP or Frame Relay). There is a separate display for PPP and Frame Relay protocol configurations. (You can set the type of protocol a logical port uses with the **lpmmod** command. See *Adding a Logical Port Configuration to a Clear Channel DS3 Port* on page 56-36 for details.)

To modify a port protocol configuration for a logical port using PPP, perform the following steps:

1. Enter the **lppmod** command as follows:

```
lppmod <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port as designated when the port was created.

For example, to modify the protocol of logical port 27 on port 3 of slot 2, enter:

```
lppmod 2/3/27
```

If the logical port is using PPP, then a screen similar to the following is displayed:

```
Protocol configuration of PPP
logical port 27, descriptor:
slot 2, ds3port 3, ds1channel 10
ds0 channel mask 0x000000
1) Administrative state {enabled(1), disabled(2)}           : Enabled
2) Bridging admin state {enabled(1), disabled(2)}         : Enabled
   21) Bridging group {1-65535}                             : 3
   22) PPP bridging mode {BridgeAll(1), BridgeEthernet(2)} : BridgeEthernet
3) IP routing admin state {enabled(1), disabled(2)}       : Enabled
   31) Remote IP Address                                     : 255.255.255.255
   32) Local IP Address                                     : 255.255.255.255
4) Authentication type {None(1), PAP(2), CHAP(3)}         : None
   41) Remote user Id (8 chars max)                         : TESTReId
   42) Remote password (8 chars max)                       : TESTRePw
   43) Local user Id (8 chars max)                         : TESTLoId
   44) Local password (8 chars max)                        : TESTLoPw
5) Max failure count {1-65535}                             : 4
6) Max configure count {1-65535}                           : 5
7) Max terminate count {1-65535}                           : 6
8) Max timeout count {1-65535}                             : 7
```

```
Enter (option=value/save/cancel) :
```

2. Make changes to the options in this screen at the colon prompt (:). You do this by entering the line number of the option you want to change, an equal sign (=), and then the value for the new parameter.

For example, to change the **Max configure count** to 10, you would enter 7 (the line number for **Max configure count**), then an equals sign, then 10, as follows:

```
7=10
```

3. After you have entered the required values, be sure to save your configuration.

Field Descriptions for Logical Port using PPP

1) Administrative state {enabled(1), disabled(2)}

This field indicates the Administrative State of the logical port, which can be either Enabled or Disabled. If **Enabled**, the logical port has been enabled and can transmit data as long as its Operational State is also **enabled**. If the Admin Status is **Disabled**, the port will not pass data.

2) Bridging admin state {enabled(1), disabled(2)}

This field allows you to enable or disable the Bridging function for this PPP logical port.

21) Bridging group {1-65535}

Indicates the VLAN Group to be used for PPP Bridging. A value of zero (0) indicates that this PPP Entity will not perform a bridging service and will discard all bridged format packets received or transmitted.

22) PPP bridging mode {BridgeAll(1), BridgeEthernet(2)}

This field allows you to select the operational mode for bridging. The options are **BridgeEthernet**, which enables bridging on Ethernet interfaces only, or **BridgeAll**, which enables it for all interfaces.

3) IP routing admin state {enabled(1), disabled(2)}

This field is used to enable or disable the routing of IP packets over PPP. The options are **Enabled** or **Disabled**.

31) Remote IP Address

This field allows you to specify the Remote IP address of the PPP connection when IP routing is enabled. Valid IP address notation must be used. If this parameter is set to 0.0.0.0 and IP routing is enabled, the Remote IP address will be learned during Internet Protocol Control Protocol (IPCP) negotiation.

32) Local IP Address

This field allows you to specify the local IP address for this logical port, if IP routing is enabled. Valid IP notation must be used.

4) Authentication type {None(1), PAP(2), CHAP(3)}

Specifies the type of authentication that is to be expected on incoming calls. The options are **None**, **PAP** (Password Authentication Protocol), and **CHAP** (Challenge Handshake Authentication Protocol). Set this parameter to the type of authentication that you expect your callers to be using. If you enable either PAP or CHAP authentication, the next two parameters must also be set (remote user ID and password), or the caller's connection requests will be refused. If you set this parameter to **None**, you must also set the Default Bridge and IP Configuration Administration Status parameters or the caller's connection requests will be refused. See Chapter 50, titled "Point-to-Point Protocol" of your switch manual for more details on PAP and CHAP.

41) Remote user Id (8 chars max)

Specifies the User ID expected from the remote end during PAP or CHAP authentication.

42) Remote password (8 chars max)

Specifies the password expected from the remote end during PAP or CHAP authentication.

43) Local user Id (8 chars max)

Specifies the User ID to be sent to the remote end during PAP or CHAP authentication. This parameter is used only for outgoing calls.

44) Local password (8 chars max)

Specifies the password sent to the remote end during PAP or CHAP authentication. This parameter is used only for outgoing calls.

5) Max failure count {1-65535}

The maximum number of times a CONFIGURATION_REQUEST packet will be sent when the previous attempts received responses, but did not receive a CONFIGURATION_ACK. This counter applies to all Link Control Protocol (LCP) and Network Control Protocol (NCP) negotiations.

6) Max configure count {1-65535}

The maximum number of times a CONFIGURATION_REQUEST packet will be sent when the previous attempts did not receive any responses. This counter applies to all LCP and NCP negotiations.

7) Max terminate count {1-65535}

The maximum number of TERMINATE_REQUEST packets that will be sent without receiving a TERMINATE_ACK packet. This counter applies to all LCP and NCP negotiations.

8) Max timeout count {1-65535}

Indicates the number of seconds to wait between CONFIGURATION_REQUEST retries that do not receive a response. This timeout value applies to all LCP and NCP negotiations.

Modify the Protocol Configuration of a Logical Port using Frame Relay

The **lppmod** command displays a different screen than the one described above if you want to modify the configuration of a logical port protocol using Frame Relay. (You can set the type of protocol a logical port uses with the **lpmmod** command. See *Adding a Logical Port Configuration to a Clear Channel DS3 Port* on page 56-36 for details.)

To modify a port protocol configuration for a logical port using Frame Relay, perform the following steps:

1. Enter the **lppmod** command as follows:

```
lppmod <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port as designated when the port was created.

For example, to modify the protocol of logical port 27 on port 3 of slot 2, enter:

```
lppmod 2/3/27
```

If the logical port is using Frame Relay, then the following screen appears:

```
Protocol configuration of FR
logical port 27, descriptor:
slot 2, ds3port 3, ds1channel 10
ds0 channel mask 0x000000
1) Administrative state {enabled(1), disabled(2)}           : Enabled
2) DLCMI type
   {No LMI Configured(1), LMI Rev.1.0(2),
   T1.617 AnnexD(3), T1.617 AnnexB(4),
   Q.933 AnnexA(5), T1.617 AnnexD-1994(6)}           : No LMI Configured
3) Polling interval T391/nT1 {1-255 sec}                 : 1
4) Full status interval N391/nN1 {1-10}                   : 1
5) Error threshold N392/nN2 {1-10}                       : 1
6) Monitored events counter N393/nN3 {1-10}              : 1
7) Dynamic VC creation {enabled(1), disabled(2)} : Enabled
   71) Default IP routing admin state {enabled(1), disabled(2)}: Enabled
   72) Default bridging admin state {enabled(1), disabled(2)} : Enabled
   73) Default bridging mode
       {BridgeAll(1), BridgeEthernet(2)}               : BridgeEthernet
   74) Default bridging VLAN {1-65535}                  : 1

Enter (option=value/save/cancel) :
```

2. Make changes to the options in this screen at the colon prompt (:). You do this by entering the line number of the option you want to change, an equal sign (=), and then the value for the new parameter.

For example, to change the **DCLMI type** to No LMI Configured, you would enter 2 (the line number for **DCLMI type**), then an equals sign, then 1 (the value for No LMI Configured), as follows:

```
2=1
```

3. After you have entered the required values, be sure to save your configuration.

As a variation of this command, enter the following:

```
lppmod <slot>/<ds3port>/<logPort>/<DLCI>
```

where **<slot>**, **<ds3port>**, and **<logPort>** are as described above, and **<DLCI>** is the unique Data Link Control Identifier assigned to a virtual circuit. This only applies if a logical port is using Frame Relay and it has been assigned a virtual circuit. For information on creating virtual circuits for logical ports, see *Add Frame Relay DLCI on a Logical Port* on page 56-60.

◆ Note ◆

In order to tie routing or bridging services to specific DLCI's, an **lppmod** command must be issued for each DLCI configured. Failure to do so will result in all services being assigned to the M013 routing group whether they are routing or bridging after a reboot.

Field Descriptions for Logical Port using Frame Relay

1) Administrative state {enabled(1), disabled(2)}

This field indicates the Administrative State of the logical port, which can be either Enabled or Disabled. If **Enabled**, the logical port has been enabled and can transmit data as long as its Operational State is also **enabled**. If the Admin Status is **Disabled**, the port will not pass data.

2) DLCMI type

This field specifies the Data Link Control Management Interface (DLCMI) that you want to use for Frame Relay and virtual circuit management. You have four choices for this protocol, each of which corresponds to an existing widely-used protocol. The numbers used in the **lppmod** screen correspond to the following DLCMIs:

- 1 **No LMI Configured**
- 2 **LMI Rev. 1.0 (LMI)**
- 3 **ANSI T1.617 Annex D**
- 4 **CCITT-ITU-T Q.933 Annex A**

Enter your choice by specifying the number corresponding to your choice.

◆ Important Note ◆

The DLCMI protocol that you enter must match that used by your service provider. Entering an incorrect DLCMI protocol may cause the port to fail. The WSX needs to know the protocol you are using to establish communication with the Frame Relay network.

3) Polling interval {1-255 sec}

This interval is the time in seconds between WSX logical port polls of the Frame Relay network. The WSX port polls the network by sending STATUS ENQUIRY messages, which check the link integrity of the Frame Relay connection. By default this interval is set to 10 seconds, but you can increase or decrease it. The default is the standard Frame Relay value. Increasing the polling interval lightens the data load on the logical port, as it does not have to poll as often. The interval may range from 1 second to 4 minutes and 15 seconds (255 seconds).

◆ Important Note ◆

The **Polling Interval** that you enter must match that used by your service provider. This option should only be modified by experienced Frame Relay network administrators.

4) Full status interval {1-10}

This interval is the time in seconds between FULL STATUS ENQUIRIES initiated by the WSX to the Frame Relay network. The Frame Relay network returns a list of all virtual circuits and whether they are active or inactive. You can set this interval from 1 to 10 seconds. By default, this interval is set to 6 seconds, which is the standard Frame Relay default value.

◆ Important Note ◆

The **Full Status Interval** that you enter must match that used by your service provider. This option should only be modified by experienced Frame Relay network administrators.

5) Error threshold {1-10}

The number of DLCMI protocol errors that will be tolerated before determining the logical port Frame Relay line is down and all associated virtual circuits are inactive. These errors may include timeouts from STATUS ENQUIRY polls and invalid STATUS messages returned from the Frame Relay network. By default, this threshold is set to 3, which is the standard Frame Relay default value.

◆ Important Note ◆

The **Error Threshold** that you enter must match that used by your service provider. This option should only be modified by experienced Frame Relay network administrators.

6) Monitored events counter {1-10}

The number of status polling intervals over which the **Error Threshold** is counted. This value should be greater than or equal to the **Error Threshold**. If the station received the number of errors specified in **Error Threshold** within the number of polling intervals specified for the **Monitored Events Counter**, then the Frame Relay line is considered down and all associated virtual circuits are considered inactive. By default, this counter is set to 4, which is the standard Frame Relay default value.

◆ Important Note ◆

The **Monitored Events Counter** that you enter must match that used by your service provider. This option should only be modified by experienced Frame Relay network administrators.

7) Dynamic VC creation {enabled(1), disabled(2)}

This option allows you to set whether virtual circuits are dynamically created (learned) when the Frame Relay network determines it is necessary.

71) Default IP routing admin state {enabled(1), disabled(2)}

This field determines the default status of Internet Protocol (IP) routing of learned virtual circuits. The options are **enabled** or **disabled**.

72) Default bridging admin state {enabled(1), disabled(2)}

This field determines the default bridging administration state of learned virtual circuits. The options are **enabled** or **disabled**.

73) Default bridging mode {BridgeAll(1), BridgeEthernet(2)}

If bridging is enabled, this field indicates which bridging mode is being employed for learned virtual circuits. The options are **BridgeEthernet** or **BridgeAll**.

74) Default bridging VLAN {1-65535}

If bridging is enabled, this field indicates the default VLAN group used for bridging on this logical port.

Display Protocol Configuration and Statistics of a Logical Port using PPP

The **lppview** command allows you to view logical port protocol configuration and statistics (either PPP or Frame Relay). There is a separate display for PPP and Frame Relay protocol configuration and statistics. (You can set the type of protocol a logical port uses with the **lpmmod** command. See *Adding a Logical Port Configuration to a Clear Channel DS3 Port* on page 56-36 for details.)

To view logical port protocol configuration and statistics for PPP, enter the **lppview** command as follows:

```
lppview <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port as designated when the port was created. For example, to view the protocol statistics of logical port 27 on port 3 or slot 2, enter:

```
lppview 2/3/27
```

If the logical port is configured to use PPP, a screen similar to the following is displayed:

```

Protocol (PPP) configuration of logical port 2/3/27
AdminState:Enabled          PPPMode:                Normal
RoutingEnable:             Enabled                 BridgingEnable:        Enabled
BridgingMode:              BridgeEthernet         BridgingGroup:         3
LQMEnable:                 Enabled                 AuthenticationType:    None
MaxConfigCount:            5                       MaxFailCount:          4
LocalUserId:               TESTLoid               MaxTerminateCount:    6
LocalPassword:             TESTLoPw               RemoteUserId:          TESTReId
LocalIpAddress:            255.255.255.255       RemotePassword:        TESTRePw
RetryTimeout:              7                       RemoteIPAddress:      255.255.255.255

PPP protocol specific statistics
LcpFramesRcvd:             0                       lcpFramesRcvd:         0
BcpFramesRcvd:             0                       LcpFramesSent:         0
lcpFramesSent:             0                       BcpFramesSent:         0

Common FR/PPP statistics
CircuitSent8023Frames:    10                      CircuitSent8023Octets:  20
CircuitReceived8023Frames: 30                      CircuitReceived8023Octets: 40
CircuitSentBPDUFrames:   50                      CircuitSentBPDUOctets:  60
CircuitReceivedBPDUFrames: 70                      CircuitReceivedBPDUOctets: 80
CircuitSentIPFrames:     90                      CircuitSentIPOctets:    10
CircuitReceivedIPFrames: 20                      CircuitReceivedIPOctets: 30
CircuitSent8025Frames:   80                      CircuitSent8025Octets:  90
CircuitReceived8025Frames: 10                      CircuitReceived8025Octets: 20
CircuitSentFDDIFrames:   30                      CircuitSentFDDIOctets:  40
CircuitReceivedFDDIFrames: 50                      CircuitReceivedFDDIOctets: 60

```

As a variation of this command, you can enter **lppview <slot>/<ds3port>** to see the protocol configuration for every logical port on the selected port, or **lppview <slot>** to see the protocol configuration for every logical port in the selected module.

Field Descriptions for Logical Port Protocol using PPP

The following section explains the fields and their corresponding values.

Configuration information

AdminState. This field indicates the Administrative State of the logical port, which can be either Enabled or Disabled. If **Enabled**, the logical port has been enabled and can transmit data as long as its Operational State is also **enabled**. If the Admin Status is **Disabled**, the port will not pass data.

PPPMode. This field indicates which PPP mode the logical port is using.

RoutingEnable. This field indicates whether IP routing is enabled or disabled for this logical port.

BridgingEnable. This field indicates whether bridging is enabled or disabled for this logical port.

BridgingMode. If bridging is enabled, this field indicates which bridging mode is being employed. The options are **BridgeEthernet** or **BridgeAll**.

BridgingGroup. If bridging is enabled, this field indicates the bridging group number, as specified with the **lppmod** command.

LQMEnable. This field indicates whether Line Quality Monitoring (LQM) is enabled. LQM counts the number of packets sent across a link and periodically asks the remote end how many packets it received. Discrepancies are evidence of packet loss and indicate link quality problems.

AuthenticationType. This field indicates which type of authentication is being used by this logical port. The options are **none**, **PAPS**, or **CHAPS**.

MaxFailCount. This field indicates the maximum number of times a CONFIGURATION_REQUEST packet will be sent when the previous attempts received responses, but did not receive a CONFIGURATION_ACK. This counter applies to all LCP and NCP negotiations.

MaxConfigCount. This field indicates the maximum number of times a CONFIGURATION_REQUEST packet will be sent when the previous attempts did not receive any responses. This counter applies to all LCP and NCP negotiations.

MaxTerminateCount. This field indicates the maximum number of TERMINATE_REQUEST packets that will be sent without receiving a TERMINATE_ACK packet. This counter applies to all LCP and NCP negotiations.

LocalUserId. This field displays the User ID to be sent to the remote end during PAP or CHAP authentication. This parameter is used only for outgoing calls.

RemoteUserId. This field displays the User ID expected from the remote end during PAP or CHAP authentication.

LocalPassword. This field displays the password sent to the remote end during PAP or CHAP authentication. This parameter is used only for outgoing calls.

RemotePassword. This field displays the password expected from the remote end during PAP or CHAP authentication.

LocalIpAddress. This field allows you to specify the local IP address for this logical port, if IP routing is enabled. Valid IP notation must be used.

RemoteIpAddress. This field displays the Remote IP address of the PPP connection when IP routing is enabled. Valid IP address notation must be used. If this parameter is set to 0.0.0.0

Display Protocol Configuration and Statistics of a Logical Port using PPP

and IP routing is enabled, the Remote IP address will be learned during Internet Protocol Control Protocol (IPCP) negotiation.

RetryTimeout. This field indicates the number of seconds to wait between CONFIGURATION_REQUEST retries that do not receive a response. This timeout value applies to all LCP and NCP negotiations.

PPP Protocol Specific Statistics information

The following statistics are specific to a logical port configured to use PPP.

LcpFramesRcvd. This field displays the number of Link Control Protocol (LCP) frames received on this logical port.

lcpFramesRcd. This field displays the number of Internet Protocol Control Protocol (IPCP) frames received on this logical port.

BcpFramesRcvd. This field displays the number of Bridge Control Protocol (BCP) frames received on this logical port.

LcpFramesSent. This field displays the number of Link Control Protocol (LCP) frames sent by this logical port.

lcpFramesSent. This field displays the number of Internet Protocol Control Protocol (IPCP) frames sent by this logical port.

BcpFramesSent. This field displays the number of Bridge Control Protocol (BCP) frames sent by this logical port.

Common FR/PPP Statistics information

These are statistics for the different protocols possible for traffic on both Frame Relay and PPP.

◆ Note ◆

The descriptions below combine frames and octets, though they are represented as separate statistics in the UI.

CircuitSent8023Frames/Octets. This counter indicates transmitted traffic for Ethernet (bridged 802.3 or trunked format) frames and octets on this logical port. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

CircuitReceived8023Frames/Octets. This counter indicates received traffic for Ethernet (bridged 802.3 or trunked format) frames and octets on this virtual circuit. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

CircuitSentBPDUFrames/Octets. This counter indicates transmitted traffic for BPDU frames and octets on this logical port. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

CircuitReceivedBPDUFrames/Octets. This counter indicates received traffic for BPDU frames and octets on this virtual circuit. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

CircuitSentIPFrames/Octets. This counter indicates transmitted traffic for routed IP, ARP, and Inverse ARP format frames and octets on this logical port. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

CircuitReceivedIPFrames/Octets. This counter indicates received traffic for routed IP, ARP, and Inverse ARP format frames and octets on this logical port. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

CircuitSent8025Frames/Octets. This counter indicates traffic for Token Ring (802.5 format) frames and octets on this logical port. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

CircuitReceived8025Frames/Octets. This counter indicates received traffic for Token Ring (802.5 format) frames and octets on this logical port. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

CircuitSentFDDIFrames/Octets. This counter indicates transmitted traffic for FDDI frames and octets on this logical port. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

CircuitReceivedFDDIFrames/Octets. This counter indicates traffic for FDDI frames and octets on this logical port. Statistics for octets, or bytes, include the data and Frame Relay header fields, but they do not include CRC or flag characters.

Display Protocol Configuration and Statistics of a Logical Port using Frame Relay

The **lppview** command displays a different screen if you want to see logical port configuration and statistics information for a logical port using Frame Relay. (You can set the type of protocol a logical port uses with the **lpmmod** command. See *Adding a Logical Port Configuration to a Clear Channel DS3 Port* on page 56-36 for details.)

To view logical port protocol configuration and statistics for Frame Relay, enter the **lppview** command as follows:

```
lppview <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port as designated when the port was created. For example, to view the protocol statistics of logical port 27 on port 3 of slot 2, enter:

```
lppview 2/3/27
```

If the logical port is configured to use frame relay, a screen similar to the following is displayed:

```

Protocol (FR) configuration of logical port 2/3/27
AdminState:                Enabled   DlcmiType:                No LMI Configured
IPRoutingAdminStatus:     Enabled   BridgingAdminStatus:     Enabled
DefaultBridgeMode:       BridgeEthernet   DefaultBridgingVlan:     1
PollingInterval:         1        FullStatusInterval:     1
ErrorThreshold:          1        MonitoredEventsCounter: 1
MaxVcs:                  1        DynamicVcCreation:      Enabled
DlcmiAddress:            Q.921    DlcmiAddressLen:        ThreeOctets
DlcmiMulticast:          NonBroadcast

Frame Relay VC configuration
DLCI:                      1        AdminState:              Enabled
CommittedInfoRate:        1000    CommittedBurstRate(BPS): 2000
ExcessBurstRate:          3000    Multicast:               NonBroadcast
RoutingEnable:            Enabled   TrapEnable:              Enabled
BridgingEnable:           Enabled   BridgingMode:            BridgeEthernet
BridgingVlan:             10

FR protocol specific statistics
CircuitReceivedFECNs:     1        CircuitReceivedBECNs:    2
CircuitSentFrames:        3        CircuitSentOctets:       4
CircuitReceivedFrames:    3        CircuitReceivedOctets:   6
CircuitDiscards:          7        CircuitReceivedDEs:      8
CircuitDiscards:          8

Common FR/PPP statistics
CircuitSent8023Frames:    10       CircuitSent8023Octets:   20
CircuitReceived8023Frames: 30       CircuitReceived8023Octets: 40
CircuitSentBPDUFrames:    50       CircuitSentBPDUOctets:   60
CircuitReceivedBPDUFrames: 70       CircuitReceivedBPDUOctets: 80
CircuitSentIPFrames:      90       CircuitSentIPOctets:     10
CircuitReceivedIPFrames:  20       CircuitReceivedIPOctets:  30
CircuitSent8025Frames:    80       CircuitSent8025Octets:   90
CircuitReceived8025Frames: 10       CircuitReceived8025Octets: 20
CircuitSentFDDIFrames:    30       CircuitSentFDDIOctets:   40
CircuitReceivedFDDIFrames: 50       CircuitReceivedFDDIOctets: 60

```

As a variation of this command you can enter the following:

```
lppview <slot>/<logPort>/<DLCI>
```

where **<slot>** and **<logPort>** are as described above, and **<DLCI>** is the unique Data Link Control Identifier assigned to a virtual circuit. This only applies if a logical port is using Frame Relay and it has been assigned a virtual circuit. For information on creating virtual circuits for logical ports, see *Add Frame Relay DLCI on a Logical Port* on page 56-60.

As another two variations of this command, you can enter **lppview <slot>/<ds3port>** to see the protocol configuration for every logical port on the selected port, or **lppview <slot>** to see the protocol configuration for every logical port in the selected module.

Field Descriptions for Logical Port Protocol using Frame Relay

The following section explains the fields and their corresponding values.

Configuration

AdminState. This field indicates the Administrative State of the logical port, which can be either Enabled or Disabled. If **Enabled**, the logical port has been enabled and can transmit data. If the Admin Status is **Disabled**, the port will not pass data.

DlcmiType. This field indicates the Data Link Control Management Interface (DLCMI) type used by the logical port for frame relay and virtual circuit management. The four options for this field are **none**, **LMI Rev. 1.0**, **ANSI T1.617 Annex D**, and **CCITT-ITU-T-Q.933 Annex A**.

◆ Important Note ◆

The DLCMI protocol used by the logical port must match that of the Frame Relay service.

IPRoutingAdminStatus. This field indicates the status of IP routing for this logical port. The options are **Enabled** or **Disabled**.

BridgingAdminStatus. This field displays the Bridging status of this logical port. The options are **enable** or **disable**.

DefaultBridgeMode. This field indicates the default bridging mode of this logical port. The options are **BridgeAll** or **BridgeEthernet**.

DefaultBridgingVlan. Indicates the VLAN Group to be used for Frame Relay Bridging. A value of zero (0) indicates that this logical port will not perform a bridging service and will discard all bridged format packets received or transmitted.

PollingInterval. This field indicates the interval in seconds between WSX logical port polls of the Frame Relay network. The WSX port polls the network by sending STATUS ENQUIRY messages, which check the link integrity of the Frame Relay connection. By default this interval is set to 10 seconds, but you can increase or decrease it. The default is the standard Frame Relay value. Increasing the polling interval lightens the data load on the logical port, as it does not have to poll as often. The interval may range from 1 second to 4 minutes and 15 seconds (255 seconds).

◆ Important Note ◆

The **Polling Interval** that you enter must match that of the Frame Relay service. This option should only be modified by experienced Frame Relay network administrators.

FullStatusInterval. This field indicates the interval in seconds between FULL STATUS ENQUIRIES initiated by the WSX to the Frame Relay network. The Frame Relay network returns a list of all virtual circuits and whether they are active or inactive. You can set this interval from 1 to 10 seconds. By default, this interval is set to 6 seconds, which is the standard Frame Relay default value.

◆ Important Note ◆

The **Full Status Interval** that you enter must match that of the Frame Relay service. This option should only be modified by experienced Frame Relay network administrators.

ErrorThreshold. This field indicates the number of DLCMI protocol errors that will be tolerated before determining the logical port Frame Relay line is down and all associated virtual circuits are inactive. These errors may include timeouts from STATUS ENQUIRY polls and invalid STATUS messages returned from the Frame Relay network. By default, this threshold is set to 3, which is the standard Frame Relay default value.

◆ Important Note ◆

The **Error Threshold** that you enter must match that of the Frame Relay service. This option should only be modified by experienced Frame Relay network administrators.

MonitoredEventsCounter. This field indicates the number of status polling intervals over which the **Error Threshold** is counted. This value should be greater than or equal to the **Error Threshold**. If the station received the number of errors specified in **Error Threshold** within the number of polling intervals specified for the **Monitored Events Counter**, then the Frame Relay line is considered down and all associated virtual circuits are considered inactive. By default, this counter is set to 4, which is the standard Frame Relay default value.

◆ Important Note ◆

The **Monitored Events Counter** that you enter must match that of the Frame Relay service. This option should only be modified by experienced Frame Relay network administrators.

MaxVcs. This field indicates the maximum number of virtual circuits supported by this logical port.

DynamicVcCreation. This field indicates whether virtual circuits can be dynamically created (learned) by the logical port. The options for this are **enabled** and **disabled**.

DlcmiAddress. This field displays which address format is in use by this logical port. The format determines the length of the address, in bits. The options are **Q921** (13 bits), **Q922March90** (11bits), **Q922November90** (10 bits), and **Q922** (final standard).

DlcmiAddressLen. This field indicates the length of the DLMI address in octets. The options are 2, 3, or 4 octets.

◆ Note ◆

In the case of a Q922 format, the length indicates the entire length of the address including the control portion.

DlcmiMulticast. This field indicates whether the logical port is using a multicast service. The options are **Broadcast** (yes) or **NonBroadcast** (no).

Frame Relay VC Configuration information

The following fields show the defaults for the virtual circuit associated with this logical port. For more information on virtual circuits, see Chapter 49 titled “Managing Frame Relay” in your switch manual.

DLCI. The Data Link Control Identifier (DLCI) for this virtual circuit.

AdminState. This field indicates the Administrative State of the virtual circuit, which can be either Enabled or Disabled. If **Enabled**, the logical port has been enabled and can transmit data. If the Admin Status is **Disabled**, the port will not pass data.

CommittedInfoRate. This field sets the Committed Information Rate (CIR) for this virtual circuit.

◆ Important Note ◆

The **CIR** that you set must match that of the Frame Relay service. This option should only be modified by experienced Frame Relay network administrators.

CommittedBurstRate. The Committed Burst Rate (Bc) is the amount of data that the network will guarantee to transfer under normal conditions.

◆ Important Note ◆

The **Bc** that you enter must match that of the Frame Relay service. This option should only be modified by experienced Frame Relay network administrators.

ExcessBurstRate. The Excess Burst Rate (Be) is the amount of data over-and-above the Committed Burst Rate (Bc) that the network will transmit as long as excess bandwidth is available.

◆ Important Note ◆

The **Be** that you enter must match that of the Frame Relay service. This option should only be modified by experience Frame Relay network administrators.

Multicast. This field indicates whether the virtual circuit is using a multicast service. The options are **Broadcast** (yes) or **NonBroadcast** (no).

RoutingEnable. This field indicates whether Routing is enabled or disabled for this virtual circuit.

TrapEnable. This field indicates whether this virtual circuit is enabled to send SNMP traps.

BridgingEnable. This field indicates whether Bridging is enabled or disabled for this virtual circuit.

BridgingMode. If Bridging is enabled, this field indicates which bridging mode is being employed for this virtual circuit. The options are **BridgeEthernet** or **BridgeAll**.

BridgingVlan. If Bridging is enabled, this field indicates the VLAN Group to be used for Bridging. A value of zero (0) indicates that this PPP Entity will not perform a bridging service and will discard all bridged format packets received or transmitted.

FR Protocol Specific Statistics

The following statistics are specific to logical ports employing Frame Relay.

CircuitReceivedFECNs. This field indicates the number of frames received by this logical port indicating forward congestion since its creation.

CircuitReceivedBECNs. This field indicates the number of frames received by this logical port indicating backward congestion since its creation.

CircuitSentFrames. The number of frames sent by this logical port since its creation.

CircuitSentOctets. The number of octets sent by this logical port since its creation

CircuitReceivedFrames. The number of frames received by this logical port since its creation.

CircuitReceivedOctets. The number of octets received by this logical port since its creation.

CircuitDiscards. The number of frames on this logical port discarded due to errors.

CircuitReceivedDEs. The number of Discard Eligibility (DE) frames or octets received by this logical port. A DE is a single bit attached to a frame that signifies it is the first thing to be discarded if bandwidth is reaching maximum usage.

CircuitDiscards. The number of octets on this logical port discarded due to errors.

Common FR/PPP Statistics information

The statistics information displayed for these counters is the same as the counters for a logical port using PPP. See *Common FR/PPP Statistics information* on page 56-52 for their descriptions.

Clear Protocol Statistics of a Logical Port

The **lppcls** command allows you to clear statistics associated with a logical port. To clear statistics:

1. Enter the **lppcls** command as follows:

```
lppcls <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port as designated when the port was created.

For example, to clear the protocol statistics of logical port 27 on port 3 of slot 2, enter:

```
lppcls 2/3/27
```

A confirmation message similar to the following will appear:

```
Confirm to clear protocol statistics of logical port 2/3/27
```

```
Enter (option=yes,no)
```

2. To confirm, enter **yes** and press **<Enter>**. The following confirmation is displayed:

```
Statistics on logical port 2/3/27 are cleared
```

As a variation to this command, you can enter a DLCI number as follows:

```
lppcls <slot>/<ds3port>/<logPort>/<DLCI>
```

where **<slot>**, **<ds3port>**, and **<logPort>** are as described above and **<DLCI>** is the unique Data Link Control Identifier assigned to the virtual circuit for this logical port. This can only be done for logical ports using Frame Relay as virtual circuits are not applicable to Point-to-Point Protocol.

As another two variations of this command, you can enter **lppcls <slot>/<ds3port>** to clear the protocol configuration for every logical port on the selected port, or **lppcls <slot>** to clear the protocol configuration for every logical port in the selected module.

Add Frame Relay DLCI on a Logical Port

The **ipfradd** command allows you to add a Frame Relay DLCI, or a virtual circuit, to a logical port that has been configured to use Frame Relay. To add a virtual circuit, perform the following steps:

1. Enter the **ipfradd** command as follows:

```
ipfradd <slot>/<ds3port>/<logPort>/<DLCI>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, **<logPort>** is the number of the specific logical port as designated when the port was created, and **<DLCI>** is the The Data Link Control Identifier for the new virtual circuit. For example, to create a virtual circuit with a DLCI of 16 for logical port 27 on port 3 of slot 2, enter:

```
ipfradd 2/3/27/16
```

A screen similar to the following is displayed:

```
Add Frame Relay VC with DLCI 16
logical port 27, descriptor:
slot 2, ds3port 5, ds1channel 10
ds0 channel mask 0x000000
1) Administrative state {enabled(1), disabled(2)} : Disabled
2) Committed information rate (Cir)
   {0 through line speed in BPS} :0
3) Committed burst rate (Bc)
   {0 through positive number in bits} :0
4) Excess burst rate (Be)
   {0 through positive number in bits} :0

Enter (option=value/save/cancel) :
```

2. Make changes to the options in this screen at the colon prompt (:). You do this by entering the line number of the option you want to change, an equal sign (=), and then the value for the new parameter. After you have entered the required values, be sure to save your configuration.

For more information on virtual circuits, see Chapter 49 titled “Managing Frame Relay” in your switch manual.

Field Descriptions

1) Administrative state {enabled(1), disabled(2)}

This option enables or disables a virtual circuit on this logical port. Setting this option to **enable** allows data to be sent and received on it, while setting this option to **disable** means no data can be sent on the circuit.

2) Committed information rate (Cir) {0 through line speed in BPS}

This field sets the Committed Information Rate (CIR) for this virtual circuit.

◆ Important Note ◆

The **CIR** that you set must match that of the Frame Relay service. This option should only be modified by experienced Frame Relay network administrators.

3) Committed burst rate (Bc) {0 through positive number in bits}

The Committed Burst Rate (Bc) is the amount of data that the network will guarantee to transfer under normal conditions.

◆ Important Note ◆

The **Bc** that you enter must match that of the Frame Relay service. This option should only be modified by experienced Frame Relay network administrators.

4) Excess burst rate (Be) {0 through positive number in bits}

The Excess Burst Rate (Be) is the amount of data over-and-above the Committed Burst Rate (Bc) that the network will transmit as long as excess bandwidth is available.

◆ Important Note ◆

The **Be** that you enter must match that of the Frame Relay service. This option should only be modified by experience Frame Relay network administrators.

Delete Frame Relay DLCI on a Logical Port

The **ipfrdel** command allows you to delete a Frame Relay DLCI, or virtual circuit, from a logical port. To delete a virtual circuit, perform the following steps:

1. Enter the **ipfrdel** command as follows:

```
ipfrdel <slot>/<ds3port>/<logPort>/<DLCI>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, **<logPort>** is the number of the specific logical port as designated when the port was created, and **<DLCI>** is the the Data Link Control Identifier for the new virtual circuit. For example, to create a virtual circuit with a DLCI of 16 for logical port 27 on port 3 of slot 2, enter:

```
ipfrdel 2/3/27/16
```

A message similar to the following is displayed:

```
Confirm to delete FR VC with DLCI 16. logical port 2/3/27
```

```
Enter (option=yes/no) :
```

2. Confirm deletion by entering **yes** at the colon prompt (:) followed by **<Enter>**. The following notice appears:

```
FR VC with DLCI 16 deleted, logical port 2/3/27
```

Adding a Router Interface

The **riadd** command allows you to create a router interface for PPP, a frame relay circuit, or a virtual circuit. A router interface connects to a virtual circuit or set of virtual circuits and identifies on the network for IP routing. To create a router interface:

1. Enter the **riadd** at the system prompt in the following manner:

```
riadd <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port as designated when the port was created. For example, to create a router interface for logical port 27 on port 3 of slot 2, enter:

```
riadd 2/3/27
```

A screen similar to the following is displayed:

```
1) IP address           : 0.0.0.0
2) IP mask              : 0.0.0.0
3) Administrative state
   {enabled (1), disabled (0)} :
```

```
Enter (option=value/save/cancel) :
```

2. Make changes to the options in this screen at the colon prompt (:). You do this by entering the line number of the option you want to change, an equal sign (=), and then the value for the new parameter. After you have entered the required values, be sure to save your configuration.

One router interface per logical port is allowed.

Field Descriptions

The following section explains the fields and their corresponding values.

IP address

The Internet Protocol (IP) address assigned to this router interface.

IP mask

The subnet mask that the above IP address is a member of.

Administrative state

This option enables or disables the router interface for this logical port. Setting this option to **enable** allows data to be sent and received on it, while setting this option to **disable** means no data can be sent on the circuit.

Modifying a Router Interface Configuration

The **rimod** command allows you to configure an existing router interface by modifying the IP address or routing parameters associated with the selected interface. To modify a router interface:

1. Enter the **rimod** command as follows:

```
rimod <slot>/<ds3port>/<logPort>/
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port as designated when the port was created. For example, to modify a router interface for logical port 27 on port 3 of slot 2, enter:

```
rimod 2/3/27
```

A screen similar to the following is displayed:

```
1) IP address           : 0.0.0.0
2) IP mask             : 0.0.0.0
3) Administrative state
   {enabled (1), disabled (0)} :
```

```
Enter (option=value/save/cancel) :
```

2. Make changes to the options in this screen at the colon prompt (:). You do this by entering the line number of the option you want to change, an equal sign (=), and then the value for the new parameter. After you have entered the required values, be sure to save your configuration.

The displayed fields are the same as the ones shown for the **riadd** command. See *Adding a Router Interface* on page 56-62 for more details.

Deleting a Router Interface

The **ridel** command allows you to delete a router interface. To delete a router interface, perform the following steps:

1. Enter the **ridel** command as follows:

```
ridel <slot>/<de3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port as designated when the port was created. For example, to delete a router interface for logical port 27 on port 3 of slot 2, enter:

```
ridel 2/3/27
```

A message similar to the following is displayed:

```
Confirm to delete router interface on logical port 2/3/27
Enter (option=yes/no) :
```

2. Confirm the interface deletion by entering **yes** at the prompt followed by a **<Enter>**. The following message is displayed:

```
Router interface deleted
```

Viewing Router Interfaces

The **riview** command allows you to view a router interface's configuration information. To view an interface configuration enter the **riview** command as follows:

```
riview <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port the interface was added to when created. For example to view a router interface assigned to logical port 27 on DS3 port 3 of slot 2, enter:

```
riview 2/3/27
```

When you have entered the command, the following display is shown:

```
Router interface on Logical port 2/3/27 Admin state: Disabled  
IP address: 5.5.5.5, IP Mask: 6.6.6.6  
Control pdu statistics: Total in 4, out 6, Errors in 3, out 4
```

Definitions for the **Admin state**, **IP address**, and **IP Mask** fields can be found in the section *Adding a Router Interface* on page 56-62. The **Control pdu statistics** show the number of control packets sent and received.

There are three variations to this command. You can enter **riview <slot>/<ds3port>** to display the statistics of all router interfaces for the specified port, **riview <slot>** to display the statistics of all router interfaces for the specified slot, and **riview** to display the statistics of all router interfaces for the switch.

Clearing Statistics for a Router Interface

The **ricls** command allows you to clear the statistics for a selected router interface. To clear the statistics of a router interface, enter the **ricls** command as follows:

```
ricls <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port the interface was added to when created. For example, to clear the statistics of a router interface assigned to logical port 27 on DS3 port 3 of slot 2, enter:

```
ricls 2/3/27
```

When you have entered the command, the following display is shown:

```
Confirm to clear router interface statistics on logical port 2/3/27?  
Enter (option=yes/no):
```

Enter **yes** to delete statistics, or **no** to retain them.

There are three variations to this command. You can enter **ricls <slot>/<ds3port>** to clear the statistics of all router interfaces for the specified port, **ricls <slot>** to clear the statistics of all router interfaces for the specified slot, and **ricls** to clear the statistics of all router interfaces for the switch.

Creating a Bridging or Trunking Service

The **m013cas** command allows you to create a bridging or trunking service for a logical port. (For more information on bridging and trunking services see Chapter 49, titled “Managing Frame Relay” in your switch manual.) Creating a service for a logical port using Frame Relay differs slightly than creating a service for a port using PPP. Both are detailed below.

To create a bridging or trunking service for a logical port using Frame Relay, do the following:

1. Enter the **m013cas** command at the prompt as shown:

```
m013cas <slot>/<ds3port>/<logPort>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, and **<logPort>** is the number of the specific logical port as designated when the port was created. For example, to add a service to logical port 27 on port 2 of slot 3, you would enter:

```
m013cas 3/2/27
```

A screen similar to the following appears:

```
Adding service on logical port 27, slot 3
1) Service description (30 chars max)      :
2) Service type {trunking(4), bridging(6)} : Bridging
3) Administrative state {enabled(1), disabled(2)} :
4) DLCI                                     :
51) Bridging group {1-65535}               : 0
52) Bridging mode {BridgeAll(0), BridgeEthernet(1)} : BridgeAll
```

```
Enter (option=value/save/cancel) :
```

2. Make changes to the options in this screen at the colon prompt (:). You do this by entering the line number of the option you want to change, an equal sign (=), and then the value for the new parameter. For example, to use **testservice** as the **Service description**, enter **1** (the line number for the **Service description**), then the equals sign, then **testservice**.
3. Choose what type of service you wish to create, either **trunking (4)** or **bridging (6)**, as above. For example, to create a bridging service, enter **2** (the line number for the **Service type**), an equals sign, and then **6** (the value for bridging).
4. Select the administrative state for this service, either **enabled (1)** or **disabled (2)**, as above. Enabling a port means it is active and can receive and transmit data.
5. Enter the virtual circuit that is assigned to the logical port. The virtual circuit has a Data Link Control Identifier (DLCI) that is assigned when it is created. For more information on creating a virtual circuit, see *Add Frame Relay DLCI on a Logical Port* on page 56-60.
6. If you are creating a bridging service, select a bridging group for the service by entering the line number, an equals sign, and the group number. For example, to create a bridging service for group 10, you would enter **51** (the line number for **Bridging group**), an equals sign, and then **10**.
7. If you are creating a bridging service, select which bridging mode the service uses. The mode is either **BridgeAll (0)** or **BridgeEthernet (1)**. **BridgeAll** allows bridging for all interfaces, while **BridgeEthernet** enables bridging on Ethernet interfaces only.

Creating a Bridging or Trunking Service

- Remember to save the configuration before you exit by typing **save** at the command prompt. A message similar to the following is shown:

**Created bridge service for logical port 3/2/27
Service id 100 should be used in future references.**

Remember the service ID number as it is needed for other service commands such as **m013das**, **m013vas**, and **m013mas**. For more information, see *Deleting Services* on page 56-67, *Viewing Service Configurations* on page 56-67, and *Modifying Service Configurations* on page 56-69.

Creating a service for a logical port using Point-to-Point Protocol (PPP) is nearly identical to the procedure described in the steps above, with the exceptions that there is no field for a DLCI, and that only a bridging service can be created. You cannot create a trunking service for a logical port using PPP.

To create a service for a logical port using PPP, enter the **m013cas** command as described above. The menu for creating a service for a logical port using PPP is almost the same as the one displayed for a logical port using Frame Relay, and is shown below:

```
Adding service on logical port 2, slot 3
1) Service description (30 chars max)      :
2) Service type {trunking(4), bridging(6)} : Bridging
   for PPP only bridging is available
3) Administrative state {enabled(1), disabled(2)} :
41) Bridging group {1-65535}              : 0
42) Bridging mode {BridgeAll(0), BridgeEthernet(1)} : BridgeAll
```

Enter (option=value/save/cancel) :

Proceed using the steps outlined above.

Deleting Services

The **m013das** command allows you to delete a service from a logical port. To delete a service:

1. Enter the **m013das** command as follows:

```
m013das <slot>/<ds3port>/<logPort>/<serviceld>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, **<logPort>** is the number of the specific logical port as designated when the port was created, and **<serviceld>** is the identification number of the service as assigned when it was created. For example, to delete bridging service 100 for logical port 27 on port 2 of slot 3, you would enter:

```
m013das 3/2/27/100
```

The following message should appear:

```
Confirm to delete bridge service 100 for logical port 3/2/27
```

```
Enter (option=yes/no) :
```

2. Enter **yes** to confirm and delete the service, or **no** to abort. A confirmation message similar to the following appears:

```
Deleted bridge service 100 for logical port 3/2/27
```

Viewing Service Configurations

Once you have created a service or a number of services, you can view their configurations and locations using the **m013vas** command. To view the configuration of a service enter the **m013vas** command as follows:

```
m013vas <slot>/<ds3port>/<logPort>/<serviceld>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, **<logPort>** is the number of the specific logical port as designated when the port was created, and **<serviceld>** is the identification number of the service as assigned when it was created. For example, to view service 100 for logical port 27 on port 2 of slot 3, you would enter:

```
m013vas 3/2/27/100
```

The following screen is displayed:

Slot Ds3 LogPort	Opr Sts	VC	Group	Ser vice Id	VPort	Service Description	Type
3/2/27	UP	PPP	1	100		Testservice	Bridge

There are four variations of this command. You can enter **m013vas <slot>/<ds3port>/<logPort>** to view all services for the specified logical port, **m013vas <slot>/<ds3port>** to view all services for the specified DS3 port, **m013vas <slot>** to view all the services for the specified slot, or **m013vas** to view all the services for the switch.

Field descriptions

The following sections describe the fields displayed by the **m013vas** command.

Slot/Ds3/LogPort. The slot, port, and logical port numbers for this service are shown in this field. For example, if the service was assigned to slot 3, port 2, logical port 27, the field would show **3/2/27**.

Opr Sta. This field shows the administration status of the service. It is either enabled or disable.

VC. In the case of service for a logical port using Frame Relay, this field shows the Data Link Control Identifier (DCLI) of the virtual circuit associated with the logical port. A virtual circuit can be attached to more than one logical port and be supported by more than one service type. If a logical port uses Point-to-Point Protocol (PPP) rather than Frame Relay, this field will show **PPP** rather than a number.

Group. The number of the Group or Groups associated with this service. Only one Group is supported by a bridging service. Trunking services can supports multiple groups.

Service Id. Each service for a port is assigned a number. This field shows the number assigned to this service when it was created.

VPort. The virtual port associated with this service. For bridging services there is a one-to-one mapping between a virtual port and a virtual circuit. For trunking services, multiple virtual ports can map to a single virtual circuit.

Service Description. The textual description of this service as entered when the service was created.

Type. The type of service, either trunking or bridging. Bridging and Trunking services cannot coexist on the same virtual circuit.

Modifying Service Configurations

Once you have created a service, you can modify it using the **m013mas** command. To modify a service:

1. Enter the **m013mas** command as follows:

```
m013mas <slot>/<ds3port>/<logPort>/<serviceld>
```

where **<slot>** is the slot number of the board on which the logical port is located, **<ds3port>** is the DS3 port number on the board, **<logPort>** is the number of the specific logical port as designated when the port was created, and **<serviceld>** is the number of service as designated when the service is created. For example, to view service 100 for logical port 27 on port 2 of slot 3, you would enter:

```
m013mas 3/2/27/100
```

A screen similar to the following is displayed:

```
Service configuration on logical port 3/2/27
1) Service description (30 chars max)      : testservice
2) Service type {trunking(4), bridging(6)}  : Bridging
3) Administrative state {enabled(1), disabled(2)} : Enabled
4) DLCI                                     : 16
51) Bridging group {1-65535}               : 1
52) Bridging mode {BridgeAll(0), BridgeEthernet(1)} : BridgeAll
```

Enter (option=value/save/cancel) :

◆ Note ◆

The above screen shows a service for a logical port using Frame Relay. The screen for a service for a logical port using PPP looks slightly different. Specifically, the DLCI field is absent, and you can only configure a bridging service for logical port using PPP.

2. Make any changes to the service configuration at the colon prompt (:). You do this by entering the line number of the option you want to change, an equal sign (=), and then the value for the new parameter. For example, to change the **Bridging group** to 18, enter **51** (the line number for the **Bridging group** parameter), then an equals sign, then **18**, as follows:

```
51=18
```

3. After you have entered the required values, be sure to save your configuration.

Deleting the Module Configuration

Using the **m013cfgdel** command, you can completely delete the channelized DS3 module configuration and start again. To delete the entire configuration:

Enter the **m013cfgdel** command at the system prompt, as shown:

```
m013cfgdel
```

The following message appears, asking you to confirm your choice:

```
Confirm to delete current M013 configuration
```

```
Enter (option=yes/no) :
```

Enter **yes** at the prompt to confirm the deletion of the channelized DS3 module configuration. When it is finished, the following message appears:

```
M013 configuration deleted.
```

◆ Important Note ◆

Using this command *completely* deletes the configuration parameters in the channelized DS3 module. All information on configuration and statistics will be lost.

57 Troubleshooting

This chapter provides information that will help you troubleshoot OmniSwitch and Omni Switch/Router hardware and software problems. The sections within this chapter describe problems or errors you may encounter during switch hardware and software installation, configuration, or operation. Subsections within these categories reflect unique problems and provide the recommended corrective action(s).

Common problems installing switch software and possible solutions are described on page 57-5. Common network problems and possible solutions are described on page 57-6. Common hardware problems and possible solutions are described on page 57-9. And User Interface (UI) error messages, which can be used to diagnose problems, are described in page 57-12.

◆ Important Note ◆

In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. See Chapter 8, “The User Interface,” for documentation on changing from CLI mode to UI mode.

Detecting Problems

The Omni Switch/Router and OmniSwitch provide several mechanisms to detect problems. Hardware problems can be detected through:

- LEDs (OK1)
- PING tests using the **ping** command
- Network Management Software (NMS) error reporting
- Diagnostics software
- Command Line Interface (CLI) commands (e.g., **view atm port**)
- UI error messages

This chapter lists UI error messages. Refer to the appropriate hardware chapters for a complete description of LED states. Refer to NMS online documentation for explanations of NMS error messages. Refer to Chapter 30, “IP Routing,” for procedures to use the **ping** command. Refer to Chapter 58, “Running Hardware Diagnostics,” for documentation on diagnostics software. And refer to the *Text-Based Configuration CLI Reference Guide* for documentation on CLI commands.

Software problems can be detected through:

- LEDs (OK2)
- NMS error reporting
- CLI diagnostic commands (e.g., **dump** and **configuration check**)
- UI error messages

This chapter lists UI error messages. Refer to NMS online documentation for explanations of NMS error messages. And refer to the *Text-Based Configuration CLI Reference Guide* for documentation on CLI commands.

Reporting Problems

In some cases, you will not be able to correct the problem that occurs (for instance, a module failure). In such cases, you should contact Alcatel Technical Support at one of the following locations:

West Coast:

Alcatel Technical Support
26801 West Agoura Road
Calabasas, CA 91301

Telephone: 1-800-995-2696 (Domestic) 818-878-4507 (International)

Fax: 818-878-3505

Web: www.ind.alcatel.com/support

Email: support@ind.alcatel.com

East Coast:

Alcatel Technical Support
100 Nagog Park
Acton, MA 01720

Telephone: 1-800-995-2696 (domestic); 818-878-4507 (international)

Fax: (978) 264-3933

Web: www.ind.alcatel.com/support

Email: support@ind.alcatel.com

When reporting problems, you should note hardware and software details, as described in the subsections that follow.

Report Hardware Details

When reporting problems you should be ready to report the following hardware details to Alcatel Technical Support:

- Type of chassis (Omni Switch/Router or OmniSwitch) and version of chassis (e.g., Omni-3wx, OmniS/R-9)
- Frame- or cell-based backplane
- Serial number of chassis and module(s)
- Type of module that failed
- Hardware revision of module
- Model number of power supply
- UPS or direct connect to power source
- Any dump files on the flash file system

Report Software Details

When reporting problems you should be ready to report the following software details to Alcatel Technical Support:

- Software revision (e.g., 3.4.8, 4.3.2)
- Whether the feature never worked or was intermittent
- Bridging or routing configured
- Multiple groups or VLANs configured
- IP PING access
- Statistics incrementing correctly
- Protocols used
- Any capture file (trace) available
- Any dump files on flash file system

Understanding Problems

The following self-questions can be used to get a better idea on the nature of the problem:

- Has this functionality ever worked?
- What changes have occurred in the network? Was software upgraded? Were device(s) added?
- Are all users affected or are the problems related to a single port, module, or switch?
- Are statistics (as reported by UI commands such as **vs**, **ve**, **bps**, and **rmon**) incrementing on the affected port(s)?
- Are all protocols (routed or switched) failing?
- Can the affected device be successfully pinged via IP/IPX?
- Can a trace be captured on the affected segment(s)?
- Is an external analyzer, such as a Sniffer or Alcatel's Port Mirroring/Port Monitoring, available?

This chapter provides documentation on some common problems and potential solutions for problems with your switch in the sections that follow.

Software Installation Problems

If you encounter problems during software installation, most likely you will see error messages that indicate the problem.

If you cannot install the software, you can use the Boot Line prompt to download files via ZMODEM or a computer attached to a SLIP line. You can also temporarily set boot parameters and load from Boot Line in an attempt to load under different settings (refer to Appendix A, "The Boot Line Prompt"). For more information about loading software via ZMODEM, refer to Chapter 9, "Installing Switch Software."

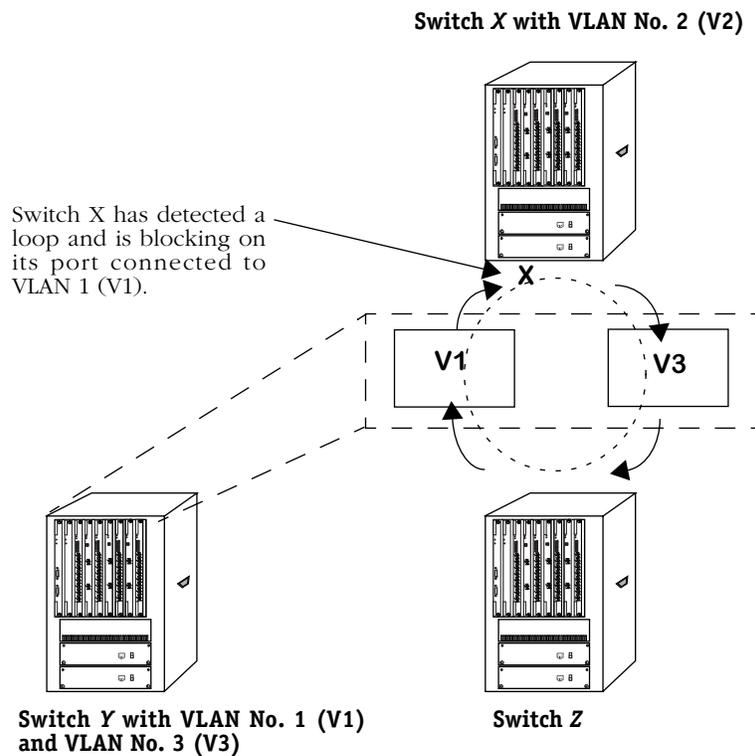
Operational Problems

The following paragraphs describe operational problems you may encounter.

Deadlocked VLAN

Occasionally, a VLAN may deadlock. This may be a result of the configuration process you used when you set up the VLANs.

If, for example, you have a setup with three switches, as shown in the following figure, the VLAN can enter a deadlock. In this example, there are two switches, one configured with one VLAN (Switch X), another configured with two VLANs (Switch Y), and another switching device that connects to the VLANs (Switch Z).



Deadlocked VLANs Due to Loop

In this situation, VLAN 2 (V2) in the Switch X is in a loop because it has not learned that it has connected to Switch Y with two virtual bridges (V1 and V3), which are inside one switch. Since V2 detects a loop, it invokes blocking at the port connected to V1, which results in a deadlock. V1 and V3, inside Switch Y, can still communicate, and traffic still exits V2 in Switch X, going to V3; however, traffic will not exit V3.

To determine if this problem has occurred in your setup, you can use the **vi** command to display information about a specific port. (See Chapter 24, “Managing Groups and Ports,” for more information on the **vi** command.) The syntax for this command is as follows:

```
vi <slot>/<interface>
```

The system will show the port in Blocking mode and not in Forwarding mode.

Probable Cause

You did not configure the network from the point furthest away from the point of connection.

Solution

To rectify the problem, you should always start configuration from the switch that is the furthest away from the point of connection. In the figure on page 57-6, for example, you would start the change from V2 in Switch X. By configuring this switch first, you would set it up to see the two VLANs in Switch Y, and use two Spanning Trees to looping.

Problems with IP Applications

You may have enabled routing on a VLAN, but have problems with PING and other IP applications.

Probable Cause

When routing is enabled on a VLAN, packets will not be forwarded unless the Spanning Tree Status for the port being forwarded to has progressed from Listening to Learning to Forwarding.

You can determine if Spanning Tree Protocol has entered the Forwarding state for a port by viewing port status with the **sts** command. Refer to Chapter 22, “Configuring Bridging Parameters,” for information on Spanning Tree Status and the **sts** command.

Solution

Spanning Tree algorithms put the ports into the correct state. There may be propagation delays when the Spanning Tree passes protocol information throughout a bridged network. This is normal as bridge ports wait for new topology information and for the lifetime of frames being forwarded using the old topology to expire. Immediate transitions from port state to port state should not be expected.

If the port is in the blocking mode, then the Spanning Tree has detected a loop. Blocking is a desired, preventive measure invoked by the Spanning Tree algorithm.

You should not attempt to alter the port state or remove the Spanning Tree. If you attempt to move a port from non-participation to the forwarding state, you take the risk of introducing data loops.

Once in the Forwarding state, PINGs and other IP applications should function properly.

Protocol Problems

You may notice an abnormal number of errors in a particular protocol. You can view protocol errors by using the networking commands. Refer to Chapter 30, "IP Routing," for more information on the networking commands.

Probable Cause

Incompatible versions of the protocol are running on stations in the network.

Solution

Check the version of the protocol and verify that you are using the same version on all stations in the network. For example, you may be required to run Spanning Tree, Revision C on all stations.

Also, check the parameter values that you set for the protocol.

Hardware Problems

The following sections describe problems you may encounter with switch hardware.

LEDs Do Not Light on All Modules

You have turned on the power supply to the switch, but the LEDs on the modules do not light.

Probable Cause

The power supply has blown a fuse.

Solution

Call Alcatel Technical Support unless you have an Omni-5 or Omni-9. The power supplies on these chassis are shipped with a spare, 250-Volt, 3.15 amp fuse. See Chapter 5, "OmniSwitch Power Supplies," for information on locating the spare and replacing the fuse.

If replacing the fuse does not cause the LEDs to light, call Alcatel Technical Support.

Amber Color in LEDs

During power-up, the switch goes through a Power-On Self Test (POST). Results of the test are reflected in the OK1 and OK2 LEDs on the MPM/MPX and switching modules; specifically, OK1 indicates hardware failures, while OK2 indicates software failures.

The first time you start the switch, the OK1 LED will blink in amber once to indicate start mode. The OK2 LED will blink in green rapidly to indicate image loading. Thereafter, OK2 should blink slower in green to indicate operational mode.

Probable Cause

Hardware failure or software failure.

Solution

If the amber LED displays on a switching module, replace the module with a known, good module.

If the amber LED displays on the MPM/MPX, or after replacing the switching module the problem persists, shut down the switch and call Alcatel Technical Support.

Non-Blinking OK2 LED

When the switch is operating properly, the OK2 LED blinks in green. When the OK2 LED displays a steady green light, this is an indication of problems.

Probable Cause

The MPM/MPX or the software is malfunctioning. Typically the problem cannot be resolved by rebooting.

Solution

Shut down the switch and call Alcatel Technical Support.

TEMP LED is Amber

If the TEMP LED is amber, the internal temperature of the switch has exceeded the operational limit.

Solution

Perform the following steps:

1. Turn off the switch and wait until it has completely cooled down.
2. Check the immediate environment and ensure that the switch is not located in an area where it can be overheated by other heat-producing devices.
3. Ensure that the switch is located in an area where there is ample room for air flow around the chassis.

If the environment is satisfactory, check the internal cooling fans. The switch is shipped with redundant fans that start automatically when you power up the unit. Try powering up and listen for the fan motors. Also, you should feel a slight air flow near the chassis. If the fans are not working, power down and contact Alcatel Technical Support.

STA LED Is Off

There is one status LED per port on Ethernet switching modules. When lit, it indicates that a good cable connection exists to an Ethernet device.

Probable Cause

The LAN cable is not connected properly or is faulty.

Solution

Check all port connections and inspect the cable. If you find a faulty cable, replace the cable.

Cannot Use SLIP Line on an MPM

You may have connected a SLIP line or terminal to either of the two serial ports, and configured SLIP, using the **slipc** command, in the UI, but you still cannot connect.

Probable Cause

Jumper settings on the MPM are not set up for SLIP.

Solution

Move shunts on jumper block 452-457 for SLIP. Chapter 6, "The Management Processor Module (MPM)," describes the jumper block location and jumper settings for SLIP.

◆ Note ◆

The MPX, MPM-C, and MPM-III do not have jumpers that affect SLIP.

Switch Does Not Boot When Flash File System Is Full and Trying To Create the `mpm.cnf` File

You may have saved too many files to the flash file system. If the flash file system is full, it will be unable to create the `mpm.cnf` file and it will be unable to complete the boot process.

Probable Cause

Unnecessary image or data files exist in the flash file system.

Solution

Follow the steps below to free up memory in the flash file system.

1. Reboot the switch and enter the Boot Line prompt. (See Appendix A, “The Boot Line Prompt,” for more information.)
2. Use the Boot Line **R** command to delete any unnecessary files. Make sure you have enough room for the switch to create the `mpm.cnf` file.
3. Use the Boot Line **@** command to continue the boot process.

Error Messages

This section provides error messages that you may encounter in the UI.

Understanding Error Messages

Error messages reflect hardware or software problems that the switch encountered during initialization, configuration, or operation.

In some instances, the messages that display on the UI show the C program function name. For example:

cmSetTTY(): Illegal port requested

where **cmSetTTY** represents the function, and **()** indicates that parameters are passed. This information is for internal debugging purposes.

In this section, the phrase **xxx** in error messages represents a value that is specific to that message. For example, in the message **board type xxx**, the specific board type displays in the error message.

Correcting Errors

In most cases, you will not be able to correct error conditions that result because of internal hardware or software malfunctions. You should contact Alcatel Technical Support when you receive these messages. Refer to *Reporting Problems* on page 57-3.

You can correct error conditions that result because incorrect parameter values were entered during configuration. The tables that follow list error messages to which you can respond.

Module Startup/Shutdown Error Messages	
Message	Corrective Action
False Shutdown: restarting to handle queued msgs	This message does not reflect an error condition. No action required.
P3 diags failed...	Message results when the module fails diagnostic tests. Try replacing the module.
Download failed	Try replacing the module.
No reply from VSE driver board-up request	Try replacing the module.
No reply from MBox	Try replacing the module.

Serial Port Configuration Errors	
Message	Corrective Action
Problem deleting SLP port xxx, errno=xx	Reboot the system, then use the Boot Line configuration to force SLIP down at the boot line (refer to Appendix A “The Boot Line Prompt”).
Can't modify SLIP if it's not up! current mode=xxx	Reconnect the SLIP line; reconfigure using the slipc command; on MPMS, verify that jumpers on are set for SLIP (refer to Chapter 6 “The Management Processor Module (MPM)”).
Problem changing SLIP remote IP addr to xxx	Check the remote IP address by using the slipc command at the UI. Refer to Chapter 10, “Configuring Management Processor Modules.”
Couldn't setup SLIP port slxxx on xxx	Reboot the switch.

Module Connection Errors	
Message	Corrective Action
interrupt: Link Error Monitor ALERT on xxx/xxx PHY-xxx	If this message shows up once or twice, it probably means that someone is plugging a new cable in slot/port xxx/xxx, physical connector xxx. If it displays more frequently, then there is probably a bad CDDI or FFDI connection on slot/port xxx/xxx, physical connector xxx, caused by either dirty connectors or bad cabling. Try cleaning the connections or replacing the cabling.

Chassis Error Messages

The slots in the messages within the following table are all zero based. That is, Slot 1 will be displayed as “Slot 0,” Slot 2 will be displayed as “Slot 1,” etc.

Chassis Error Messages Table	
Message	Corrective Action
Problem deleting SLP port xxx, errno=xx	Reboot the system, then use the Boot Line configuration to force SLIP down at the boot line (refer to Appendix A “The Boot Line Prompt”).
Unknown mod type xxx in slot xxx	Remove the module from the slot.
Board xxx needed to be restarted at xxx	The module appears dead. Remove the module from the slot and replace with a known good module.
Chassis mgr discovered xxx has a problem!	The software has discovered a dead task. The system will reboot automatically.
System seems to have (perhaps) recovered. A reboot may not be unwise, however.	The system encountered an unexpected condition. Reboot the switch.
cm_Mod_Event(): the slot wasn't empty	The system is confused. Clear the system by rebooting it.
ERROR: can't read ID info from MPM in slot xxx...shutting down chassis manager	This may indicate a bad MPM/MPX. Try power cycling.
Please run cmConfigEPROMxxx and reboot	This may indicate a bad MPM/MPX. Try power cycling.
Can't read ID info from slot.xxx fail...	This may indicate a bad module in slot xxx. Try power cycling.
cm_Mod_Event(): slot was already empty!	Reboot the system.
Problem reading ID PROM on module xxx	Try power cycling. If the problem remains, remove the module and try another slot.
ID PROM on module xxx has unknown format number xxx	Try power cycling. If the problem remains, remove the module and try another slot.
Real-Time Clock not set yet! Starting at zero.	Reset the clock by using the uic command.
Unknown modem stop bits=xxx	Change stop bits by configuring boot line (refer to Appendix A “The Boot Line Prompt”).
Couldn't read reset count, returning 0	This message appears only once if the configuration file is removed.

continued on next page...

Chassis Error Messages Table (Cont.)	
Message	Corrective Action
Couldn't read chassis description, setting default	Enter a new chassis description with the syscfg command.
cmSavePortInfo() successful	This message does not indicate an error.

58 Running Hardware Diagnostics

Hardware diagnostics provide you with software tools for diagnosing hardware-related problems on OmniSwitch and Omni Switch/Router switching modules. These diagnostics allow you to test switching modules off-line during network down time.

The OmniSwitch and Omni Switch/Router have a variety of switching modules interconnected by a frame backplane and/or cell backplane, and a management backplane. When a hardware failure occurs, the problem may be related to a number of different failures. As part of a systematic troubleshooting procedure, you can use the built-in diagnostic software to test basic connectivity and functionality.

The diagnostic software includes two basic types of tests: static tests and port tests. Static tests verify the basic functions of memory and control/status registers of submodules. Port tests check for data packet processing functions.

You can run the tests individually or sequentially. Diagnostic software also provides an option that allows you to run all the tests in one session (exception: WSX modules require power recycle after static test). The diagnostic tests performed vary, depending on the switching module type under test.

◆ Important Note ◆

For Release 4.4 and later, the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. Because Hardware Diagnostics are supported only in UI mode, you must change from CLI mode to UI mode to run Hardware Diagnostics. See Chapter 8, “The User Interface” for information on changing from CLI mode to UI mode.

The following tests are available for the OmniSwitch and Omni Switch/Router:

- **alpreg** Alpine ASIC Register Test
- **bigft** Bigfoot ASIC Register Test
- **csr** Command Status Register Test
- **gigareg** Giga-Chip ASIC Register Test
- **ifled** Submodule LED Test
- **ilb** Internal Loopback Test (replaces **mloopphy** in Release 3.4 and later)
- **ilbstress** Internal Loopback Stress Test
- **mammem** Mammoth ASIC Register and Memory Test
- **mamcam** Mammoth CAM Test
- **mloopmac** Mammoth MAC Loopback Test
- **mvbus** Mammoth VBUS Test
- **port** Port Traffic Test

- **sahi** SAHI Register and Memory Test
- **stress** Port Stress Test (available for Ethernet and CSM modules)
- **submem** Submodule Local Memory Test
- **sunl** SUNI Register Test
- **whsreg** Whistler Register Test
- **wsmcable** WSM/WSX Cable Connection Test

The following tests available for the Omni Switch/Router only:

- **elsy** ELSY SARs and Memory Test (ASX-M-622F-2W modules)
- **hrexmem** HRE-X Memory Test
- **hrexport** HRE-X Port Test (MPX only)
- **morreg** Moriah Register Test
- **mreg** M013 Register Test
- **pcam** Pseudo CAM Test
- **pcibus** IOP480 PCI Bridge and Host DRAM Test (ASX-M-622F-2W modules)
- **tdat** TDAT042G5 Framer Test (ASX-M-622F-2W modules)
- **tellreg** Telluride Register Test
- **ward** Ward FPGA and CAMs Test (ASX-M-622F-2W modules)
- **xcam** Alcatel CAM Off-Board Test

The following tests available for the OmniSwitch only:

- **boardup** Board Up Test
- **camoffbrd** CAM Off-board Test
- **camonbrd** CAM On-board Test
- **cbrport** Constant Bit Rate Port Test
- **cmreg** CSM-AB-CM Register Test
- **cmtest** CSM-AB-CM Clock Test
- **dmux** Mux/Dmux Register Test
- **fabric** Fabric Register Test
- **hrecam** HRE CAM Test
- **hremem** HRE Memory Test
- **hreport** HRE Data Port Test
- **iop** Input/Output Processing Register and Memory Tests, and BIST
- **loopdle** DLE Loopback Test
- **loopfi** FCSM Fabric Interface (FI) Loopback Test
- **looppmc** PMC Loopback Test

- **loopsahi** FCSM II SAHI Loopback Test
- **loopvit** Vitesse Loopback Test
- **mpmmem** MPM-C Memory Test
- **pal** PAL Test
- **phyreg** PHY Register Test
- **sercable** Serial Cable Connection Test
- **vbus** VRAM Bus Test
- **vram** Video RAM Test

Running Diagnostics

You must log in to the **diag** account to access the hardware diagnostics functionality or use the **framefab** and **cellfab** commands.

There are several image files used for hardware diagnostics. These files have the following uses:

- **diagx.img** Omni Switch/Router diagnostics image file
- **desx.img** Omni Switch/Router stress test image file
- **diag.img** OmniSwitch diagnostics image file (MPM, MPM-II, MPM-1G)
- **diagc.img** OmniSwitch diagnostics image file (MPM-C)
- **diag3.img** OmniSwitch diagnostics image file (MPM-III)
- **dmesm.img** OmniSwitch stress test image file
- **dni.img** OmniSwitch on-board diagnostics test image file (must be used with non Mammoth-based modules)

◆ Note ◆

To function properly, hardware diagnostics must be run offline (i.e., the switch should not be connected to a network) or during network downtimes. In addition, spanning tree must be set to **OFF** via the **stc** command. For details on using the **stc** command, see Chapter 22, “Configuring Bridging Parameters.”

The OK2 LED of the module under test will be set to red if a failure is detected by diagnostic testing. The OK2 LED can be restored by resetting the module or by rebooting the chassis.

Diagnostics may not run if the **mpm.cfg** and **mpm.cnf** files (for OmniSwitch) or **mpx.cfg** and **mpx.cnf** files (for Omni Switch/Router) are not in their default configurations. In addition, some diagnostics may affect the settings in configuration files. Therefore, any customized **mpm.cfg** and **mpm.cnf** files (for OmniSwitch) or **mpx.cfg** and **mpx.cnf** files (for Omni Switch/Router) should be saved prior to testing. Once testing is completed, these files should be restored and the chassis rebooted prior to normal operation.

◆ Note ◆

The following steps reference the **mpm.cfg** and **mpm.cnf** filenames for OmniSwitch. For Omni Switch/Router, use **mpx.cfg** and **mpx.cnf** as the filenames instead.

The default **mpm.cfg** and **mpm.cnf** files are obtained by performing the following steps:

1. Remove these files from flash memory by renaming the files to names besides **mpm.cfg** and **mpm.cnf**. For example, you can rename **mpm.cfg** to **mpm_cfg.old** to highlight the fact that it is the original version of the file.
2. Delete the **mpm.cfg** and **mpm.cnf** files from flash memory.
3. Reboot the system. The management processor module (an MPM on an OmniSwitch and an MPX on an Omni Switch/Router) will create default **mpm.cfg** and **mpm.cnf** files when these files are missing from flash memory. These default files are the ones to be used with diagnostic software.

Login to Run Diagnostics

You must log in to the **diag** account to access the hardware diagnostics functionality. The **diag** user is a superset of the **admin** user. The **diag** user can run all hardware diagnostics in addition to all of the capabilities available to the **admin** user. The default password for the **diag** user is **switch**.

Once logged in as a **diag** user, the Main Menu will display as follows.

Command	Main Menu
File	Manage system files
Summary	Display summary info for VLANs, bridge, interfaces, etc.
VLAN	VLAN management
Networking	Configure/view network parameters such as routing, etc.
Interface	View or configure the physical interface parameters
Security	Configure system security parameters
System	View/set system-specific parameters
Services	View/set service parameters
Switch	Enter Any to Any Switching Menu
Help	Help on specific commands
Diag	Display diagnostic level commands
Exit/Logout	Log out of this session
?	Display the current menu contents

Note the menu listing for **Diag** underneath the **Help** sub-menu. To access the diagnostics sub-menu, enter **diag** at the prompt. If the display mode is set to verbose, the diagnostics sub-menu will display as follows:

Command	Diagnostic Menu
reset	Reset a module in a slot
maskta	Control masking of temperature alarm led
test	Run tests on one or more slot modules
cellfab	Run the Cell Fabric Tests
framefab	Run the Frame Fabric Tests
testdisp	Display test blocks on one or all slot modules
testcfg	Configure test parameters on one or all slot modules

The **test** command is the main interface into the diagnostics functionality; you must log in as **diag** to run this command. The **testdisp** and **testcfg** commands also require being logged in as **diag** to run these commands. The **reset** and **maskta** commands have specialized functionality; you do not have to be logged in as **diag** to use these commands, but you do at least need to be logged in as **admin**. Each of the sub-menu options are described in the sections that follow.

Resetting a Switching Module

The **reset** command initiates a soft reset on the module in a specified slot. Conceptually, resetting a switching module with this command is similar to switching off power to the module; the module will be in the same state after a reset as it is after a power on.

◆ Notes ◆

Some NI modules do not support the **reset** command.

The primary MPM module cannot be reset. To reset the secondary MPM, use the **secreset** command, which is described in Chapter 10, “Configuring Management Processor Modules.”

To reset a switching module, enter the **reset** command followed by the slot number for the module. For example, to reset the switching module in slot 4, enter:

```
reset 4
```

A message similar to the following displays:

```
Resetting slot of type xxxx may crash system
Attempt reset anyway {Y/N}? (N) :
```

Enter a **Y** and press **<Enter>** at this point. The module will be reset and the following message will indicate the reset took place:

```
resetting slot 4 to enable
```

Disabling a Switching Module

The **reset** command can also be used to disable a switching module. When used in conjunction with the **swap** command, this option is useful if you want to hot swap a module. (See Chapter 7, “OmniSwitch Switching Modules,” for information on how to hot swap a switching module.)

To disable a switching module, enter the **reset** command followed by the slot number for the module and followed by **disable** at the system prompt. For example, to reset the switching module in slot 4, enter:

```
reset 4 disable
```

To enable the switching module again, enter the reset command followed by the slot number for the module, and followed, optionally, by **enable** (**enable** is the default for the **reset** command). For example, to enable a previously disabled switching module in slot 4, enter:

```
reset 4 enable
```

Temperature Masking

The temperature sensor on the original MPM (not the MPM II, MPM III, MPM-C or MPM 1G) initiates an alarm in some cases when an over-temperature condition does not exist. In addition, due to device hysteresis, once this alarm is triggered it does not reset until the device cools down significantly. These false alarms are due to the low accuracy of the temperature sensor on the original MPM (not applicable to the OmniStack).

The **maskta** command provides a way of modifying the behavior of the temperature alarm to mask the effect of the temperature sensor. By masking the temperature alarm bits, you can ensure that the MPM's TEMP LED doesn't signal or that it resets after a specified delay time. By default, temperature masking is disabled.

To enable temperature masking, enter

```
maskta enable
```

This command masks the temperature alarm completely. The TEMP LED will not signal, even if the temperature exceeds the set ranges. The following message confirms the masking:

```
Masking of Temperature Alarm enabled
```

You could also enable temperature alarm masking but not mask the alarm completely. If you enter an integer after the **maskta enable** command, the TEMP LED will still signal, but it will reset after the number of minutes you specified. For example, if you enter the command

```
maskta enable 5
```

the temperature alarm will still signal, but it will reset automatically five (5) minutes after the alarm-initiating event occurs.

◆ Note ◆

Once you enter a minute value when enabling temperature alarm masking, that value is saved even if you disable masking. To reset the minute value, you must re-enable temperature alarm masking and set the minute value to zero (i.e., enter the command **maskta enable 0**).

To disable temperature alarm masking, enter:

```
maskta disable
```

This is the default setting, so you only need to specify this command if you had previously enabled alarm masking. The following message confirms that you disabled masking:

```
Masking of Temperature Alarm disabled
```

Running Hardware Diagnostics

The **test** command initiates one or more test routines on a switching module that you specify. You can also optionally test all switching modules in one test session. Test status, instructions, and a summary of results are provided as output. Start a diagnostic test session using the following command syntax:

```
test <slot_number> [<repeat_count> [<test_name>]]
```

where

- <slot_number>** Indicates the slot number in the OmniSwitch/OmniStack for the module on which you want to run tests. If you enter **all** for this parameter, then all switching modules in the chassis will be tested. This parameter is required; if you do not enter a slot number then the test session will not start.
- <repeat_count>** Indicates the number of times to run the specified tests on the module. This value can be an integer between 0 and 999. A value of zero (0) repeats the test infinitely. The default value is 1. This default will be assumed if you do not enter a **repeat_count**.
- <test_name>** Indicates the test to be performed on the module. You can indicate the test name or **all** to run all tests. You can enter only one test name or **all**. The default is **all**. This default will be assumed if you do not enter a **test_name**.

◆ Note ◆

A combination of **repeat_count** set to **0** and **test_name** set to **all** allows the user to run either the port test infinitely or all off-board tests infinitely. If the user chooses to run the port test when prompted, all the static tests (memory and control/status register tests) are run once, followed by an infinite run of the port test. See *Sample Command Lines* on page 58-13 for more information.

Descriptions of each test follows:

- alpreg** Tests the Alpine registers. Test the Alpine control logic, registers, and data/address lines.
- bigft** Tests the Bigfoot registers. Test the Bigfoot control logic, registers, and data/address lines.
- boardup** Basic tests of the switching module including an image file download, communication with the MPM over the MBUS, reset circuitry, interprocessor communication, and the switching module's CPU.
- camoffbrd** Tests the CAM memory on the switching module. This test is run by the MPM over the management bus. It tests the CAM control logic, CAM access, and the data line and buffers.
- camonbrd** This CAM test is similar to the one executed by **camoffbord** except it is executed by code downloaded to the switching module. The switching module's CPU runs this CAM test.

cbrport	Tests the CBR Port. Two port tests are performed: one through the Utopia Mux/AAL5 port, and the other through the CBR Port. The Utopia Mux/AAL5 port test generates packets in the switching module's AAL1 SAR and sends them through interface Mux and AAL5 network port and back to the AAL1 SAR for verification. The CBR port test generates packets in the switching module's AAL1 SAR and sends them through the CBR port and back to the AAL1 SAR for verification. This test requires external cables. The system will provide user with instructions for setting up external cables or wrap plugs for port test and prompts the user for input upon completion of setup. This test can be bypassed in case cables are not available. For information on cables required for port test, see <i>OmniSwitch Port Test Wrap Cable/Plug Requirements</i> on page 58-14.
cmreg	Tests the CSM Clock Module registers. Test the CSM Clock Module control logic, registers, and data/address lines.
cmtest	Tests the CSM Clock Module external and internal clock resolution logic. This test requires additional hardware (e.g., FCSM, WSM-T1, CSM-AB-155, CSM-AB-DS1.)
csr	Tests the command/status registers. Includes testing management bus buffers, management bus read/write control logic, reset and LED memory, ID EEPROM, and reset circuitry.
dmux	Tests the Demux registers. Test the Demux control logic, registers, and data/address lines.
elsy	Tests Tx and Rx ELSY registers, data/address lines and attached external memory (2MB SRAM, 32MB DRAM).
fabric	Tests the Fabric ASIC registers. Test the Fabric ASIC control logic, registers, and data/address lines.
gigareg	Tests the Giga-Chip registers. Test the Giga-Chip control logic, registers, and data/address lines.
hrecam	Tests the HRE CAM. Tests the HRE CAM control logic, CAM access, and the data line and buffers.
hremem	Tests the HRE local memory. Includes testing the HRE read/write functions, data/address, and the memory.
hreport	Tests the HRE. Packets are generated by the MPM and placed on the VBUS to be claimed by the HRE. The HRE will insert additional routing information to the claimed packet and place it back on the VBUS to be claimed and verified by the MPM. This test does not require external cables. This test can be bypassed.
hrexmem	Tests the HRE-X's local memory. Includes testing the HRE-X read/write functions, data/address, and the memory.
hreport	Tests the HRE-X's functions. Packets are generated by the MPX, sent out to the port, and claimed by the HRE-X. The HRE-X will insert additional routing information to the claimed packet and place it back on MVBUS to be claimed and verified by the MPX. This test can be bypassed. See <i>Running Diagnostics on an Entire Chassis</i> on page 58-37.

ilb	Performs a port test using the internal loopback at the PHY or framer interface. Packets are generated by the MPM/MPX and sent out to the port and returned through an internal loopback within the PHY or framer. The MPM/MPX verifies the packets on a bit by bit basis.
ilbstress	Performs a stress test using the internal loopback at the PHY or framer interface. Packets are generated by the MPM/MPX and sent out to the port and returned through an internal loopback within the PHY or framer. The MPM/MPX verifies the packets on a bit by bit basis. See the description for stress test on page 58-12. If Ethernet type switch is tested, this test requires the dmesm.img (OmniSwitch) or desx.img (Omni Switch/Router) to be in the flash memory.
ifled	Tests the Control/Status LED register. Tests the write function of the Control/Status LED register, LED data lines, and LEDs.
iop	Tests the IOP registers, external memories and control logic. Includes testing IOP functionality by invoking and verifying IOP Built In Tests. Data/address are also tested.
loopdle	Tests the DLE internal loopback. Packets are generated by the MPM packet and sent through the VBUS to the switching module, internally looped back, and returned to the MPM for verification. This test does not require external cables. This test can be bypassed.
loopfi	Tests the FCSM IOP internal loopback. Packets are generated by the MPM packets and sent through the VBUS to the switching module, internally looped back, and returned to the MPM for verification. This test does not require external cables. In addition, this test can be bypassed.
looppmc	Tests the PMC Internal Loopback. Packets are generated by the MPM packets and sent through the VBUS to the switching module, internally looped back, and returned to the MPM for verification. This test does not require external cables. This test can be bypassed.
loopsahi	Performs a port test using the internal loopback within the SAHI ASIC. Packets are generated by the MPM/MPX and sent out to the port and returned through an internal loopback within the SAHI ASIC. The MPM/MPX verifies the packets on a bit by bit basis.
loopvit	Tests the Vitesse Internal Loopback. Packets are generated by the MPM packets and sent through the VBUS to the switching module, internally looped back, and returned to the MPM for verification. This test does not require external cables. This test can be bypassed.
mamcam	Tests the Mammoth CAM. Tests the Mammoth CAM control logic, CAM access, and the data line and buffers.
mammem	Tests the Mammoth registers and memory. Includes testing the Mammoth control logic, registers, internal memory, internal cache, external SDRAM, SRAM, and data/address lines.
mloopmac	Performs a port test using the internal loopback within the Mammoth MAC chip. Packet are generated by the MPM/MPX and sent out to the port and returned through an internal loopback within the Mammoth MAC chip. The MPM/MPX verifies the packets on a bit by bit basis.
morreg	Tests the Moriah registers. Test the Moriah control logic, registers, and data/address lines.
mpmmem	Tests MPM-C's memory.

mreg	Tests the M013 submodule registers' control logic, registers, and data/address lines.
mvbus	Tests the mammoth VBUS circuitry. Frames are generated within the Mammoth buffer system, sent out the VBUS, and then received on various Mammoth queues. Data integrity is verified.
pal	Tests the LED PAL. Includes testing the PAL control logic, LEDs, and data lines.
pcam	Tests the HRE-X Pseudo CAM. Tests the HRE-X Pseudo CAM control logic, CAM access, and the data line and buffers.
phyreg	Tests the PHY registers. Test the PHY control logic, registers, and data/address lines.
pcibus	Tests the IOP480 PCI Bridge, data/address lines, and host memory (16MB DRAM).
port	Functional testing of physical ports with a burst of data packets generated by the MPM/MPX. Packets are generated by the MPM/MPX, sent out the physical port, looped back through external cables or wrap plugs, and returned to the MPM/MPX. The returned packets are verified bit by bit by the MPM/MPX. Except for FCSM I/II, the port test requires the use of external cables or wrap plugs. The system will provide user with instructions for setting up external cables or wrap plugs for port test and prompts the user for input upon completion of setup. This test can be bypassed if cables are not available. For more information on port tests, see <i>Port Tests</i> on page 58-13. For information on cables required for the port test, see <i>OmniSwitch Port Test Wrap Cable/Plug Requirements</i> on page 58-14 for the OmniSwitch and <i>Omni Switch/Router Port Test Wrap Cable/Plug Requirements</i> on page 58-22 for the Omni Switch/Router.
◆ Important Note ◆	
	For VSD and VSA submodules, the port test requires no outside cabling. It is a combination of multiple static tests for the submodule, rather than a traffic test.
sahi	Tests SAHI registers. Includes testing SAHI control logic, internal memory, and data/address.
sercable	Tests the switching module's capability of identifying whether a serial cable is connected or not and what type of serial cable connected to its port(s). Includes testing of serial cable line, transceiver, and PLD.

stress	Functional testing of physical ports with continuous full-wire traffic. The data packets are initially generated by the MPM/MPX, sent out the physical port, and looped back through external cables or wrap plugs. Once the packets are returned, modifications in the packets' destination address allows the packets to continuously circulate between the NI CPU and the external cables or wrap plugs for a predefined period. Once the predefined period is reached the packets are returned to the MPM/MPX. The packets are checked on a bit by bit basis by the MPM/MPX. If Ethernet type switch is tested, this test requires the dmesm.img (OmniSwitch) or desx.img (Omni Switch/Router) to be in the flash memory. Stress test requires the use of external cables or wrap plugs. The system will provide user with instructions for setting up external cables or wrap plugs for stress test and prompts the user for input upon completion of setup. For more information on port tests, see <i>Port Tests</i> on page 58-13. For information on cables required for the port test, see <i>OmniSwitch Port Test Wrap Cable/Plug Requirements</i> on page 58-14 for the OmniSwitch and <i>Omni Switch/Router Port Test Wrap Cable/Plug Requirements</i> on page 58-22 for the Omni Switch/Router.
submem	Tests the submodule's local memory. Includes testing local memory control logic, data/address lines, and local memory.
sunl	Tests the SUNI registers. Includes testing the SUNI control logic, registers, and data/address lines.
tdat	Tests TDAT042G5 Framer registers and data/address lines.
tellreg	Tests the Telluride ASIC registers. Test the Telluride ASIC control logic, registers, and data/address lines.
vbus	Test the VBUS transmit and receive functions. Packets generated in the switching module's VRAM are sent out the VBUS from the switching module under test to itself. The switching module claims and inspects the packets. Also tests the SAM control logic and the VRAM Sequence Engine (VSE).
vram	Tests the VRAM memory. Includes testing VRAM control logic, VRAM access memory, and data/address lines.
ward	Tests Ward FPGA, CAMs, and memory (64K SRAM).
whsreg	Tests the Whistler registers. Test the Whistler control logic, registers, and data/address lines.
wsmcable	Tests the detection of DCE and DTE cables by the WSM circuitry. The operator is prompted for the appropriate cable connection.
xcam	Tests the Alcatel CAM. Tests the Alcatel CAM control logic, CAM access, and the data line and buffers.

Sample Command Lines

There are numerous ways to specify a test session through the **test** command. The following are some sample command lines along with a description of what they test. The following command:

```
test all 100 vram
```

would run the VRAM test on all the modules in the chassis that are capable of executing the VRAM test for 100 times. In another example, the following command:

```
test 3 0 all
```

would run either all the static tests or the port test on the module in slot 3 infinitely. Finally, the following command:

```
test 4 5
```

would run all tests (the default) on the module in slot 4 five (5) times.

Halting Diagnostic Tests in Progress

Depending on how many tests and repeat iterations you specify, a test session could take some time to complete. If you need to halt in-progress tests, enter **CTRL-C**. This key sequence pauses the testing and provides a test summary report. You will be prompted to resume or terminate the testing after the pause.

◆ Note◆

During certain phases of diagnostic testing, the **CTRL-C** will not be immediately processed. This delay may last several seconds, or longer.

Port Tests

Because port-to-port cabling is required, port tests may not be available on some modules with only one port, one daughtercard, or on some modules with mismatched daughtercards. (For example, 100BaseTx modules cannot run port tests with single or mismatched daughtercards.) When a port test is run, packets are generated in the MPM and sent out to the switching module, externally looped, and sent back to the MPM. The MPM then inspects the packets. The tables on the following pages provide specific cable/plug information.

◆ Important Note ◆

For VSD and VSA submodules, the **port** test requires no outside cabling. It is a combination of multiple static tests for the submodule, rather than a traffic test.

OmniSwitch Port Test Wrap Cable/Plug Requirements	
Module Type	Cable Type
ASM-155C	ASM/CSM Wrap Plug. Refer to <i>ASM/CSM Wrap Plug – RJ-45 Connector</i> on page 58-40.
ASM-155FM	Multi-mode fiber optic wrap plug with SC connectors.
ASM-155FS	Single-mode fiber optic cable with SC connectors.
ASM-CE (SC port)	Single-mode fiber optic cable with SC connectors.
ASM-CE (Serial port)	Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.
ASM-CE (T1/E1 port)	T1/E1 Crossover Wrap Cable. Refer to <i>T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
ASM-DS3	RG 59/U Type coaxial cable with BNC connectors.
ASM-E3	RG 59/U Type coaxial cable with BNC connectors.
ASM2-155FM	Multi-mode fiber optic wrap plug with SC connectors.
ASM2-155FS	Single-mode fiber optic cable with SC connectors.
ASM2-155FH	Single-mode fiber optic cable with SC connectors. Requires fiber optic attenuator.
ASM2-155RFM	Multi-mode fiber optic wrap plug with SC connectors.
ASM2-155RFS	Single-mode fiber optic cable with SC connectors.
ASM2-622FM	Multi-mode fiber optic wrap plug with SC connectors.
ASM2-622FS	Single-mode fiber optic cable with SC connectors.
ASM2-622FH	Single-mode fiber optic cable with SC connectors. Requires fiber optic attenuator.
ASM2-622RFM	Multi-mode fiber optic wrap plug with SC connectors.
ASM2-622RFS	Single-mode fiber optic cable with SC connectors.
ASM2-622RFH	Single-mode fiber optic cable with SC connectors. Requires fiber optic attenuator.

continued on next page...

OmniSwitch Port Test Wrap Cable/Plug Requirements (cont.)	
Module Type	Cable Type
CSM-A25-12 CSM-A25-24	ASM/CSM Wrap Plug. Refer to <i>ASM/CSM Wrap Plug – RJ-45 Connector</i> on page 58-40.
CSM-155C-8	ASM/CSM Wrap Plug. Refer to <i>ASM/CSM Wrap Plug – RJ-45 Connector</i> on page 58-40.
CSM-155FM-8	Multi-mode fiber optic wrap plug with SC connectors.
CSM-155FS-8	Single-mode fiber optic cable with SC connectors.
CSM 155FH-8	Single-mode fiber optic cable with SC connectors. Requires fiber optic attenuator.
CSM-622FM-2	Multi-mode fiber optic wrap plug with SC connectors.
CSM-622FS-2	Single-mode fiber optic wrap plug with SC connectors.
CSM-622FH-2	Single-mode fiber optic cable with SC connectors. Requires fiber optic attenuator.
CSM-U/CSM-U+ (CSM-AB-155C-2)	ASM/CSM Wrap Plug. Refer to <i>ASM/CSM Wrap Plug – RJ-45 Connector</i> on page 58-40.
CSM-U/CSM-U+ (CSM-AB-155FM-2)	Multi-mode fiber optic wrap plug with SC connectors.
CSM-U/CSM-U+ (CSM-AB-155FS-2)	Single-mode fiber optic cable with SC connectors.
CSM-U/CSM-U+ (CSM-AB-155FH-2) (CSM-ABT-155FH-2)	Single-mode fiber optic cable with SC connectors. Requires fiber optic attenuator.
CSM-U/CSM-U+ (CSM-AB-E1-4)	T1/E1 Crossover Wrap Cable. Refer to <i>T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
CSM-U/CSM-U+ (CSM-AB-T1-4)	T1/E1 Crossover Wrap Cable. Refer to Figure <i>T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
CSM-U/CSM-U+ (CSM-AB-DS3-2)	RG 59/U Type coaxial cable with BNC connectors.
CSM-U/CSM-U+ (CSM-AB-E3-2)	RG 59/U Type coaxial cable with BNC connectors.

continued on next page...

OmniSwitch Port Test Wrap Cable/Plug Requirements (cont.)	
Module Type	Cable Type
CSM-U/CSM-U+ (CSM-AB-CE-E1)	T1/E1 Crossover Wrap Cable. Refer to <i>T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
CSM-U/CSM-U+ (CSM-AB-CE-T1)	T1/E1 Crossover Wrap Cable. Refer to <i>T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
CSM-U/CSM-U+ (CSM-AB-CM-E1)	T1/E1 Crossover Wrap Cable. Refer to Figure <i>T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39. Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.
CSM-U/CSM-U+ (CSM-AB-CM-T1)	T1/E1 Crossover Wrap Cable. Refer to Figure <i>T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39. Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.
CSM-U/CSM-U+ (CSM-AB-IMA-E1)	T1/E1 Crossover Wrap Cable. Refer to <i>T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
CSM-U/CSM-U+ (CSM-AB-IMA-DS1)	T1/E1 Crossover Wrap Cable. Refer to Figure <i>T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.

continued on next page...

OmniSwitch Port Test Wrap Cable/Plug Requirements (cont.)	
Module Type	Cable Type
ESM-100FM-FD	Multi-mode fiber optic cable with ST connectors.
ESM-100FS-FD	Single-mode fiber optic cable with ST connectors.
ESM-100C-FD	ESM Wrap Plug. Refer to <i>ESM Wrap Plug – RJ-45 Connector</i> on page 58-39.
ESM-100C-4	ESM Wrap Plug. Refer to <i>ESM Wrap Plug – RJ-45 Connector</i> on page 58-39.
ESM-100C-8	ESM Wrap Plug. Refer to <i>ESM Wrap Plug – RJ-45 Connector</i> on page 58-39.
ESM-100C-5	Ethernet Crossover Wrap Cable. Refer to <i>Ethernet Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
ESM-100CFM-5 (Multi-mode fiber port)	Multi-mode fiber optic cable with ST connectors.
ESM-100CFS-5 (Single-mode fiber port)	Single-mode fiber optic cable with ST connectors.
ESM-100CFx-5 (copper ports)	Ethernet Crossover Wrap Cable. Refer to <i>Ethernet Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.

continued on next page...

OmniSwitch Port Test Wrap Cable/Plug Requirements (cont.)	
Module Type	Cable Type
ESM-C-8	Ethernet Crossover Wrap Cable. Refer to <i>Ethernet Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
ESM-C-12	Ethernet Crossover Wrap Cable. Refer to <i>Ethernet Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
ESM-F-8	Multi-mode fiber optic wrap plug with ST connectors.
ESM-T-12	Port/Stress (Full Duplex) test: Telco Full Duplex Wrap Cable. Refer to <i>Telco (Full Duplex) Wrap Plug – 50-pin RJ-21 Connector</i> on page 58-42 Port/Stress (Half Duplex) test: Telco Half Duplex Wrap Cable. Refer to <i>Telco (Half Duplex) Wrap Plug – 50-pin RJ-21 Connector</i> on page 58-41.
ESM-U (AB-AFD)	AUI to 10BaseFL full-duplex transceiver and a multi-mode fiber optic cable with ST connectors.
ESM-U (AB-AT)	AUI to 10BaseT transceiver and Ethernet Crossover Wrap Cable. Refer to <i>Ethernet Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
ESM-U (AB-T)	Ethernet Crossover Wrap Cable. Refer to <i>Ethernet Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
ESM-U (AB-B)	RG 59/U Type coaxial cable with BNC connectors.
ESM-U (AB-FL)	Multi-mode fiber optic cable with ST connectors.
ESM-U (AB-FL-S)	Single-mode fiber optic cable with ST connectors.

continued on next page...

OmniSwitch Port Test Wrap Cable/Plug Requirements (cont.)	
Module Type	Cable Type
ESM-C-16	ESM Wrap Plug. Refer to <i>ESM Wrap Plug – RJ-45 Connector</i> on page 58-39.
ESM-C-32	Ethernet Crossover Wrap Cable. Refer to <i>Ethernet Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
ESM-FM-16W	Multi-mode fiber optic wrap plug with ST connectors.
ESM-100C-12	ESM Wrap Plug. Refer to <i>ESM Wrap Plug – RJ-45 Connector</i> on page 58-39. Ethernet Crossover Wrap Cable. Refer to <i>Ethernet Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
ESM-100FM-8	Multi-mode fiber optic wrap plug with SC connectors.
ESM-T-24W	Port/Stress (Full Duplex) test: Telco Full Duplex Wrap Cable. Refer to <i>Telco (Full Duplex) Wrap Plug – 50-pin RJ-21 Connector</i> on page 58-42 Port Stress (Half Duplex) test: Telco Half Duplex Wrap Cable. Refer to <i>Telco (Half Duplex) Wrap Plug – 50-pin RJ-21 Connector</i> on page 58-41.
ESM-100C-32W	Port/Stress (Full Duplex) test: ESM Wrap Plug. Refer to <i>ESM Wrap Plug – RJ45 Connector</i> . Port/Stress (Half Duplex) test: Ethernet Crossover Wrap Cable. Refer to <i>Ethernet Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
GSM-FM-2W	Port/Stress (Full Duplex) test: Multi-mode fiber optic wrap plug with SC connectors. Port/Stress (Half Duplex) test: Multi-mode fiber optic cable with SC connectors.
GSM-FS-2W	Port (Full and Half Duplex) and Stress tests: Single-mode fiber optic cable with SC connectors.

continued on next page...

OmniSwitch Port Test Wrap Cable/Plug Requirements (cont.)	
Module Type	Cable Type
FCSM I	No cables or wrap plugs required.
FCSM II	No cables or wrap plugs required.
TSM-F-6	Multi-mode fiber optic cable with ST connectors.
TSM-C-6	Token Ring Straight Through Wrap Cable. Refer to <i>Token Ring Straight Through Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-40. (A Multistation Access Unit (MAU) is required to perform the port test in on this module.)
TSM-CD-6	Token Ring Straight Through Wrap Cable. Refer to <i>Token Ring Straight Through Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-40.
TSM-CD-16W	Token Ring Straight Through Wrap Cable. Refer to <i>Token Ring Straight Through Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-40.

continued on next page...

OmniSwitch Port Test Wrap Cable/Plug Requirements (cont.)	
Module Type	Cable Type
WSM-S-2 (no compression)	Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.
WSM-SC-4 WSM-SC-4W WSM-SC-8 WSM-SC-8W	Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.
WSM-BRI-SC	BRI S/T Crossover Wrap Cable. Refer to <i>BRI S/T Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-48 (RJ-45) Connectors</i> on page 58-42. Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.
WSM-FE1-SC-2	T1/E1 Crossover Wrap Cable. Refer to <i>T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39. Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.
WSM-FT1-SC-2	T1/E1 Crossover Wrap Cable. Refer to Figure <i>T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39. Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.

The table below provides specific cable/plug information for Omni Switch/Router switching modules.

Omni Switch/Router Port Test Wrap Cable/Plug Requirements	
Module Type	Cable Type
GSX-FM-2W GSX-FM-4W	Port/Stress (Full Duplex) test: Multi-mode fiber optic wrap plug with SC connectors. Port/Stress (Half Duplex) test: Multi-mode fiber optic cable with SC connectors.
GSX-FS-2W GSX-FS-4W	Port (Full and Half Duplex) and Stress tests: Single-mode fiber optic cable with SC connectors.
GSX-FH-2W GSX-FH-4W	Port (Full and Half Duplex) and Stress tests: Single-mode fiber optic cable with SC connectors.
GSX-K-FM-2W	Port/Stress (Full Duplex) test: Multi-mode fiber optic wrap plug with SC connectors. Port/Stress (Half Duplex) test: Multi-mode fiber optic cable with SC connectors.
GSX-K-FS-2W	Port (Full and Half Duplex) and Stress tests: Single-mode fiber optic cable with SC connectors.
ESX-100C-12W	Port Stress (Full Duplex) test: ESM Wrap Plug. Refer to <i>ESM Wrap Plug – RJ-45 Connector</i> on page 58-39. Port Stress (Half Duplex) test: Ethernet Crossover Wrap Cable Refer to <i>Ethernet Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
ESX-100C-32W	Port/Stress (Full Duplex) test: ESM Wrap Plug. Refer to <i>ESM Wrap Plug – RJ-45 Connector</i> on page 58-39. Port/Stress (Half Duplex) test: Ethernet Crossover Wrap Cable Refer to <i>Ethernet Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.
ESX-K-100C-32W	Port/Stress (Full Duplex) test: ESM Wrap Plug. Refer to <i>ESM Wrap Plug – RJ-45 Connector</i> on page 58-39. Port/Stress (Half Duplex) test: Ethernet Crossover Wrap Cable Refer to <i>Ethernet Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39.

continued on next page...

Omni Switch/Router Port Test Wrap Cable/Plug Requirements (cont.)	
Module Type	Cable Type
ESX-100FM-12W	<p>Port/Stress (Full Duplex) test: Multi-mode fiber optic wrap plug with MT-RJ connectors.</p> <p>Port/Stress (Half Duplex) test: Multi-mode fiber optic cable with MT-RJ connectors.</p>
ESX-100FS-12W	<p>Port/Stress (Full Duplex) test: Single mode fiber optic wrap plug with MT-RJ connectors.</p> <p>Port/Stress (Half Duplex) test: Single mode fiber optic cable with MT-RJ connectors.</p>
ESX-K-100FM-16W	<p>Port/Stress (Full Duplex) test: Multi-mode fiber optic wrap plug with MT-RJ connectors.</p> <p>Port/Stress (Half Duplex) test: Multi-mode fiber optic cable with MT-RJ connectors.</p>
ESX-K-100FS-16W	<p>Port/Stress (Full Duplex) test: Single mode fiber optic wrap plug with MT-RJ connectors.</p> <p>Port/Stress (Half Duplex) test: Single mode fiber optic cable with MT-RJ connectors.</p>
ESX-FM-24W	<p>Port/Stress (Full Duplex) test: Multi-mode fiber optic wrap plug with VF-45 connectors.</p> <p>Port/Stress (Half Duplex) test: Multi-mode fiber optic cable with VF-45 connectors.</p>

continued on next page...

Omni Switch/Router Port Test Wrap Cable/Plug Requirements (cont.)	
Module Type	Cable Type
ASX-155FM	Port test: Multi-mode fiber optic wrap plug with SC connectors.
ASX-155FS	Port test: Single-mode fiber optic cable with SC connectors.
ASX-155FH	Port test: Single-mode fiber optic cable with SC connectors. Requires fiber optic attenuator.
ASX-155RFM	Port test: Multi-mode fiber optic wrap plug with SC connectors.
ASX-155RFS	Port test: Single-mode fiber optic cable with SC connectors.
ASX-622RFS-1W	Port test: Single-mode fiber optic cable with SC connectors.
ASX-622RFM-1W	Port test: Multi-mode fiber optic wrap plug with SC connectors.
ASX-M-622RFS-1W	Port test: Single-mode fiber optic cable with SC connectors.
ASX-M-622RFM-1W	Port test: Multi-mode fiber optic wrap plug with SC connectors.
ASX-M-622RFH-1W	Port test: Single-mode fiber optic cable with SC connectors. Requires fiber optic attenuator.
ASX-DS3	RG 59/U Type coaxial cable with BNC connectors.
ASX-E3	RG 59/U Type coaxial cable with BNC connectors.
TSX-CD-16W	Token Ring Straight Through Wrap Cable. Refer to <i>Token Ring Straight Through Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-40.
TSX-C-32W	Token Ring Straight Through Wrap Cable. Refer to <i>Token Ring Straight Through Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-40.

continued on next page...

Omni Switch/Router Port Test Wrap Cable/Plug Requirements (cont.)	
Module Type	Cable Type
WSX-S-2W (no compression)	Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.
WSX-SC-4W	Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.
WSX-SC-8W	Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.
WSX-BRI-SC-2W	BRI S/T Crossover Wrap Cable. Refer to <i>BRI S/T Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-48 (RJ-45) Connectors</i> on page 58-42. Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.
WSX-FE1-SC-2W	T1/E1 Crossover Wrap Cable. Refer to <i>T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39. Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.
WSX-FT1-SC-2W	T1/E1 Crossover Wrap Cable. Refer to <i>Figure T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors</i> on page 58-39. Twisted pair 28GA serial cable with HD50-26 connectors – DCE to DTE.
WSX-M013-2W WSX-M013-4W	RG 59/U Type coaxial cable with BNC connectors.
VSD-128M-12CH VSD-128M-24CH VSD-128M-36CH VSD-128M-48CH VSD-128M-60CH VSA-FXO VSA-FXS VSA-4	No Cable Required.

Sample Test Session: Ethernet Module

Test sessions and results will vary among the various switching modules. This section shows the output from a test session on an ESM-C-12. The module is in slot 3 and all tests were requested to be run one time. The command to start this test is:

test 3

After you enter the **test** command line, the following displays:

**Port Tests are available for the selected slot(s).
These tests require external cabling.**

Do you wish to run the Port Tests (y/n) (y)

Enter **y** to run port tests or **n** to skip them. If you select to run the port tests, you will be instructed on how to cable the ports. This cabling will vary depending on the test configuration, module type, number of ports and cable type. In this example, the following displays:

Connect the following cables on Slot 3:
Port 1 to Port 2
Port 3 to Port 4
Port 5 to Port 6
Port 7 to Port 8
Port 9 to Port 10
Port 11 to Port 12

Press <Enter> when finished.

Cable the ports according to the instructions. For Ethernet tests, you should use cross-over cable to connect the ports. Press **<Enter>** when you have finished the cabling.

The module is reset, and then the rest of the tests will run.

Testing Slot 3 - Ether/12
 Resetting slot 3...
 Test In Progress: CSR Test
 OK1, OK2 LEDS will display the following pattern: OFF RED OFF GREEN OFF
 AMBER OFF - Passed
 Test In Progress: VRAM Test - Passed
 Test In Progress: CAMOFFBRD Test(1K) - Passed
 Loading dni.img...
 Test In Progress: BOARDUP Test - Passed
 Test In Progress: CAMONBRD Test(1K) - Passed
 Test In Progress: VBUS Test - Passed
 Restoring slot 3...
 Test In Progress: PORT Test (3-0)
 Wait for ports to come up . Done.
 Error - Frame #1 not found - Failed
 FAILED - PORT TEST: Tx Port1 -> Rx Port2 at Test Number 95001
 Expected Data: 1
 Measured Data: 0

Test Summation:

Started: WED DEC 17 10:48:13 2000

Slot 3	Passes	Fails
Ether/12 (3-0)		
CSR	1	0
VRAM	1	0
CAMOFFBRD	1	0
BOARDUP	1	0
CAMONBRD	1	0
VBUS	1	0
PORT	0	1

Failure Summation:

Ether/12 (3-0)

Test	Fail No.	Test No.	Exp. Data	Meas. Data	Iter. No.	Time	Temp (C)
PORT	1	95001	00000001	00000000	1	10:49:47	30.5

Completed: WED DEC 17 10:49:47 2000

Disconnect the following cables on Slot 3:

- Port 1 to Port 2
- Port 3 to Port 4
- Port 5 to Port 6
- Port 7 to Port 8
- Port 9 to Port 10
- Port 11 to Port 12

Press <Enter> when finished.

The tests are complete at this point. A summary of the test results and failures is displayed at the end of the test sequence. In this example, the module passed all tests except the port test. The ESM-C-12 module in slot 3 should have a red OK2 LED to indicate diagnostics failure. And the **Failure Summation** section displays only the first three failures when you request multiple test iterations.

You should now disconnect the cables used in the external loopback tests. Press **<Enter>** and the module will be restored to its normal, pre-testing state. The OK2 LED will remain red until the module is reset or the chassis is rebooted.

The main system command prompt re-displays.

Displaying Available Diagnostic Tests

The **testdisp** command provides the user with a display of applicable tests for a particular slot or for the entire chassis configuration. To display available diagnostic tests for a switching module, enter the **testdisp** command followed by the slot number for the module. The slot number is an integer ranging from 1 to the number of slots in the chassis (3 for 3-slot OmniSwitches; 5 for 5-slot OmniSwitches and 9 for 9-slot OmniSwitches).

No default value is set and input must be provided at the time of entering the command. For example, to display available diagnostic tests for the switching module in slot 3, enter:

```
testdisp 3
```

at the system prompt. The following is a sample display.

```
Ether/12 (3-0)  
  CSR - Tests the Command/Status Registers  
  VRAM - Tests the VRAM  
  CAMOFFBRD - Tests the CAM  
  BOARDUP - Basic NI Tests  
  CAMONBRD - Tests the CAM  
  VBUS - Tests the VSE/SAM  
  PORT - Tests the Ports
```

To display all available diagnostic tests for the entire chassis, excluding slot(s) occupied by an MPM without an HRE, enter:

```
testdisp all
```

at the system prompt. The tests are displayed per slot module starting from slot module 1.

Configuring the Diagnostic Test Environment

The **testcfg** command allows the user to tailor diagnostic testing characteristics per slot module. To configure diagnostic tests for a switching module, enter the **testcfg** command followed by the slot number for the module. The slot number is an integer ranging from 1 to the number of slots in the chassis (3 for 3-slot OmniSwitches; 5 for 5-slot OmniSwitches and 9 for 9-slot OmniSwitches).

The **testcfg** command allows the user to bypass testing individual slots when running the **test all** command. In addition, the **testcfg** command allows the user to configure the port speed and port mode for applicable Ethernet or Token Ring modules for tailoring of individual slots during diagnostic testing.

No default value is set and input must be provided at the time of entering the command. For example, to configure applicable diagnostic tests for the switching module in slot 4, enter:

```
testcfg 4
```

at the system prompt. The following is a typical example for an ATM switching module.

```
Test Configuration for slot 4
```

```
1) Skip this slot during test { No (1),  
                               Yes (2) } : No
```

```
Enter (option=value/save/cancel) :
```

Note that for all switching modules other than Ethernet and Token Ring modules, the **Skip this slot during test** option is the only available one. See *Configuring Tests for Ethernet Modules* on page 58-31 for information on using the **testcfg** command with Ethernet modules, and *Configuring Tests for Token Ring Modules* on page 58-32 for information on using the **testcfg** command with Token Ring modules.

Skip this slot during test. Allows the user to select to bypass this slot when the **test all** command is issued. The default is **No**. If you want the **test all** command to skip this module, enter

```
1=2
```

The following will then be displayed.

```
Test Configuration for slot 4
```

```
1) Skip this slot during test { No (1),  
                               Yes (2) } : Yes
```

```
Enter (option=value/save/cancel) :
```

Enter **save** if you want to make this change. If you enter **save**, the change will be made and the following will be displayed.

```
Configuration Saved
```

If you want to cancel this change, enter **cancel** and the **testcfg** command will terminate and the following will be displayed.

```
Exiting menu - Test Configuration not modified
```

Configuring Tests for Ethernet Modules

Tailoring of applicable Ethernet modules includes selection of Port Speeds and of Port Modes. To configure applicable diagnostic tests for an Ethernet 10/100 switching module in slot 3, enter:

```
testcfg 3
```

The following is a sample display of the test configuration for an Ethernet 10/100 switching module.

Test Configuration for slot 3

```
1) Skip this slot during test { No (1),
                               Yes (2) } : No
2) Port Speed { 10/100 (1),
                100   (2),
                10    (3) }           : 10/100
3) Port Mode { Full Duplex (1),
              Half Duplex (2) }       : Full Duplex
Enter (option=value/save/cancel)    :
```

To change any of the values above, enter the line number, followed by an equal sign, and followed by the new value. For example, to change the **Port Mode** field to half duplex, enter

```
3=2
```

The configurable fields displayed by the **testcfg** command for an Ethernet module are described below.

Skip this slot during test. Allows the user to select to bypass this slot when the **test all** command is issued. The default is **No**.

Port Speed. Allows the user to select module port speed during the diagnostic port test. Selection includes 10/100BaseT, 100BaseT, or 10BaseT. The default is **10/100BaseT**, which alternates the speed of the port test from 10 to 100 on each pass of the port test.

Port Mode. Allows the user to select module port mode during diagnostic port test. Selection includes Full Duplex or Half Duplex. The default value is **Full Duplex**.

Enter **save** if you want to make this change. If you want to cancel this change, enter **cancel** and the **testcfg** command will terminate.

Configuring Tests for Token Ring Modules

Token Ring configuration tailoring includes selection of Port Speeds and of Port Modes. To configure applicable diagnostic tests for a TSM-CD-6 switching module in slot 4, enter:

```
testcfg 4
```

The following is a sample display of the test configuration for a TSM-CD-6 slot module.

Test Configuration for slot 4

```
1) Skip this slot during test { No (1),  
                               Yes (2) } : No  
2) Port Speed { 4/16 (1),  
                16 (2),  
                4 (3) } : 16  
3) Port Mode { Stn/Lobe, Lobe/Stn (1),  
               Stn/Lobe Only (2),  
               Lobe/Stn Only (3) } : Stn/Lobe  
  
Enter (option=value/save/cancel) :
```

To change any of the values above, enter the line number, followed by an equal sign, and followed by the new value. For example, to change the **Port Speed** field to 16Mbps, enter

```
2=2
```

The configurable fields displayed by the **testcfg** command for a Token Ring module are described below.

Skip this slot during test. Allows the user to select to bypass this slot when the **test all** command is issued. The default is **No**.

Port Speed. Allows the user to select module port speed during the diagnostic port test. Selection includes 4/16Mbps, 16Mbps, or 4Mbps. The default is **16Mbps**. Selecting **4/16** alternates the speed of the port test between 4 to 16 on each pass of the port test.

Port Mode. Allows the user to select module port mode during the diagnostic port test. Selection includes Stn/Lobe, Lobe/Stn, or Stn/Lobe Only, or Lobe/Stn Only. The default value is **Stn/Lobe**. **Stn/Lobe, Lobe/Stn** alternates each physical port pair between station to lobe and lobe to station on each speed selected for pass of the port test.

Enter **save** if you want to make this change. If you want to cancel this change, enter **cancel** and the **testcfg** command will terminate.

Running Cell Fabric Tests on OmniSwitch CSMs

You can test the OmniSwitch cell bus backplane and the cell fabric ASIC of every switching module with the **cellfab** command. The syntax for this command is as follows:

```
cellfab [<repeat_count>]
```

The **<repeat_count>** option lets you set the number of times to run the test, which can be from 0 to 999. If you enter **0**, the **cellfab** test will continue indefinitely. If you do not use the **<repeat_count>** option, then the **cellfab** test will be executed once.

The chassis should be fully loaded to achieve a thorough testing of both the cell fabric ASICs and cell bus. In addition, the chassis should be configured as a “pure” ATM switch with an MPM II, MPM III or MPM 1G, a Frame to Cell Switching Module (FCSM), Cell Switching Modules (CSMs), and *no* frame-based switching modules. See Chapter 40, “Cell Switching Modules, (CSMs)” for more information on configuring an OmniSwitch as a pure ATM switch.

To execute the **cellfab** test once, for example, enter

```
cellfab
```

at the system prompt. A screen similar to the following will be displayed.

```
Avoiding ARP delay ...  
Testing All Slots  
Test In Progress: FABRIC Test - Passed
```

```
Test Summation:
```

```
Started: WED OCT 28 17:38:59 2000
```

All Slots	Passes	Fails
FABRIC	1	0

```
Test Coverage:
```

```
All Fabric Inputs/Outputs not tested:
```

```
Fabric in slot 2 (FCSM) has 33 inputs (0-32) and 1 output (0)  
Input 0 2 3 4  
All Outputs tested
```

```
Fabric in slot 3 (CSM-OC12) has 33 inputs (0-32) and 4 outputs (0-3)  
Input 0 2 3 4  
All Outputs tested
```

```
Fabric in slot 4 (CSM-OC12) has 33 inputs (0-32) and 4 outputs (0-3)  
Input 0 2 3 4  
All Outputs tested
```

—Output continues on next page —

Fabric in slot 5 (CSM-OC12) has 33 inputs (0-32) and 4 outputs (0-3)
Input 0 2 3 4
All Outputs tested

Fabric in slot 6 (CSM-OC12) has 33 inputs (0-32) and 4 outputs (0-3)
Input 0 2 3 4
All Outputs tested

Fabric in slot 7 (CSM-OC12) has 33 inputs (0-32) and 4 outputs (0-3)
Input 0 2 3 4
All Outputs tested

Fabric in slot 8 (CSM-OC12) has 33 inputs (0-32) and 4 outputs (0-3)
Input 0 2 3 4
All Outputs tested

Fabric in slot 9 (CSM-OC12) has 33 inputs (0-32) and 4 outputs (0-3)
Input 0 2 3 4
All Outputs tested

Completed: WED OCT 28 17:39:45 2000

If you need to halt the **cellfab** test, press **CTRL-C**. This key sequence pauses the testing and provides a test summary report. You will be prompted to restart the testing after the pause.

◆ **Note** ◆

During certain phases of diagnostic testing, the **CTRL-C** will not be immediately processed. This delay may last several seconds, or longer.

Running Frame Fabric Tests on Omni Switch/Routers

You can test the Omni Switch/Router Multi VBUS (MVBUS) backplane and the frame fabric ASIC of every switching module with the **framefab** command. The syntax for this command is as follows:

```
framefab [<repeat_count> | ilb <repeat_count>]
```

The **<repeat_count>** option lets you set the number of times to run the test, which can be from 0 to 999. If you enter **0**, the **framefab** test will continue indefinitely. If you do not use the **<repeat_count>** option, then the **framefab** test will be executed once.

Using the **<repeat_count>** option requires the use of external cables or wrap plugs for the first physical port of every switching module in the chassis. The external cables or wrap plugs used in this test are identical to the one listed in the full duplex port test. See *Omni Switch/Router Port Test Wrap Cable/Plug Requirements* on page 58-22 for more information.

The **ilb** option, which can be used with the **<repeat_count>** option, performs an internal loop-back. Using this option performs the **framefab** test without the use of external cables or wrap plugs.

The chassis should be fully loaded (i.e., Omni Switch/Router modules in all slots) to achieve a thorough testing of both the frame fabric ASICs and the Omni Switch/Router backplane. In addition, an MPX should be installed in Slot 1.

To execute the framefab test indefinitely, for example, enter

```
framefab 0
```

at the system prompt. A screen similar to the following will be displayed.

```
Testing All Slots  
Test In Progress: FABRIC Test
```

```
Test Summation:
```

```
Started: TUE OCT 27 18:40:31 2000
```

All Slots	Passes	Fails
FABRIC	1199	18

```
Failure Summation:
```

Test	Fail No.	Test No.	Exp. Data	Meas. Data	Iter. No.	Time	Temp (C)
FABRIC	1	110402	00004cec	00000000	6	18:50:34	43.0
FABRIC	2	110504	0000a9e4	00000000	13	18:56:45	43.0
FABRIC	3	110307	0008a6ff	00000000	159	21:26:05	43.0

```
First 3 Failure(s) Detail:
```

```
Fail No. 1 - FRAME FABRIC TEST: Slot 5 failed. No packet Received from slot: 3  
Fail No. 2 - FRAME FABRIC TEST: Slot 6 failed. No packet Received from slot: 5  
Fail No. 3 - FRAME FABRIC TEST: Slot 4 failed. No packet Received from slot: 8
```

— Output continues on next page —

Test Coverage:

All Fabric Inputs/Outputs not tested:

Fabric in slot 2 (ESX-C12) has 9 inputs (0-8) and 1 output (0)
All inputs tested
All Outputs tested

Fabric in slot 3 (ESX-C12) has 9 inputs (0-8) and 1 output (0)
All inputs tested
All Outputs tested

Fabric in slot 4 (ESX-C12) has 9 inputs (0-8) and 1 output (0)
All inputs tested
All Outputs tested

Fabric in slot 5 (ESX-C12) has 9 inputs (0-8) and 1 output (0)
All inputs tested
All Outputs tested

Fabric in slot 6 (ESX-C12) has 9 inputs (0-8) and 1 output (0)
All inputs tested
All Outputs tested

Fabric in slot 7 (ESX-C12) has 9 inputs (0-8) and 1 output (0)
All inputs tested
All Outputs tested

Fabric in slot 8 (ESX-C12) has 9 inputs (0-8) and 1 output (0)
All inputs tested
All Outputs tested

Fabric in slot 9 (ESX-C32) has 9 inputs (0-8) and 1 output (0)
All inputs tested
All Outputs tested

Completed: WED OCT 28 16:24:04 2000

If you need to halt the **framefab** tests, press **CTRL-C**. This key sequence pauses the testing and provides a test summary report. You will be prompted to restart the testing after the pause.

◆ Note ◆

During certain phases of diagnostic testing, the **CTRL-C** will not be immediately processed. This delay may last several seconds, or longer.

If your chassis is not fully loaded, the **framefab** test will report that the frame fabric in the empty slot was not tested.

Running Diagnostics on an Entire Chassis

The **testcfg** command allows you to tailor diagnostic testing characteristics by module or for an entire chassis. (Please refer to *Configuring the Diagnostic Test Environment* on page 58-30 for configuring tests for a single module.)

For example, to configure diagnostic tests for an entire chassis, enter:

```
testcfg all
```

A screen similar to the following will be displayed.

```

Test Configuration

1) Diagnostic Mode { Normal          (1),
                  { Diagnostic       (2) } : Normal
2) Stop on Failure { Disable        (1),
                  { Enable          (2) } : Disable
3) Port Test Bypass { Disable       (1),
                   { Enable        (2) } : Disable
4) Port Test Type  { Port           (1),
                   { ILB           (2),
                   { STRESS        (3),
                   { ILBSTRESS     (4) } : Port
5) HRE-X Test Mode { Do not test HRE-X (1),
                  { Test HRE-X      (2) } : Test HRE-X

Enter (option=value/save/cancel) :
```

◆ Note ◆

Option 5, **HRE-X Test Mode**, does not display on the OmniSwitch.

Select the number of the item you want to change. To change any of the values listed above, enter the line number, followed by an equal sign, and then the new value. For example, to change the port test type to **STRESS**, enter:

```
4=3
```

To update the values you have changed, enter **save**. If you do not want to save the changes enter **quit** or **cancel**, or press **Ctrl-D**. If you enter **save**, the change will be made and the following message will be displayed.

```
Configuration Saved
```

If you cancel the **testcfg** command, it will terminate and the following will be displayed.

```
Exiting menu - Test Configuration not modified
```

The fields displayed by the **testcfg** command with the **all** option are described below.

1) Diagnostic Mode

Enter **1** (the default) to set to normal diagnostics testing or **2** for a more detailed version of diagnostic testing. However, setting this field to **2** requires more user intervention during a test.

2) Stop on Failure

Enter **2** to halt diagnostics in an active state when a failure occurs or **1** (the default) to exit diagnostics and display the **Test Summation** and **Failure Summation** sections of the **test** command output. Setting this field to **2** can be used to further troubleshoot problems. However, setting this field to **2** requires more user intervention during a test.

3) Port Test Bypass

Enter **2** to complete testing of all ports regardless of port test failures or **1** (the default) to stop testing at the first port failure. Setting this field to **2** can be used to further troubleshoot problems.

4) Port Test Type

Enter **1** (the default) for a port test, **2** for an Internal Loopback (ILB) test, **3** for a stress test, or **4** for an ILB stress test. External cables are required for the port and stress tests but not for the ILB test. In addition, the stress test requires a special image file (see *Running Diagnostics* on page 58-3) and is only available for Cell Switching Modules (CSMs) and Mammoth-based Ethernet switching modules on the OmniSwitch, and Ethernet (ESX and GSX) modules on the Omni Switch/Router.

◆ Note ◆

Option 5, **HRE-X Test Mode**, is for the Omni Switch/Router only.

5) HRE-X Test Mode

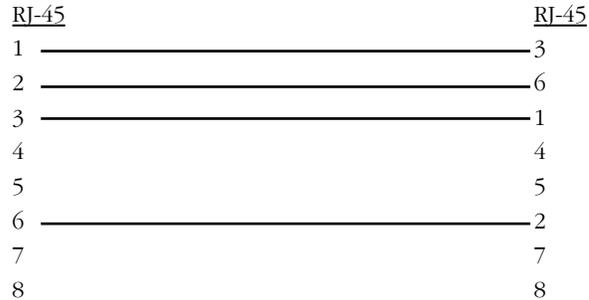
This option lets you configure port tests for HRE-Xs installed on Omni Switch/Router switching modules. It does not affect the port test for HRE-Xs installed on MPXs. Currently, the port test on HRE-Xs installed on switching modules runs in conjunction with the normal port test.

Each physical port is tested with the normal port test path and then through the HRE-X port test path before testing the next physical port. Subsequent physical ports are tested with only the normal port test path.

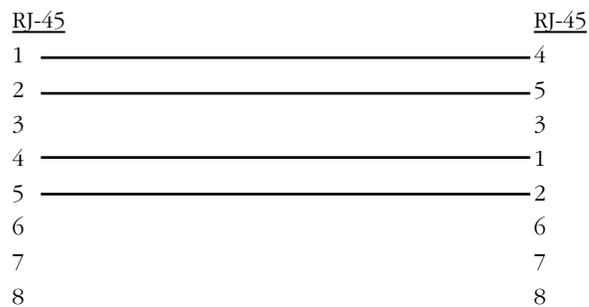
Enter **1** to bypass testing of the HRE-X when the port test is run or **2** to perform the test as described above.

Diagnostic Test Cable Schematics

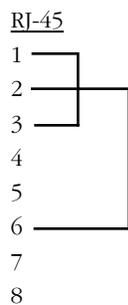
The figures below and on the following pages provide information on port test cables and plugs.



Ethernet Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors

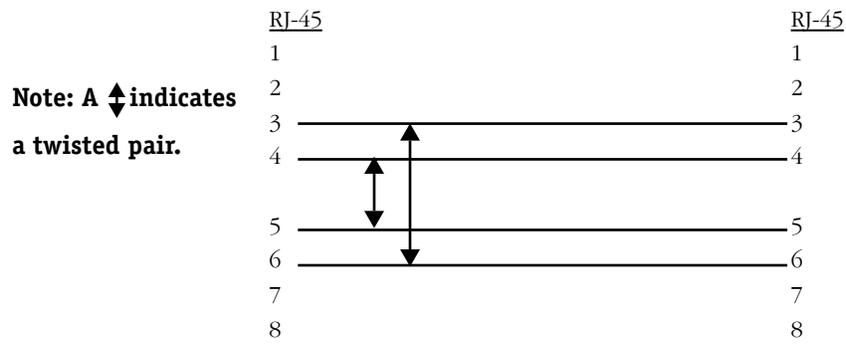


T1/E1 Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors

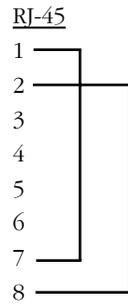


ESM Wrap Plug – RJ-45 Connector

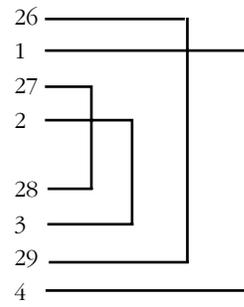
Diagnostic Test Cable Schematics



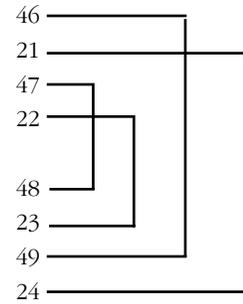
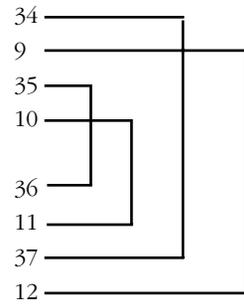
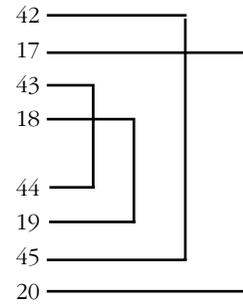
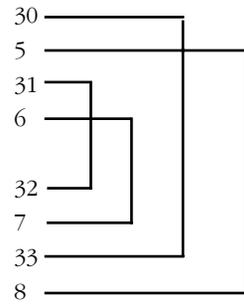
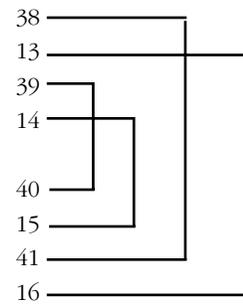
Token Ring Straight Through Wrap Cable — Category 5 UTP Copper Cable with RJ-45 Connectors



ASM/CSM Wrap Plug – RJ-45 Connector

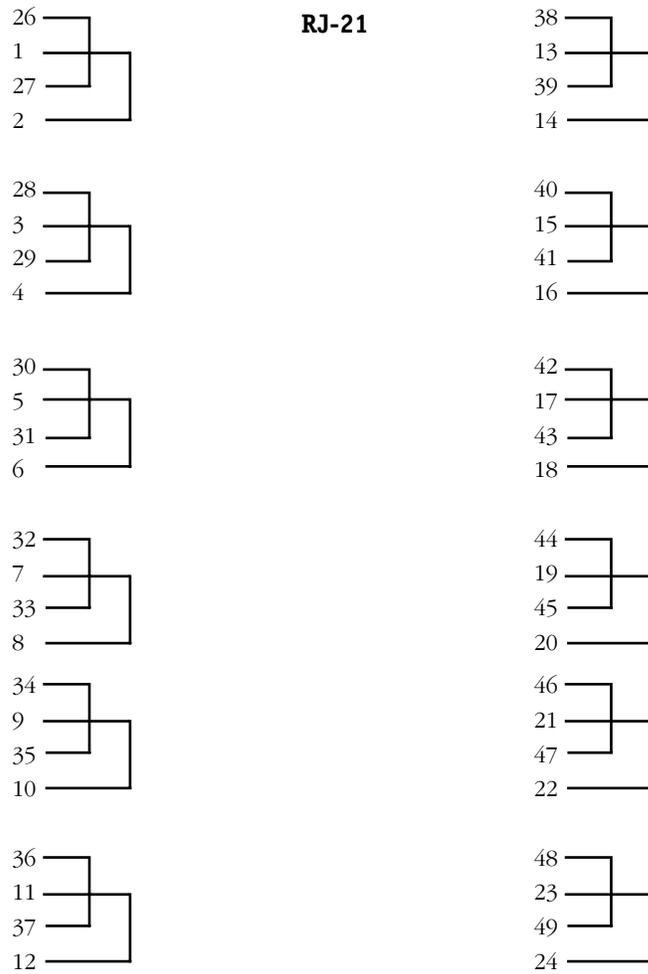


RJ-21

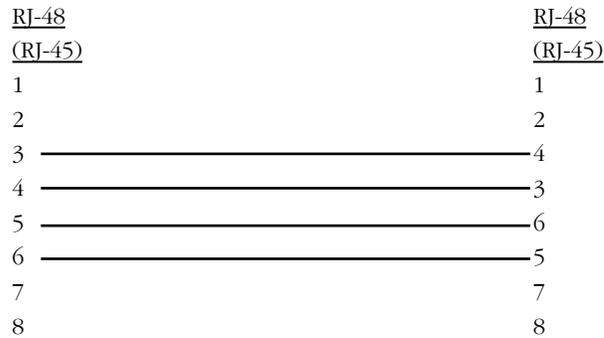


Telco (Half Duplex) Wrap Plug – 50-pin RJ-21 Connector

Diagnostic Test Cable Schematics



Telco (Full Duplex) Wrap Plug – 50-pin RJ-21 Connector



BRI S/T Crossover Wrap Cable — Category 5 UTP Copper Cable with RJ-48 (RJ-45) Connectors

A The Boot Line Prompt

When the switch boots, it requires basic information so that it can configure itself. The switch is delivered with factory default configuration parameters that provide basic information; however, you can change or customize the configuration parameters using the Boot Line prompt. You can only access the Boot Line configuration through an ASCII terminal.

Customizing parameters can be helpful when troubleshooting your system. Changing configuration items in the boot process allows you to:

- Stop the boot process
- Boot from a SLIP device
- Boot from a ZMODEM connection
- Revert back to factory default settings
- Boot/load with a different set of parameters

In addition, you can use the Boot prompt to configure an IP address for the Ethernet management port (MPX, MPM-C, and MPM-III only) or you can use the **ethernetc** command (which is described in Chapter 10, “Configuring Management Processor Modules”). You can use the Ethernet management port to Telnet into the UI, perform high-speed software loads, or as a connection to a boot device. See *Configuring a Switch with an MPX/MPM-C/MPM-III* on page A-7 for more information on configuring the Ethernet management port with the Boot prompt.

To enter the Boot line prompt, see the section that follows. See *Boot Prompt Basics* on page A-3 for documentation on basic Boot prompt commands. If you are configuring an Omni Switch/Router or an OmniSwitch with an MPM-C or MPM-III, see *Configuring a Switch with an MPX/MPM-C/MPM-III* on page A-7. If you are configuring an OmniSwitch with an MPM-1G, MPM-II, or an original MPM, see *Configuring a Switch with an MPM/MPM-II/MPM-1G* on page A-10.

◆ Important Note ◆

In Release 4.4 and later, both the OmniSwitch and Omni Switch/Router are factory-configured to boot up in CLI (Command Line Interface) mode, rather than in UI (User Interface) mode. Chapter 8, “The User Interface,” includes documentation on changing from CLI mode to UI mode.

Entering the Boot Prompt

Perform the following steps to reach the Boot prompt.

1. Connect an ASCII terminal (or computer with a terminal emulator) to the console port on the MPX (Omni Switch/Router) or on the MPM (OmniSwitch). The default communication parameters are:
 - 9600 bps
 - 8 data bits
 - 1 stop bit
 - no parity
 - no hardware flow control (Windows 95 and later)
2. Turn on the switch.
3. You should see text scrolling on the terminal, indicating that the boot is starting. If you do not see any text within a few seconds of turning on the switch press the **<Enter>** key. If you still do not see any text on the screen, verify your connections, turn off the switch, and turn it back on again.
4. Once the boot process starts you have approximately two (2) seconds to interrupt the boot. Press any key during this time to enter the Boot prompt.

◆ Note ◆

MPXs or MPMs in redundant configurations should not be stopped during the boot process. If you must do this, remove one of the MPXs (or MPMs) while configuring the other.

The following screen prompt displays.

[Boot]:

See the following section for documentation on basic Boot prompt commands. If you are configuring an Omni Switch/Router or an OmniSwitch with an MPM-C or MPM-III, see *Configuring a Switch with an MPX/MPM-C/MPM-III* on page A-7. If you are configuring an OmniSwitch with an MPM-1G, MPM-II, or an original MPM, see *Configuring a Switch with an MPM/MPM-II/MPM-1G* on page A-10.

Boot Prompt Basics

To get a list of commands enter a question mark (?). A screen similar to the following is shown:

```

?                - print this list
@                - boot (load and go)
p                - print boot params
c                - change boot params
l                - load boot file
g adrs           - go to adrs
d adrs[,n]       - display memory
m adrs           - modify memory
f adrs, nbytes, value - fill memory
t adrs, adrs, nbytes - copy memory
e                - print fatal exception
n netif          - print network interface device address
L                - list ffs files
P                - Purge system: removes ALL ffs files
R file [files]   - remove ffs file(s)
S                - save boot configuration
V                - display bootstrap version
$dev(0,procnum)host:/file h=# e=# b=# g=# u=usr [pw=password] f=#
                 tn=targetname s=script o=other

Boot flags:
0x02            - load local system symbols
0x04            - don't autoboot
0x08            - quick autoboot (no countdown)
0x20            - disable login security
0x40            - use bootp to get boot parameters
0x80            - use tftp to get boot image
0x100          - use proxy arp
0x1000         - factory reset

available boot devices: sl ffs zm
[Boot]:

```

This menu is the same for both the OmniSwitch and the Omni Switch/Router. The commands for this menu are described in the sections below.

◆ Important Note ◆

The Boot prompt is case sensitive. Always enter letters in lowercase or uppercase as indicated in the menus.

Resuming Switch Boot (@)

If you wish to continue the boot process, enter the @ command at the prompt. This loads the last saved configuration.

Displaying Current Configuration (p)

To display the current configuration, enter a **p** at the Boot prompt. A screen similar to the following will be displayed.

```
Boot device           : ffs
Boot file             : /flash/mpm3.img
Eth IP addr[:mask]   : 192.168.11.1
Startup script       : /flash/mpm3.cmd
Console params       : 9600,n81c
Modem params         : 9600,n81
Boot flags           : 0xb
Other                 : dvip:no-name,192.168.10.1,255.255.255.0,192.168.10.255;
```

◆ Note ◆

An OmniSwitch with an MPM-1G, MPM-II, or original MPM will not display the Ethernet management port's IP address.

For information on modifying these screens, see *Configuring a Switch with an MPX/MPM-C/MPM-III* on page A-7 or *Configuring a Switch with an MPM/MPM-II/MPM-1G* on page A-10.

To change the configuration of the boot parameters, enter **c** at the prompt. For more information, see *Configuring a Switch with an MPX/MPM-C/MPM-III* on page A-7 or *Configuring a Switch with an MPM/MPM-II/MPM-1G* on page A-10.

Loading the Last Configured Boot File (l)

To load the last configured boot file, enter the **l** command. A screen similar to the following is shown:

```
Boot device           : ffs
Boot file             : /flash/mpx.img
Eth IP addr[:mask]   : 172.22.2.20
Startup script       : /flash/mpx.cmd
Console params       : 9600,n81c
Modem params         : 9600,n81d
Boot flags           : 0xb
Other                 : dvip:TECHPUB-
120,172.22.2.120,255.255.0.0,172.22.255.255;

Loading /flash/mpx.img...25320 + 2163504 + 314792
entry = 0x40e00000
```

◆ Note ◆

An OmniSwitch with an MPM-1G, MPM-II, or original MPM will not display the Ethernet management port's IP address.

Listing Available Files in the Flash Memory (L)

To list all of the available files in the flash memory that you could load onto the switch, enter the **L** command. A screen similar to the following is shown:

```
Files available in "/flash":
  mpm.cmd
  mpm.log
  asm.img
  esm.img
  mesm.img
  mpm.img
  mpm.cnf
  mpm.cfg
  switch.ascii
[Boot]:
```

Deleting All Files in the Flash Memory (P)

To delete all flash memory files, enter the **P** command at the prompt. The following message is displayed:

```
WARNING: This will remove ALL the files in the system.
Do you want to do this? ->
```

Enter **y** at the prompt to continue. The following message is shown

```
Erasing Flash File System...Done...Rebooting...
```

The switch will automatically reboot at this point. Since there are now no files in the flash memory, you are returned to the boot prompt.

Deleting Specific Files in the Flash Memory (R)

To delete a specific file from the flash memory, use the **R** command followed by the file name. You can delete a single file or multiple files with a single command. For example, to delete the **mpm.cmd** file, you would enter **R** followed by a space, and then **mpm.cmd**, as shown:

```
R mpm.cmd
```

To delete the **mpm.cmd** and the **mpm.log** files, you would enter **R**, a space, **mpm.cmd**, a space, and then **mpm.log**, as shown:

```
R mpm.cmd mpm.log
```

Saving Configuration Changes (S)

To save any changes to the configuration parameters, enter the **S** command at the prompt. The following message appears to confirm when the process is complete:

```
Saving boot information...done  
[Boot]:
```

Viewing Version Number (V)

To view the version number of the bootstrap shell, enter the **V** command at the prompt.

◆ Important Note ◆

Some of the options within the Boot Line configuration menu are for programmer's internal debugging purposes or for Customer Service diagnostics. Alcatel does not recommend that you invoke any menu options not described in this section.

Configuring a Switch with an MPX/MPM-C/MPM-III

Perform the following steps to configure an Omni Switch/Router (MPX) or an OmniSwitch with an MPM-C or MPM-III. You can press **Ctrl-D** at any time to return to the Boot prompt.

1. At the Boot prompt, enter a lowercase **c** to begin configuring parameters. A prompt similar to the following displays.

```

      '.' = clear field;      '.' = go to previous field;      ^D = quit
      Boot device           : ffs
  
```

2. To change the switch's boot device, (i.e., the device it will read the boot file from) enter **ffs** for the flash file system (the default), **pcn** for the Ethernet management port, **sl** for a SLIP device, or **zm** for ZMODEM.

A screen prompt similar to the following displays.

```

      Boot file             : /flash/mpx.img
  
```

3. Enter the boot file name or press the **<Enter>** key to accept the default (**mpx.img** for the MPX, **mpmc.img** for the MPM-C, and **mpm3.img** for the MPM-III). For FTP downloads, the path you should enter is relative to the log-in (i.e., remote) directory. A prompt similar to the following displays.

```

      Eth IP addr[:mask]   :
  
```

4. Enter an IP address for the Ethernet management port in dotted decimal notation. As an option, you can also enter an IP subnet mask in hexadecimal notation. If no mask is provided, the switch will try to determine the mask using Internet Control Message Protocol (ICMP) requests.

◆ Note ◆

The Ethernet management ports on the MPM-C and MPM-III have a default IP address of 192.168.11.1.

A screen prompt similar to the following displays.

```

      Local hostname       :
  
```

5. Enter a name for the MPX/MPM-C/MPM-III here.

◆ Note ◆

Steps 6 through 10 are only important if you are booting your switch from a network.

6. A screen prompt similar to the following displays.

```

      Remote IP addr[:mask] :
  
```

You can enter an IP address for a remote host. In addition, you can also enter an IP address mask in hexadecimal notation. If no mask is provided, it will infer it from the IP address class.

A screen prompt similar to the following displays.

```

      Remote hostname      :
  
```

7. You can enter a remote host name. A screen prompt similar to the following displays.

```

      Gateway IP addr      :
  
```

8. You can enter an IP address for the first hop router to a remote host (if the host is on a different IP net). A screen prompt similar to the following displays.

User :

9. You can enter a log-in name for a remote host. A screen prompt similar to the following displays.

Remote password :

10. You can enter a password for a remote host.

11. A screen prompt similar to the following displays.

Startup script : /flash/mpx.cmd

Enter the command file name or press the **<Enter>** key to accept the default (**mpx.cmd** for the MPX, **mpmc.cmd** for the MPM-C, and **mpm3.cmd** for the MPM-III). A prompt similar to the following displays.

Console params : 9600,n81c

12. You can change the parameters for the console port. To change the value, enter the baud rate (**1200**, **9600**, or **19200**, or **38400**), the parity (**n** for none, **e** for even, or **o** for odd), data length (**7** or **8**), stop bits (**0**, **1**, or **2**), and port type (**c** for console, **s** for SLIP, or **d** for down).

For example, **19200n81c** sets the console port to 19,200 baud, no parity, 8-bit data length, 1 stop bit, and console mode.

◆ **Note** ◆

If the default baud rate shunt (E1) has not been removed, any changes to the baud rate you enter will be ignored and a message to that affect is displayed during the boot process.

A screen prompt similar to the following displays.

Modem params : 9600,n81d

13. You can change the parameters for the modem port. To change the value, enter the baud rate (**1200**, **9600**, or **19200**, or **38400**), the parity (**n** for none, **e** for even, or **o** for odd), data length (**7** or **8**), stop bits (**0**, **1**, or **2**), and port type (**m** for modem, **s** for SLIP, or **d** for down).

For example, **19200n81m** sets the modem port to 19,200 baud, no parity, 8-bit data length, 1 stop bit, and modem mode.

A screen prompt similar to the following displays.

Boot flags : 0xb

14. To accept the default (**oxb**) and perform a normal boot, press the **<Enter>** key. To restore the factory-configured boot process, enter **0x1000**. The following flags should only be used for internal debugging or Customer Service diagnosis:

- **0x02** Load the local system symbols.
- **0x04** Do not autoboot.
- **0x08** Quick autoboot (no countdown).
- **0x20** Disable login security.
- **0x40** Use **bootp** to get the boot parameters.
- **0x80** Use **tftp** to get the boot image.
- **0x100** Use proxy arp.

A screen prompt similar to the following displays.

```
Other      : dvip:no-name,192.168.10.1,255.255.255.0,192.168.10.255;
```

15. You can enter the default VLAN IP parameters by entering them in the following format:

```
dvip:<host name>,<IP address>[,<IP mask>[,<IP broadcast address>]]
```

16. The following screen prompt displays.

```
[Boot]:
```

Enter an uppercase **S** to save any parameters you changed. The following screen prompt displays.

```
[Boot]:
```

17. Enter an **@** to boot your switch.

Configuring a Switch with an MPM/MPM-II/MPM-1G

Perform the following steps to configure an OmniSwitch with an original MPM, MPM-II, or MPM-1G. (See *Configuring a Switch with an MPX/MPM-C/MPM-III* on page A-7 if you have an MPM-C or MPM-III.) You can press **Ctrl-D** at any time to return to the Boot prompt.

1. At the Boot prompt, enter a lowercase **c** to begin configuring parameters. A prompt similar to the following displays.

```
'.' = clear field;      '.' = go to previous field;    ^D = quit
Boot device           : ffs
```

2. To change the switch's boot device, (i.e., the device it will read the boot file from) enter **ffs** for the MPM's flash file system (the default), **sl** for SLIP, or **zm** for ZMODEM.

For SLIP boots, you will be downloading the switch's image file from another computer, so you must have an assigned IP address for the SLIP connection. Also, you must configure other SLIP specific parameters for you computer as well as for the other computer. Leave these fields blank if you are not using SLIP. For ZMODEM boots, you can enter the **zm** command, followed by the baud rate. For example, to use a ZMODEM boot with a baud rate of **192000**, you would enter:

```
zm:19200.
```

By entering the baud rate, you can run the ZMODEM connection temporarily at a higher baud rate. 19200 is the maximum transfer rate for ZMODEM transfers. Due to limitations in some PC's and other equipment, you may be limited to a 9600 baud rate.

A screen prompt similar to the following displays.

```
Boot file           : /flash/mpm.img
```

3. Enter the boot file name or press the **<Enter>** key to accept the default. For FTP downloads, the path you should enter is relative to the log-in (i.e., remote) directory. A screen prompt similar to the following is displayed:

```
Local SLIP addr:
```

4. If you are using SLIP, enter the local SLIP host name and its IP address. Otherwise, press the **<Enter>** key and leave it blank. A screen prompt similar to the following displays:

```
Startup script     : /flash/mpm.cmd
```

5. Enter the MPM command file name or press the **<Enter>** key to accept the default (**mpm.cmd**). A prompt similar to the following displays.

```
Console params    : 9600,n81c
```

6. You can change the parameters for the console port. To change the value, enter the baud rate (**1200**, **9600**, or **19200**, or **38400**), the parity (**n** for none, **e** for even, or **o** for odd), data length (**7** or **8**), stop bits (**0**, **1**, or **2**), and port type (**c** for console, **s** for SLIP, or **a** for auxiliary).

For example, **19200n81c** sets the console port to 19,200 baud, no parity, 8-bit data length, 1 stop bit, and console mode.

A screen prompt similar to the following displays.

```
Modem params      : 9600,n81d
```

7. You can change the parameters for the modem port. To change the value, enter the baud rate (**1200**, **9600**, or **19200**, or **38400**), the parity (**n** for none, **e** for even, or **o** for odd), data length (**7** or **8**), stop bits (**0**, **1**, or **2**), and port type (**m** for modem, **s** for SLIP, or **a** for auxiliary).

For example, **19200n81m** sets the modem port to 19,200 baud, no parity, 8-bit data length, 1 stop bit, and modem mode.

A screen prompt similar to the following displays.

Boot flags : **0xb**

8. To accept the default (**0xb**) and perform a normal boot, press the **<Enter>** key. To restore the factory-configured boot process, enter **0x1000**. The following flags should only be used for internal debugging or Customer Service diagnosis:
- **0x02** Load the local system symbols.
 - **0x04** Do not autoboot.
 - **0x08** Quick autoboot (no countdown).
 - **0x20** Disable login security.
 - **0x40** Use **bootp** to get the boot parameters.
 - **0x80** Use **tftp** to get the boot image.
 - **0x100** Use proxy arp.
 - **0x1000** Factory reset.

A screen prompt similar to the following displays.

Other : **dvip:no-name,192.168.10.1,255.255.255.0,192.168.10.255;**

9. You can enter the default VLAN IP parameters by entering them in the following format:
- dvip:<host name>,<IP address>[,<IP mask>[,<IP broadcast address>]]**

10. The following screen prompt displays.

[Boot]:

Enter an uppercase **S** to save any parameters you changed. The following screen prompt displays.

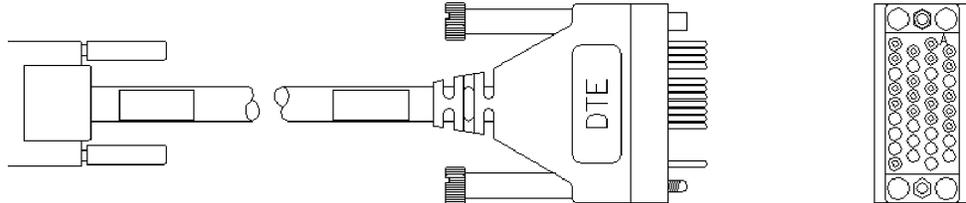
[Boot]:

11. Enter an **@** to boot your OmniSwitch.

B Custom Cables

This appendix provides detailed information, including illustrations and pin diagrams, for the cables that can be used with OmniSwitch and Omni Switch/Router Submodules. These custom cables are available from Alcatel, but you can use the following information to manufacture them.

V.35 DTE Cable (For WSM-to-DCE Device Connection)



The following parts are recommended for the end of the cable connected to the WSM.

- AMP 750833-1 26 Pin HD50 Connector-male
- AMP 750850-6 26 Pin HD50 Backshell

Parts for the customer end of the cable can be of any industry-standard manufacturer. Use of a shielded-type connector is recommended.

Cable should be constructed with data-comm-quality cable that has an overall mylar foil shield and braided-shield, terminated to the appropriate pins and connector shell at each end of the cable. Twisted-pair 28GA cable is preferred, with any of the pairs used for non-paired signals.

The table on the right shows the pinouts for the connectors.

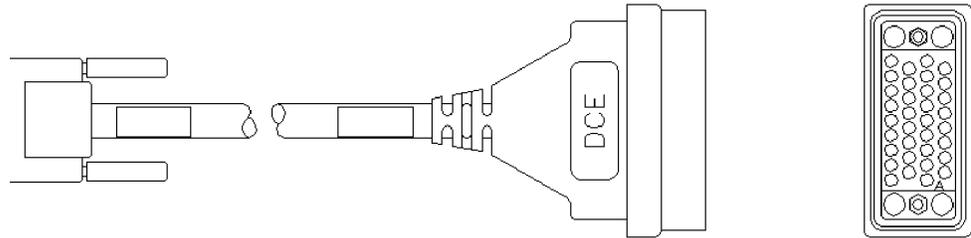
J2300		V35-M	
DTE		V35-M	
B	AB		
A	SHIELD		
P	BA-A		
S	BA-B		
R	BB-A		
T	BB-B		
Y	DB-A		
AA	DB-B		
V	DD-A		
X	DD-B		
U	DA-A		
W	DA-B		
C	CA-A		
D	CB-A		
E	CC-A		
F	CF-A		
H	CD-A		
N	RL		
NN	TM		

air

r

1, CTP0, respectively

V.35 DCE Cable (For WSM-to-DTE Device Connection)



The following parts are recommended for the end of the cable connected to the WSM.

- AMP 750833-1 26 Pin HD50 Connector-male
- AMP 750850-6 26 Pin HD50 Backshell

Parts for the customer end of the cable can be of any industry-standard manufacturer. Use of a shielded-type connector is recommended.

Cable should be constructed with data-comm-quality cable that has an overall mylar foil shield and braided-shield, terminated to the appropriate pins and connector shell at each end of the cable. Twisted-pair 28GA cable is preferred, with any of the pairs used for non-paired signals.

The table on the right shows the pinouts for the connectors.

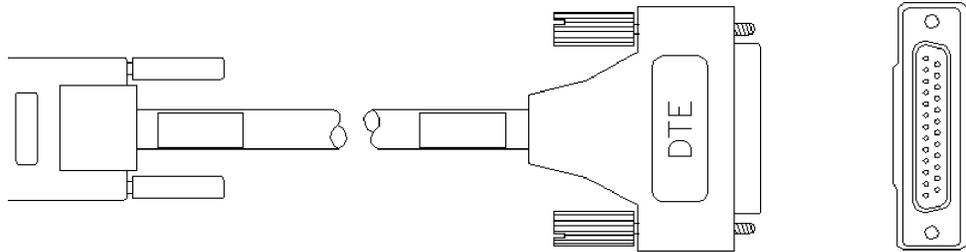
15100	DCE	V35-F
B	AB	
A	SHIELD	
R	BB-A	
T	BB-B	
P	EA-A	
S	EA-B	
Y	DB-A	
AA	DB-B	
U	DA-A	
W	DA-B	
V	DD-A	
X	DD-B	
F	CF-A	
D	CB-A	
H	CD-A	
C	CA-A	
E	CC-A	
MN	TM	
N	RL	

air

r

l, CTP0, respectively

RS232 DTE Cable (For WSM-to-DCE Device Connection)



The following parts are recommended for the end of the cable connected to the WSM.

- AMP 750833-1 26 Pin HD50 Connector-male
- AMP 750850-6 26 Pin HD50 Backshell

Parts for the customer end of the cable can be of any industry-standard manufacturer. Use of a shielded-type connector is recommended.

Cable should be constructed with data-comm-quality cable that has an overall mylar foil shield and braided-shield, terminated to the appropriate pins and connector shell at each end of the cable. Twisted-pair 28GA cable is preferred, with any of the pairs used for non-paired signals.

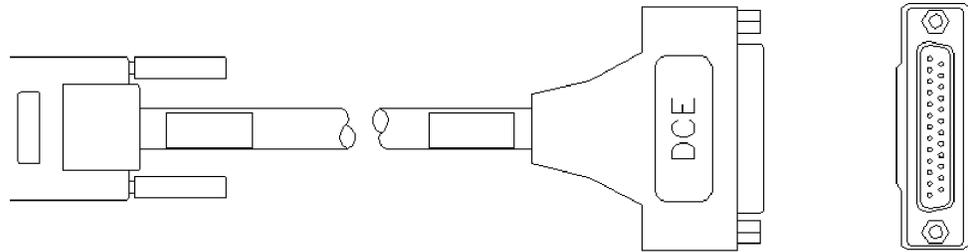
The table on the right shows the pinouts for the connectors.

<u>12002400</u>	<u>LATE DTE</u>	<u>DB25-M</u>
	7	AB
	1	SHIELD
	2	BA-A
	3	BB-A
	15	DB-A
	17	DD-A
	24	DA-A
	4	CA-A
	5	CB-A
	6	CC-A
	8	CF-A
	20	CD-A
	21	RL
	25	TM

≡d-pair

≡TP1, CTP0, respectively

RS232 DCE Cable (For WSM-to-DTE Device Connection)



The following parts are recommended for the end of the cable connected to the WSM.

- AMP 750833-1 26 Pin HD50 Connector-male
- AMP 750850-6 26 Pin HD50 Backshell

Parts for the customer end of the cable can be of any industry-standard manufacturer. Use of a shielded-type connector is recommended.

Cable should be constructed with data-comm-quality cable that has an overall mylar foil shield and braided-shield, terminated to the appropriate pins and connector shell at each end of the cable. Twisted-pair 28GA cable is preferred, with any of the pairs used for non-paired signals.

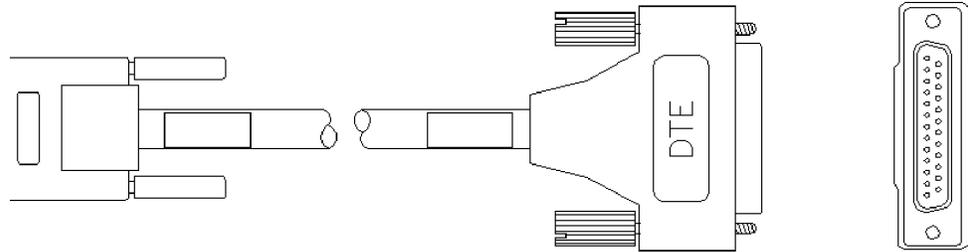
The table on the right shows the pinouts for the connectors.

12005200	
ATE DCE	DB25-F
7	AB
1	SHIELD
3	BB-A
2	BA-A
15	DB-A
24	DA-A
17	DD-A
8	CF-A
5	CB-A
20	CD-A
4	CA-A
6	CC-A
25	TM
21	RL

ed-pair

CTP1, CTP0, respectively

RS530 DTE Cable (For WSM-to-DCE Device Connection)



The following parts are recommended for the end of the cable connected to the WSM.

- AMP 750833-1 26 Pin HD50 Connector-male
- AMP 750850-6 26 Pin HD50 Backshell

Parts for the customer end of the cable can be of any industry-standard manufacturer. Use of a shielded-type connector is recommended.

Cable should be constructed with data-comm-quality cable that has an overall mylar foil shield and braided-shield, terminated to the appropriate pins and connector shell at each end of the cable. Twisted-pair 28GA cable is preferred, with any of the pairs used for non-paired signals.

The table on the right shows the pinouts for the connectors.

12500	DTE	DB25-M
7	AB	
1	SHIELD	
2	BA-A	
14	BA-B	
3	BB-A	
16	BB-B	
15	DB-A	
12	DB-B	
17	DD-A	
18	DD-B	
24	DA-A	
11	DA-B	
4	CA-A	
19	CA-B	
5	CB-A	
13	CB-B	
6	CC-A	
22	CC-B	
8	CF-A	
10	CF-B	
20	CD-A	
23	CD-B	
21	RL	
25	TM	

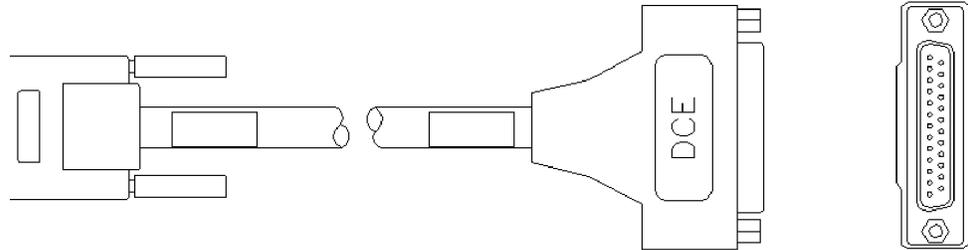
pair

r

r

l, CTP0, r respectively

RS530 DCE Cable (For WSM-to-DTE Device Connection)



The following parts are recommended for the end of the cable connected to the WSM.

- AMP 750833-1 26 Pin HD50 Connector-male
- AMP 750850-6 26 Pin HD50 Backshell

Parts for the customer end of the cable can be of any industry-standard manufacturer. Use of a shielded-type connector is recommended.

Cable should be constructed with data-comm-quality cable that has an overall mylar foil shield and braided-shield, terminated to the appropriate pins and connector shell at each end of the cable. Twisted-pair 28GA cable is preferred, with any of the pairs used for non-paired signals.

The table on the right shows the pinouts for the connectors.

RS530	DCE	DE25-F
7	AB	
1	SHIELD	
3	BB-A	
16	BB-B	
2	BA-A	
14	BA-B	
15	DB-A	
12	DB-B	
24	DA-A	
11	DA-B	
17	DD-A	
9	DD-B	
8	CF-A	
10	CF-B	
5	CB-A	
13	CB-B	
20	CD-A	
23	CD-B	
4	CA-A	
19	CA-B	
6	CC-A	
22	CC-B	
25	TM	
21	RL	

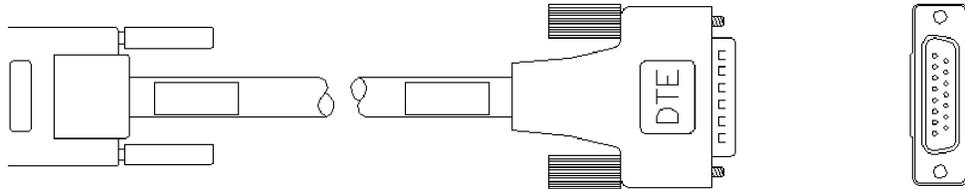
Pair

r

r

1, CTP0, respectively

X.21 DTE Cable (For WSM-to-DCE Device Connection)



The following parts are recommended for the end of the cable connected to the WSM.

- AMP 750833-1 26 Pin HD50 Connector-male
- AMP 750850-6 26 Pin HD50 Backshell

Parts for the customer end of the cable can be of any industry-standard manufacturer. Use of a shielded-type connector is recommended.

Cable should be constructed with data-comm-quality cable that has an overall mylar foil shield and braided-shield, terminated to the appropriate pins and connector shell at each end of the cable. Twisted-pair 28GA cable is preferred, with any of the pairs used for non-paired signals.

The table on the right shows the pinouts for the connectors.

12600	DTE	DE15-M
8	SIG GND	
1	SHIELD	
2	T-A	
9	T-B	
4	R-A	
11	R-B	
6	S-A	
13	S-B	
7	E-A	
14	E-B	
3	C-A	
10	C-B	
5	I-A	
12	I-B	

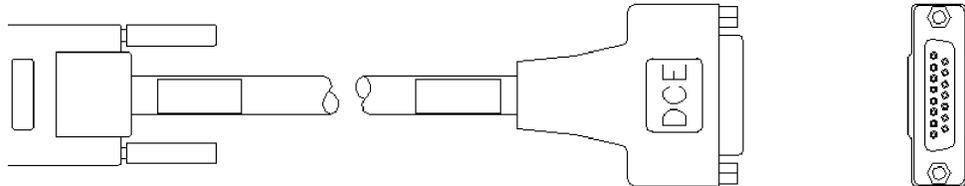
air

r

r

l, CTP0, r respectively

X.21 DCE Cable (For WSM-to-DTE Device Connection)



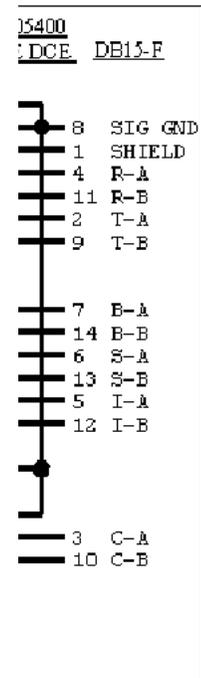
The following parts are recommended for the end of the cable connected to the WSM.

- AMP 750833-1 26 Pin HD50 Connector-male
- AMP 750850-6 26 Pin HD50 Backshell

Parts for the customer end of the cable can be of any industry-standard manufacturer. Use of a shielded-type connector is recommended.

Cable should be constructed with data-comm-quality cable that has an overall mylar foil shield and braided-shield, terminated to the appropriate pins and connector shell at each end of the cable. Twisted-pair 28GA cable is preferred, with any of the pairs used for non-paired signals.

The table on the right shows the pinouts for the connectors.



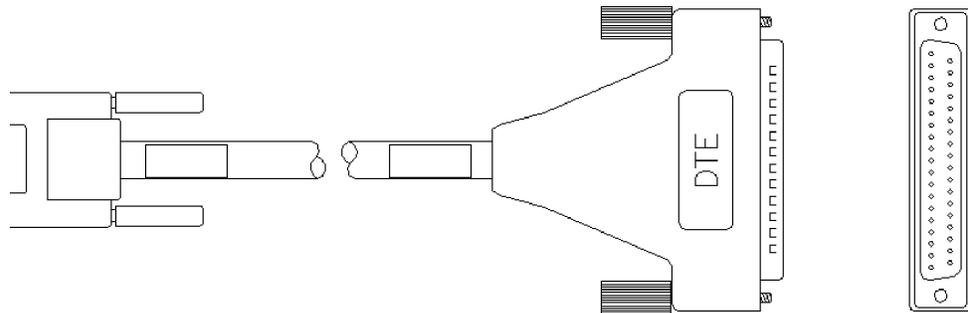
pair

r

r

1, CTP0, r respectively

RS449 DTE Cable (For WSM-to-DCE Device Connection)



The following parts are recommended for the end of the cable connected to the WSM.

- AMP 750833-1 26 Pin HD50 Connector-male
- AMP 750850-6 26 Pin HD50 Backshell

Parts for the customer end of the cable can be of any industry-standard manufacturer. Use of a shielded-type connector is recommended.

Cable should be constructed with data-comm-quality cable that has an overall mylar foil shield and braided-shield, terminated to the appropriate pins and connector shell at each end of the cable. Twisted-pair 28GA cable is preferred, with any of the pairs used for non-paired signals.

The table on the right shows the pinouts for the connectors.

12700	DTE	DB37-M
19	AB	
1	SHIELD	
4	SD-A	
22	SD-B	
6	RD-A	
24	RD-B	
5	ST-A	
23	ST-B	
8	RT-A	
26	RT-B	
17	TT-A	
35	TT-B	
7	RS-A	
25	RS-B	
9	CS-A	
27	CS-B	
11	DM-A	
29	DM-B	
13	RR-A	
31	RR-B	
12	TR-A	
30	TR-B	
14	RL	
18	TM	

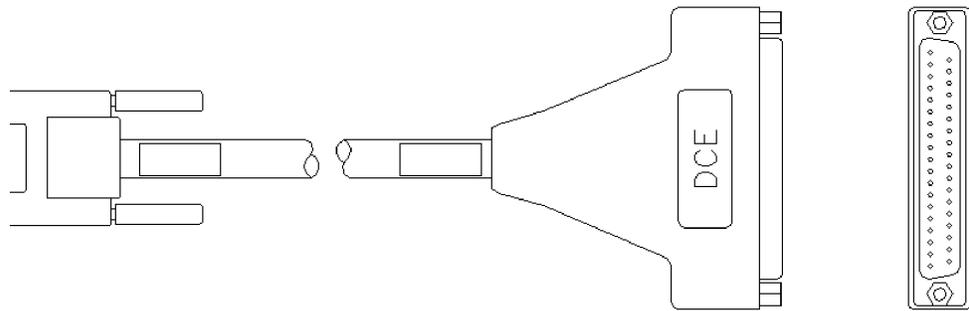
air

r

r

l, CTP0, respectively

RS-449 DCE Cable Assembly (For WSM-to-DTE Device 75Ω Connection)



The following parts are recommended for the end of the cable connected to the WSM.

- AMP 750833-1 26-Pin HD50 Connector-male
- AMP 750850-6 26-Pin HD50 Backshell

Parts for the customer end of the cable can be of any industry-standard manufacturer. Use of a shielded-type connector is recommended.

Cable should be constructed with data-comm-quality cable that has an overall mylar foil shield and braided-shield, terminated to the appropriate pins and connector shell at each end of the cable. Twisted-pair 28GA cable is preferred, with any of the pairs used for non-paired signals.

The table on the right shows the pinouts for the connectors.

15500	
DCE	DB37-F
19	AB
1	SHIELD
6	RD-A
24	RD-B
4	SD-A
22	SD-B
5	ST-A
23	ST-B
17	TT-A
25	TT-B
8	RT-A
26	RT-B
13	RR-A
31	RR-B
9	CS-A
27	CS-B
12	TR-A
30	TR-B
7	RS-A
25	RS-B
11	DM-A
29	DM-B
18	TM
14	RL

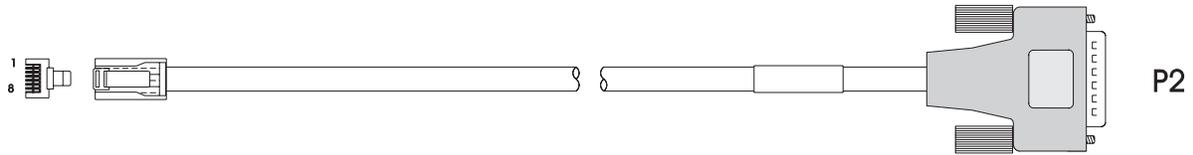
pair

r

r

l, CTP0, r respectively

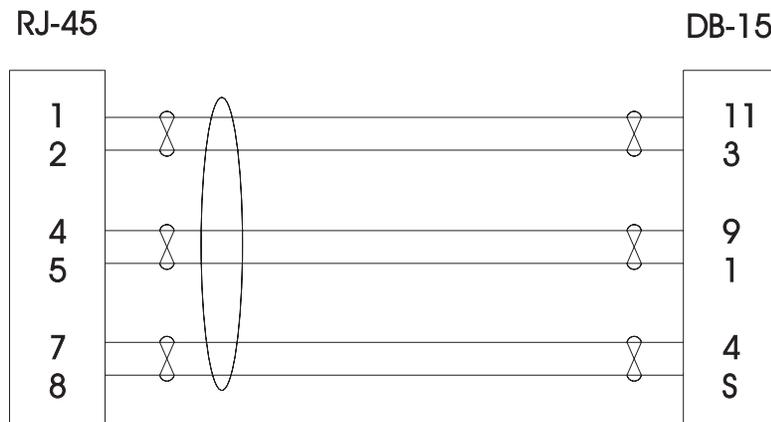
RJ-45 to DB15F Cable Assembly (For T1/E1 Port 120Ω Connections)



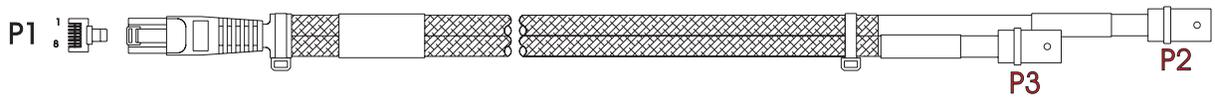
The following parts are recommended for the ends of the cable:

- For the switch side of the cable assembly (P1): 8-conductor RJ-45 round connector (MTP-88U or equivalent)
- Parts for the customer end of the cable (P2) can be of any industry-standard manufacturer. Use of a shielded-type DB-15 female connector is recommended.

Cable should be constructed with datacomm-quality cable that has an overall mylar foil shield and braided-shield, terminated to the appropriate pins and connector shell at each end of the cable. Twisted-pair 28GA cable is preferred, with any of the pairs used for non-paired signals.



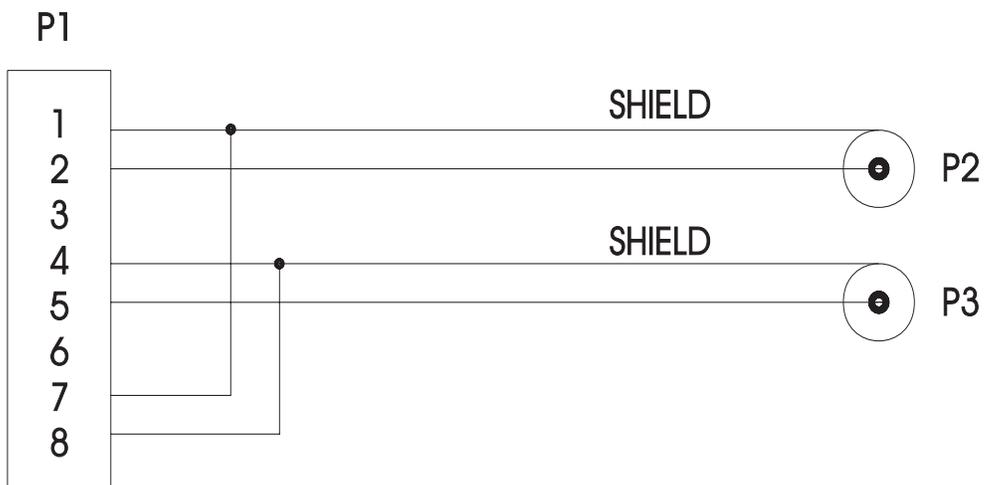
RJ-45 to BNC Cable Assembly (For E1 75Ω Port Connections)



The following parts are recommended for manufacturing the cable:

- For the switch side of the cable assembly (P1): 8-conductor RJ-45 round connector (MTP-88U or equivalent)
- For the cable: RG-187A coaxial cable (Belden 83267 or equivalent)
- For the customer end of the cable assembly (P2 and P3): Coaxial BNC connector, 75Ω (Amp 413760-8, or equivalent).

The figure below shows the pinouts for the cable assembly.



Index

- ! commands 8-30
 - + or - commands 22-7
 - ? command 8-20, 8-29
 - 10/100 20-1, 20-9
 - 10/100** command 19-6
 - 10/100 ports 19-7, 19-10
 - 10/100cfg** command 3-16, 3-19, 3-22, 7-18, 7-20, 7-22, 7-24, 7-28, 7-31, 7-85, 19-7, 19-9
 - 10/100vc** command 7-28, 19-10
 - 1483 routed format services 24-44
 - creating 36-47
 - displaying service statistics 36-74
 - modifying 36-59
 - 1483 scaling services 36-17
 - creating 36-40
 - displaying 36-72
 - mapping parameters 36-43
 - modifying 36-57
 - 802.1Q 19-1, 20-1
 - 802.2 pass through 23-16, 24-35
- ## A
- AAL5 Discard 41-35
 - IOP2 restrictions 41-15
 - aal5_dx variable 41-15
 - aat** command 36-53
 - ab** command 11-8
 - access rate 48-26, 48-31, 48-41, 48-44
 - actfstps** command 22-38, 22-39
 - adaptive clocking 34-9
 - addprtchnl** command 19-15
 - addvp** command 24-5, 24-20, 24-31, 24-52, 24-68
 - translations 23-16
 - adjacency
 - definition for XMAP 26-2
 - ADM 3-55, 3-58, 7-59, 7-62, 7-68, 7-71, 40-57, 54-25, 54-26
 - admin login 8-37, 12-2
 - aipxsr** command 32-12
 - AIS 54-18, 54-19, 54-24, 54-26, 54-27
 - LED 3-57, 3-60, 7-61, 7-70, 7-73
 - aisr** command 30-17
 - alert** command 8-35
 - alternate routing
 - in PNNI 46-26
 - any-to-any switching 23-1
 - ARP protocol 30-3
 - ARP server 33-44
 - ASCII terminal commands 8-21
 - ASM-155C 5-19, 7-45
 - ASM-155F 5-19
 - ASM-155Fx 7-42
 - fiber optic power budget 7-43
 - ASM2 and ASX modules 33-3, 33-4
 - bandwidth groups 33-60
 - MBS 33-69
 - PCR 33-68
 - SCR 33-69
 - traffic shaping 33-60
 - ASM2-155F 7-47
 - fiber optic power budget 7-48, 7-51
 - ASM2-155FR 7-50
 - ASM2-155Fx 7-42
 - ASM2-622F 7-53
 - ASM2-622FR 7-56
 - ASM2-DS3 5-19, 7-68
 - ASM2-E3 5-19, 7-71
 - ASM-CE 7-65, 34-1, 34-2, 34-21, 34-25, 53-1
 - fiber optic power budget 7-66
 - ASM-DS3 5-19, 7-59
 - ASM-E3 5-19, 7-62
 - ASX-155FH 3-42
 - ASX-155FM 3-42
 - ASX-155FM/FS/FH
 - fiber optic power budget 3-43
 - ASX-155FS 3-42
 - ASX-155RFM/RFS 3-45
 - fiber optic power budget 3-46
 - ASX-622RFM/RFS 3-48
 - fiber optic power budget 3-49
 - ASX-DS3 3-55
 - ASX-E3 3-58
 - ASX-M-622RFM/RFS/RFH-1W 3-51
 - fiber optic power budget 3-53
 - at** command 24-20

- ATM
 - 1483 routed format services 36-19, 36-47
 - 1483 scaling services 36-17
 - access modules 33-1
 - accounting 44-1
 - cell errors 33-47
 - Classical IP 36-12
 - congestion 42-43, 42-55
 - discards 33-46
 - IMA 43-1
 - improving signaling performance 40-2
 - IPX routing 24-43, 24-45
 - LAN Emulation 36-4
 - leaky buckets 42-43
 - menu 33-7
 - point-to-multipoint 41-38
 - Point-to-Point Bridging 36-14
 - priority for virtual circuits 41-45, 42-14
 - segment buffers 33-11
 - Segmentation and Reassembly (SAR) 33-11
 - statistics 33-45, 33-46, 33-50, 33-52, 33-55, 33-57
 - traffic descriptors 41-17
 - Trunking 36-31
 - VLAN clusters (X-LANE) 36-15
 - VP switching 41-51
- ATM access ports
 - cell errors 33-47
 - configuring 33-8
 - discards 33-46
 - loopback mode 33-12
 - PCR 33-17, 38-33
 - PVCs 33-15
 - Segmentation and Reassembly (SAR) 33-11
 - statistics 33-45, 33-46, 33-50
 - viewing 33-26
 - virtual channels 33-35
- ATM accounting
 - accept calls 44-10, 44-11
 - alternate collection device 44-24
 - CDRs 44-4
 - collecting CDRs manually 44-24
 - concept of "charging" 44-4
 - definition 44-2
 - parameters 44-12
 - periodic collection 44-6
 - collection interval 44-6, 44-7
 - configuration query 44-29
 - configuration using the CLI 44-20, 44-21
 - CLI conventions 44-21
 - software requirements 44-20
 - defining a collection interval 44-28
 - defining a congestion strategy 44-25
 - defining a tariff period 44-28
 - disabling at the node level 44-24
 - disabling at the port level 44-26
 - disabling at the PVC/SPVC level 44-27
 - enabling accounting 44-2, 44-22
 - enabling at the node level 44-19, 44-22
 - enabling at the port level 44-19, 44-26
 - enabling at the PVC/SPVC level 44-19, 44-27
 - MPM restart 44-22
 - overview 44-2
 - reboot 44-22, 44-23
 - refuse calls 44-10, 44-11
 - supported hardware 44-1
 - tariff period 44-6, 44-7
- ATM address
 - creating 33-24
 - deleting 33-25
 - modifying 33-25
 - viewing 33-43
- atm** command 33-7, 41-26
- ATM connections
 - total amount on a switch 41-100
 - viewing 41-100
- ATM Direct Mapped (ADM) Protocol 54-25, 54-26
- ATM modules 3-40, 7-36, 33-2
 - ASM-155C 7-45
 - ASM-155Fx 7-42
 - ASM2-155F 7-47
 - ASM2-155FR 7-50
 - ASM2-155Fx 7-42
 - ASM2-622F 7-53
 - ASM2-622FR 7-56
 - ASM2-DS3 7-68
 - ASM2-E3 7-71
 - ASM-CE 7-65
 - ASM-DS3 7-59
 - ASM-E3 7-62
 - ASX-155FH 3-42
 - ASX-155FM 3-42
 - ASX-155FS 3-42
 - ASX-155RFM/RFS 3-45
 - ASX-622RFM/RFS 3-48
 - ASX-DS3 3-55

- ASX-E3 3-58
 - ASX-M-622RFM/RFS/RFH-1W 3-51
 - pinouts 7-38
 - ATM Name Server (ANS) 42-36
 - ATM Point-to-Point Bridging 36-14
 - ATM ports
 - DS3 54-17, 54-20, 54-21, 54-22, 54-28, 54-29, 54-30, 54-31
 - E3 54-23, 54-25, 54-26, 54-32, 54-33
 - number of services supported 36-1
 - viewing 33-26
 - ATM switch
 - service registry table 42-36
 - ATM switching 4-2, 4-5, 4-9, 4-19
 - applications 40-6
 - buffer management 40-10
 - buffers supported 40-15
 - Cell Loss Priority (CLP) 41-14
 - congestion 41-13
 - connections supported 40-15
 - EFCI 41-12
 - error statistics 42-41, 42-54
 - FCSM required 40-13, 40-14, 40-17
 - input buffers 40-10
 - intelligent multicast replication 42-56
 - label swapping 41-5
 - large cell buffers 40-11
 - Maximum Burst Size (MBS) 33-69, 41-16
 - monitoring 42-46
 - Peak Cell Rate (PCR) 33-68, 33-70, 41-16
 - point-to-multipoint virtual circuits 41-6
 - point-to-point virtual circuits 41-6
 - priority levels 41-13
 - resource management 41-12
 - soft PVCs 41-7, 42-3
 - statistics 42-39
 - Sustainable Cell Rate (SCR) 33-69, 41-16
 - traffic descriptors 41-18
 - ATM Trunking 36-31
 - ATM uplinks 40-6
 - example 33-6
 - atm_use_mbus flag 40-2
 - atmlsem** command 36-75
 - atvl** command 25-23, 27-27
 - Authenticated Groups 24-1
 - as mobile group 24-5
 - configuring 24-30
 - Authentication 24-1
 - Authentication Management Console (AMC)
 - software 24-5
 - auto-activated LANE ports
 - configuring 24-37
 - autoencaps** command 23-39
 - auto-switch
 - diagram 24-33
 - timer 24-33
 - Auto-Switch bridge mode 24-33
 - AutoTracker
 - application examples 29-1
 - configuring policies 25-4
 - DHCP MAC address policy 25-3
 - DHCP policy 25-29
 - DHCP policy example 25-27
 - DHCP port policy 25-3
 - MAC address policy 25-2
 - menu 27-2
 - network address policy 25-2
 - policies 25-1, 27-3
 - port binding policy 25-2
 - port policy 25-2
 - protocol policy 25-2
 - user-defined policy 25-2
 - AutoTracker policies
 - in mobile group 24-38
 - Available Bit Rate (ABR) 40-2, 41-9, 41-25, 46-38
 - resource management 41-9
 - Available Cell Rate (AVCR)
 - minimum threshold 46-33
 - proportional multiplier 46-33
 - avlbootpmode** command 31-2
- ## B
- backbones 19-11
 - Ethernet 19-11
 - Backplane 45-4
 - backplane threshold 15-4
 - balanced T1 56-3
 - bandwidth group 33-60
 - Banyan Vines
 - translations for 23-12
 - VLAN for 27-31
 - BECN 49-11
 - BNC 56-3
 - boot configuration A-1
 - Boot prompt A-1
 - basic commands A-3
 - logging in A-2
 - MPM A-10

- MPM-1G A-10
- MPM-C A-7
- MPM-II A-10
- MPM-III A-7
- MPX A-7
- BOOTP relay 31-4
 - and authentication 31-5
- BPS 4-5, 5-3, 5-30
- br** command 22-4, 24-20
- BRI. See ISDN, Basic Rate Interface
- bridge 22-7
- bridge forwarding table 22-8
- bridge mode 24-32
 - non-Ethernet default 24-32
 - optimized 24-32
 - Spanning Tree 24-32
- bridge port
 - statistics 22-14
- bridging
 - Frame Relay 49-14, 49-54
- bsadd** command 55-3
- bsdelete** command 55-11
- bsmodify** command 55-9

C

- CAC & Call Overbooking 41-2
- cacheconfig** command 13-33
- Call Admission Control (CAC) 46-26
- CAM 7-14
 - configuring 13-25
- CAM Restrictions
 - Omni Switch/Router 13-26
 - OmniSwitch 13-25
- CAM threshold 15-5
- camcfg** command 13-25
- camstat** command 13-24
- caplog** command 14-11
- cas** command 20-9, 20-12, 24-37, 36-21
 - 1483 routed format services 36-47
 - 1483 scaling services 36-40
 - ATM Trunking 36-31
 - Classical IP (CIP) 36-33
 - Frame Relay bridging 49-54
 - Frame Relay routing 49-57
 - Frame Relay trunking 49-59
 - LAN Emulation 36-23
 - PTOP Bridging 36-36
 - VLAN Clusters 36-38

- cats** command 24-2, 24-16
- cb** command 11-7
- cd** command 11-2, 24-70
- CDRs 44-2, 44-4
 - accept calls 44-10, 44-11
 - collecting CDRs manually 44-24
 - collection interval 44-6, 44-7, 44-28
 - congestion strategy 44-10, 44-24, 44-25
 - accept calls/refuse calls 44-10, 44-11
 - threshold levels 44-10
 - traps 44-11
 - definition 44-2
 - parameters 44-12
 - periodic collection 44-6
 - refuse calls 44-10, 44-11
 - storage strategy 44-2, 44-9
 - tariff period 44-6, 44-7, 44-28
 - temporary storage 44-9, 44-10
 - terminated and intermediate CDRs 44-5, 44-6
- ceadd** command 34-12, 34-17
- cedelelete** command 34-28
- Cell Delay Variation (CDV) 41-10, 41-45, 42-14, 46-16, 46-52, 47-18
 - proportional multiplier 46-34
- Cell Loss Priority (CLP) 41-14
 - in statistics displays 42-46
- Cell Loss Ratio (CLR) 41-10, 47-18
- cell switching matrix
 - 13.2 Gbps capacity 40-9
 - distributed 40-9
- Cell Transfer Delay (CTD) 41-10, 46-16, 46-52, 47-18
 - proportional multiplier 46-34
- cellfab** command 58-3, 58-33
- cells
 - discarded 42-43
- cemodify** command 34-23
- CERR
 - LED 3-44, 3-47, 3-50, 7-44, 7-49, 7-52, 7-55, 7-58
- cestatus** command 34-29, 34-34, 34-36
- channelized DS3 56-2
- chassis
 - AC inputs 5-1
 - grounding 1-25, 5-28
 - power supplies 5-1
 - temperature 4-4
- chngmac** command 18-6
- chnlinfo** command 19-16

- circuit emulation 34-1
 - adaptive clocking 34-24
 - application example 34-10
 - ATM uplink port in 34-3
 - Cell Delay Variation Tolerance (CDVT) 34-14
 - commands 34-11
 - configuring 34-6
 - connection type 34-15
 - information 34-29
 - partial cell fill count 34-13
 - serial ports 34-3, 34-21, 34-25, 34-30
 - SRTS clocking 34-24
 - structured service 34-7, 34-23
 - synchronous clocking 34-23
 - T1/E1 ports 34-3, 34-12, 34-23
 - time Slots 34-14
 - unstructured service 34-7, 34-23
 - virtual channel connections 34-21
- circuit emulation clocking modes 34-8
- Class B 1-7, 5-17
- Class of Service
 - profiles 41-23, 41-26
- Classical IP (CIP) 24-22, 24-42, 36-33
 - ARP table 36-70
 - Group for 36-33
 - static entries 36-53
- clear channel 56-36
 - logical port 56-36
- clearstat** command 13-16
- Clocking
 - bus-level 45-4
 - port-level 45-2
- CLP 42-39
- CLPNoTagNoSCR 41-41, 42-9
- CLPNoTagSCR 41-42, 42-10
- CLPTagNoSCR 41-41, 42-10
- CLPTagSCR 41-42, 42-11
- cmdlog** command 14-9
- command families 12-13, 12-17
- command history 8-30
- Command Line Interface 8-1
- Committed Information Rate (CIR)
 - Frame Relay 49-8
- communications
 - see also serial port
- configsync** command 10-16
- configuration file
 - switch fails to create 57-11
- configuration files 11-2
- configuration submenu 46-28
- congestion
 - ATM 42-43, 42-55
- conlog** command 14-10
- console port 6-7
 - configuring 2-6, 10-2, 40-28
 - speed 10-2
- Constant Bit Rate (CBR) 34-1, 41-8, 41-23, 46-38
- consumable resources 15-2
- cp** command 11-6
- cpis** command 54-33
- CPU threshold 15-5
- crankback
 - in PNNI 46-26, 46-54
- cratvl** command 27-4, 27-16, 27-31
- creating a group 24-44
- crechnl** command 19-13
- credit
 - transmit 24-34
- crgp** command 24-5, 24-22, 27-4
 - translations 23-16
- crm cvl** command 28-5
- crtsmmap** command 21-35
- CSM modules 40-1, 40-9, 40-15, 41-1
 - CSM-155 40-30
 - CSM-155C-8 40-38
 - CSM-622 40-34
 - CSM-A25-12 40-42
 - CSM-A25-24W 40-44
 - CSM-U 40-46, 40-65
 - CSM-U+ 40-46, 40-65
 - FCSM 40-17
 - required image files 41-3
- CSM ports
 - IMA 43-5
- CSM Traffic Shaping
 - activating 42-67
 - configuration using the CLI 42-66
 - CLI conventions 42-66
 - software requirements 42-65
 - disabling 42-70
 - enabling/disabling 42-67
 - viewing 42-69
- CSM-155 40-15, 40-30
 - multicasts 40-30
 - virtual circuits supported 40-30
- CSM-155C-8 40-38
 - jumper settings 40-41
 - multicasts 40-38

- virtual circuits supported 40-38
 - CSM-155-F
 - jumper settings 40-33
 - CSM-622 40-15, 40-34
 - jumper settings 40-37
 - multicasts 40-34
 - virtual circuits supported 40-34
 - CSM-A25-12 40-15, 40-42
 - multicasts 40-42
 - virtual circuits supported 40-42
 - CSM-A25-24 40-15
 - CSM-A25-24W 40-44
 - multicasts 40-44
 - virtual circuits supported 40-44
 - CSM-AB-155C 40-52
 - jumper settings 40-54
 - multicasts 40-52
 - virtual circuits supported 40-52
 - CSM-AB-155F 40-49
 - jumper settings 40-51
 - multicasts 40-49
 - virtual circuits supported 40-49
 - CSM-AB-CE-E1-4W 40-59
 - jumper settings 40-60, 40-61
 - CSM-AB-CE-T1-4W 40-59
 - CSM-AB-CM 40-62
 - jumper settings 40-64
 - CSM-AB-DS1-4W 40-55
 - CSM-AB-DS3-2W 40-57
 - CSM-AB-E1-4W 40-55
 - CSM-AB-E3-2W 40-57
 - CSM-AB-IMA-DS1-8W 40-65, 53-1
 - upgrading flash memory 43-33
 - CSM-AB-IMA-E1-8W 40-65, 53-1
 - jumper settings 40-67, 40-68
 - upgrading flash memory 43-33
 - CSM-ABT-155F 40-69
 - installation guidelines 40-69
 - multicasts 40-69
 - traffic shaping supported 40-69
 - virtual circuits supported 40-69
 - CSM-CE 34-1, 34-4, 53-1
 - CSM-T1/E1 53-1
 - CSM-U 40-15, 40-46, 40-65, 53-1
 - wide chassis required 40-46
 - CSM-U+ 40-15, 40-46, 40-65
 - support for 14-bit VPI/VCI 40-46
 - wide chassis required 40-46
 - CSM-U/CSM-U+ adapter boards
 - CSM-AB-155C 40-52
 - CSM-AB-155F 40-49
 - CSM-AB-CE-E1-4W 40-59
 - CSM-AB-CE-T1-4W 40-59
 - CSM-AB-CM 40-62
 - CSM-AB-DS1-4W 40-55
 - CSM-AB-DS3-2W 40-57
 - CSM-AB-E1-4W 40-55
 - CSM-AB-E3-2W 40-57
 - CSM-AB-IMA-DS1-8W 40-65, 53-1
 - CSM-AB-IMA-E1-8W 40-65, 53-1
 - CSM-ABT-155F 40-69
 - cut-through routing 37-2
 - cva** command 33-24
 - cvc** command 33-15, 41-38
 - CSM virtual circuits 41-33
 - cvpt** command 42-26, 47-8, 47-9, 47-11
 - with static routes 47-3
-
- ## D
- das** command 20-20, 36-60
 - Frame Relay 49-63
 - dat** command 36-61
 - date 13-8
 - datas** command 24-16
 - Daylight Savings Time (DST) 13-8, 13-12
 - db** command 11-9
 - dbrmapp** command 22-19
 - DC power supplies 1-28, 1-31, 5-23
 - debuglog** command 14-13
 - def_group variable 24-12
 - default group 24-12
 - default VLAN 27-4, 27-5
 - routing 29-8
 - defvfl** command 27-5
 - delechnl** command 19-15
 - delprtchnl** command 19-16
 - DES 16-4
 - Designated Transit List (DTL) 46-6, 46-24, 46-39, 46-54
 - DHCP 31-4
 - and source routing 31-5
 - application example 25-27
 - overview 31-4
 - policies 25-3
 - with non-DHCP clients 31-8
 - DHCP client 25-28
 - DHCP server 25-28
 - diag login 8-37, 12-2

diag user login 58-3, 58-5
 diagnostic tests 7-12
 cell fabric test 58-33
 chassis 58-37
 frame fabric test 58-35
 diagnostics
 configuring 58-29, 58-30, 58-37
 hardware 58-1
 login 58-3, 58-5
 running 58-3, 58-8
 diagnostics sub-menu 8-20, 58-5
 digital services 53-2
 digital signal level X, see DSX
 discard cells 42-43
 Discard Eligibility
 Frame Relay 49-9
 displaying Ethernet switch statistics 23-30
 DLCI 49-6
 DLCMI 49-23
 domain bridging
 mapping table 22-19
 domain name servers 18-1
 DS0 56-2
 DS1 56-2
 DS1 channel 56-24
 configuration and statistical parameters 56-32
 statistics and errors 56-26, 56-28, 56-29, 56-31
ds1clis command 56-31
ds1dcs command 56-32
ds1dlcs command 56-28
ds1dlis command 56-29
ds1dlts command 56-26
ds1mod command 56-24
 DS2 56-2
 DS-3 3-40, 3-55, 7-36, 7-59, 7-68
 software 54-17, 54-20, 54-21, 54-22, 54-28, 54-29, 54-30, 54-31
 DS3 56-2
ds3 command 54-2
 DS3 port 56-14
 statistical parameters 56-22
 statistics and errors 56-17, 56-19, 56-20
 DS3/EC
 PLCP and 45-3
ds3clis command 56-22
ds3dcs command 56-22
ds3dlcs command 56-19
ds3dlis command 56-20

ds3dlts command 56-17
ds3mod command 56-14, 56-36
dslcs command 54-15, 56-19, 56-28
dslis command 54-16, 56-20, 56-29
dslts command 54-13, 56-17
dsmod command 54-2
dss command 54-7
 DST 13-8
 DSX 56-2
dt command 13-8
dtsmap command 21-38
 duplicate MAC addresses 13-23
dva command 33-25
dvc command 33-23, 41-53
dvpt command 42-35
 dynamic LANE services 24-5, 24-16
 deleting 24-16
 dynamic port assignment 24-2

E

E.164 addresses 47-4
 E1
 configuring 31 timeslots 48-53
 fractional 48-4
 framing 53-2
 E3 3-40, 3-58, 7-36, 7-62, 7-71
 software 54-23, 54-25, 54-26, 54-32, 54-33
eb command 11-9
echo command 8-35
edit command 11-7
 edit commands tutorial 11-11, 11-12
 egress cache table 37-20
 ELANs
 auto-activated 24-16, 24-37
 multiple 36-26
 encapsulation 23-5
 IP 23-5
 IPX 23-5, 23-7
 error messages 57-12
 ESM-100C 5-18, 7-101
 ESM-100C-12 7-18, 19-7, 19-10
 non-auto-negotiating links 19-8
 ESM-100C-32W 7-28, 19-10
 non-auto-negotiating links 19-8
 ESM-100C-5 7-109
 ESM-100C-FD 5-18, 7-105
 ESM-100CFx-5 7-112
 ESM-100FM/FS-8 7-20

- ESM-100FM-8 19-10
 - ESM-100FM-FD 5-18
 - ESM-100FS-FD 5-18
 - ESM-100Fx-FD 7-107
 - ESM-C-8 5-18, 7-91
 - ESM-C-12 5-18, 7-89
 - ESM-C-16 7-22, 19-10
 - ESM-C-32 19-10
 - ESM-C-32W 7-24
 - ESM-F-8 5-18, 7-93
 - fiber optic power budget 7-93
 - ESM-F-16 7-26
 - fiber optic power budget 7-26
 - ESM-FM-16W 19-10
 - ESM-T-12 5-18, 7-95
 - ESM-T-24W 5-18, 7-31, 19-10
 - ESM-U-6 5-18, 7-97
 - ESX-100C-12W 3-16, 19-10
 - non-auto-negotiating links 19-8
 - ESX-100C-32W 3-19, 19-10
 - non-auto-negotiating links 19-8
 - ESX-100FM/FS-12W 3-25, 19-10
 - ESX-FM-24W 3-31, 19-10
 - ESX-K-100C-32W 3-22
 - ESX-K-100FM/FS-16W 3-28
 - eth100** command 19-6
 - eth100cfg** command 7-105, 7-107, 7-109, 7-112, 19-18
 - eth100vc** command 19-19
 - ethdef** command 23-25
 - Ethernet
 - 10/100 ports 19-7
 - 802.1q 19-1
 - auto-sensing ports 19-7
 - auto-switch bridge mode 24-33
 - backbones 19-11
 - default translations 23-17, 23-25
 - duplex mode 19-10
 - Ethertype translation 23-19
 - high-density ports 19-9
 - link mode configuration 19-9
 - LLC translation 23-22
 - older Fast Ethernet 19-18
 - OmniChannel 19-1
 - path MTU discovery 30-42
 - port mapping 24-74
 - port mirroring 24-65
 - port monitoring 24-69
 - SNAP translation 23-20
 - Ethernet 10/100 ports 19-10
 - auto-negotiation 19-10
 - configuring 19-7
 - Ethernet management port
 - configuring 10-5
 - MPM-C 40-27
 - MPM-III 6-10
 - MPX 2-5
 - redundancy 10-7
 - Ethernet modules 3-16, 3-25, 3-31, 7-17, 7-28, 7-36, 7-100
 - configuring tests 58-31
 - displaying switch statistics 23-30
 - ESM-100C 7-101
 - ESM-100C-12 7-18
 - ESM-100C-32W 7-28
 - ESM-100C-5 7-109
 - ESM-100C-FD 7-105
 - ESM-100CFx-5 7-112
 - ESM-100FM/FS-8 7-20
 - ESM-100Fx-FD 7-107
 - ESM-C-8 7-91
 - ESM-C-12 7-89
 - ESM-C-16 7-22
 - ESM-C-32W 7-24
 - ESM-F-8 7-93
 - ESM-F-16 7-26
 - ESM-T-12 7-95
 - ESM-T-24W 7-31
 - ESM-U-6 7-97
 - ESX-100C-12W 3-16
 - ESX-100C-32W 3-19
 - ESX-100FM/FS-12W 3-25
 - ESX-FM-24W 3-31
 - ESX-K-100C-32W 3-22
 - ESX-K-100FM/FS-16W 3-28
 - optimized ports 19-5
 - pinouts 3-16, 7-17
 - port partitioning 19-5
 - three generations 19-2
- ethernetc** command 10-5
- event 18-3
- events** command 18-5
- Explicit Forward Congestion Indication (EFCI) 41-12, 42-40

F

- facility datalink 53-6
- Fast Ethernet 20-1
 - configuring 19-10, 19-19
- Fast Spanning Tree
 - description 22-34
 - displaying port parameters 22-36
 - enabling port parameters 22-38, 22-39
- FCC Class B 5-17
- FCSM
 - virtual channels 33-35
- FCSM I 40-19
 - PNNI frame size guidelines 46-96
 - redundancy 40-19
- FCSM II 40-22
 - 1483 scaling services 36-17
- FCSM module 40-15, 40-17
 - LAN-to-ATM internetworking 40-19
 - logical ports on 33-5, 40-17
- FCSM ports
 - cell errors 33-47
 - configuring 33-8
 - statistics 33-45, 33-46, 33-50
 - viewing 33-26
- FDDI
 - default translations 23-17, 23-26
 - LLC translation 23-22
 - SNAP translation 23-20
- FDDI raw 23-26
- fddidef** command 23-26
- FECN 49-12
- FERF 54-18, 54-19, 54-27
 - LED 7-44
- fiber optic
 - power budgets 3-43, 3-46, 3-49, 3-53, 7-26, 7-43, 7-48, 7-51, 7-66, 7-78, 7-93
 - proper handling of cables 3-5
- file** command 8-19, 11-1
- files 2-7, 6-11
 - configuration 11-2
 - flash memory 11-3
 - image 2-7, 6-11, 40-28
 - PGA 6-11
- Filter Command. See UI Table Filtering
- filter points 12-7
- flash memory 2-7, 6-1, 6-11, 40-28
- flc** command 22-21
- flood limits 24-34
 - configuring 22-21
 - displaying 22-22
- fls** command 22-22
- fping** command 30-23
- fr** command 49-20
- FR/ATM Internetworking 38-1
 - commands 38-21
 - creating an FR/ATM IWF 38-23
 - deleting an FR/ATM IWF 38-35
 - deleting FR/ATM PVCs 38-36
 - disabling 38-20
 - displaying FR/ATM configurations 38-37
 - displaying FR/ATM statistics 38-42
 - displaying the status 38-20
 - enabling 38-20
 - enabling an FR/ATM IWF 38-27
 - FCSM-II 38-15
 - FRF.5 38-2
 - FRF.8 38-9
 - hardware supported 38-1
 - loading the image file dynamically 38-19
 - modifying an FR/ATM IWF 38-28
 - overview 38-2
- fradd** command 49-31
- frame flooding 27-15
- Frame Relay
 - back-to-back configurations 49-3
 - BECN 49-11
 - bridging 49-14, 49-54
 - cables 49-4, B-1
 - CIR 49-8
 - compression 49-5
 - congestion control 49-8
 - control signals 49-44
 - Discard Eligibility 49-9
 - DLCI 49-6
 - DLCMI 49-23
 - errors 49-46
 - FECN 49-12
 - IP routing 49-15
 - IPX routing 49-18
 - polling 49-24
 - port configuration 49-21
 - Routing Group 49-56
 - self-configuration 49-7
 - split clocking 34-26, 49-39
 - statistics 49-37
 - translations 49-13
 - trunking 49-19, 49-59

- viewing parameters 49-32
- Virtual Circuit 49-6, 49-14
- Virtual Circuit configuration 49-31
- virtual ports 49-14
- Frame Relay boards
 - ipxsap** command with, 32-11
- frame relay DLCI 56-60, 56-61
- framefab** command 58-3, 58-35
- Frame-to-Cell modules
 - FCSM I 40-19
 - FCSM I redundancy 40-19
 - FCSM II 40-22
- fratm** command 38-20
- frclear** command 49-51
- frdelete** command 49-35
- frmodify** command 49-21
- frs** command 38-21
- frscvc** command 38-23
- frsdc** command 38-35
- frsdvc** command 38-36
- frsmc** command 38-28
- frsmvc** command 38-27
- frstatus** command 49-37
- frsvc** command 38-37
- frsvs** command 38-42
- frview** command 49-32
- fsck** command 11-14, 13-21
- fstps** command 22-36
- FTP
 - commands 9-3
- FTP client 9-1
- ftp** command 9-3
- FTP commands
 - ? 9-3
 - ascii 9-3
 - binary 9-3
 - bye 9-3
 - cd 9-3
 - delete 9-3
 - dir 9-3
 - get 9-3
 - hash 9-3
 - lpwd 9-3
 - ls 9-3
 - put 9-3
 - pwd 9-3
 - quit 9-3
 - remotehelp 9-3
 - user 9-3
- FTP servers 9-1, 9-2

- full-duplex 7-109, 7-112
 - Fast Ethernet 19-18
- fuses
 - spare 5-27
- fwtlv** command 25-26, 27-30

G

- Generic Cell Rate Algorithm (GCRA) 40-2, 41-19, 42-55
- generic service relays 31-19
- Giga I ASIC 20-7
- Giga II ASIC 20-7
- Gigabit 20-1, 20-7, 20-12
- Gigabit Ethernet modules 3-7, 7-17
 - GSM-FH-2W 7-33
 - GSM-FM-2W 7-33
 - GSM-FS-2W 7-33
 - GSX-FM/FS/FH-2W 3-7
 - GSX-FM/FS-4W 3-13
 - GSX-K-FM/FS/FH-2W 3-10
- global commands 12-18
- global commands** 12-18
- GMAP
 - configuring 26-11
 - gap time 26-11
 - update time 26-12
- gmappuptime** command 26-11
- gmapholdtime** command 26-12
- gmapls** command 26-13
- gmapst** command 26-11
- gmapupptime** command 26-12
- gmcfg** command 24-12, 27-2
- gmstat** command 27-2
- gp** command 24-20, 24-46
- Group 24-1
 - 1483 routed format services 24-44
 - authenticated 24-1, 24-30
 - changing parameters 24-48
 - CIP 24-22, 24-42
 - creating 24-21
 - deleting 24-51
 - flood limits 22-22
 - IP address 24-24
 - IP routing in 24-24
 - mobile 24-1, 24-5, 24-30
 - non-mobile 24-1, 24-18
 - port assignment to 24-2
 - viewing 24-46

WAN routing 24-22, 24-39
 Group Mobility 24-2
 enabling switch-wide 24-12
 Group multiplexing 36-9
 GSM-FH-2W 7-33
 GSM-FM-2W 7-33
 GSM-FS-2W 7-33
 GSX-FM/FS/FH-2W 3-7
 GSX-FM/FS-4W 3-13
 GSX-K-FM/FS/FH-2W 3-10

H

half-duplex
 Fast Ethernet 19-18
 hardware
 mounting 4-11, 4-13, 4-15, 4-17
 hardware diagnostics 58-1
hdcfg command 15-2
hdstat command 15-6, 15-7
 Health MIB 15-1
 management menu 15-1
 resource thresholds 15-2
 Hello messages
 and XMAP 26-2
 defined 46-15
 exchanges 46-21
 states 46-66
 timers 46-60
help command 8-19
history command 8-30
hmstat command 15-7
 hop reduction
 by VP tunneling 42-25
 hot swapping 1-11, 1-14, 4-4, 4-7, 4-10, 4-11,
 4-13, 4-15, 4-17, 4-19, 4-21, 5-1, 5-5, 5-6,
 5-7, 5-8, 5-9, 5-10, 5-11, 7-10
hpstat command 15-8
 HRE 6-2, 6-17
 HRE-Plus 6-17
hreset command 15-8
 HRE-VX 6-18
 router register limitations 6-18
 HRE-X 1-26
 router register limitations 1-27
 valid configurations 1-27
hrex command 13-27
hrexassign command 13-28
hrexdisplay command 13-27

hrexhashopt command 13-29
hrexutil command 13-29
 HSM 7-13

I

ib command 11-9
 IBM 8230 21-22
 IBM 8272 21-22
 ICMP protocol 30-3
 ICMP statistics and errors 30-20
icmps command 30-20
igpa command 43-15
igpclc command 43-67
igpd command 43-32
igplcs command 43-55
igplis command 43-56
igplts command 43-54
igpm command 43-21
igpmem command 43-18
igprat command 43-32
igps command 43-35
igpsts command 43-48
igptestb command 43-29
igpteste command 43-31
 IISP - see Interim Inter-Switch Signalling
 Protocol (IISP)
 IISP routes 47-3
ilkcls command 43-67
ilkcls command 43-63, 43-64
ilkits command 43-60
ilkm command 43-28
ilks command 43-44
ilksts command 43-57
 IMA 43-1
 adding links 43-18
 application example 43-8
 clearing group statistics 43-67
 clearing link statistics 43-67
 conducting tests 43-29
 configuring 43-3, 43-15
 configuring link parameters 43-28
 CSM ports 43-5, 43-19
 deleting groups 43-32
 filler cells 43-4
 group performance statistics 43-54, 43-55,
 43-56
 group statistics 43-48
 group summary status 43-35

- groups 43-4
- ICP cells 43-4
- link performance statistics 43-60, 43-63, 43-64
- Link State Machine (LSM) 43-11
- link statistics 43-57
- link summary status 43-44
- links 43-4
 - modifying groups 43-21
 - modifying links 43-20
 - restarting a group 43-32
 - stuff cells 43-4
 - synchronization 43-12
 - troubleshooting 43-68
- User Interface commands 43-13
- ima** command 43-13
- image files 2-7, 3-3, 6-11, 7-4, 11-3, 40-3, 40-28
- imcd** command 42-61
- imce** command 42-59
- imci** command 42-60
- imcr** command 42-59
- imgcl** command 11-5
- imgsync** command 10-16
- info** command 13-6
- ingress cache table 37-19
- Integrated Local Management Interface (ILMI) 33-9, 33-27, 41-69, 46-19
 - LANE 42-36
- intelligent multicast replication 42-56
 - disabling 42-59
 - displaying performance gain 42-60
 - displaying tree depth 42-61
 - enabling 42-59
 - performance gain 42-56, 42-60
 - replication trees 42-58
 - supported on OC-3 modules 42-57
 - tree depth 42-58, 42-61
- interface** command 8-19
- Interim Inter-Switch Signalling Protocol (IISP) 41-31, 41-59, 42-27, 46-1, 46-5, 46-29, 47-1
 - E.164 addresses 47-4
 - route addresses 47-9
 - transit networks 47-6
 - virtual path tunnels 47-3
- Interswitch Protocols (XIP) 26-1
 - submenu 26-1
- Inverse ARP 49-15
- Inverse Multiplexing over ATM (IMA) - See IMA
- IP
 - abbreviated address format 8-32
 - address 9-2
 - BOOTP relay 31-4
 - DHCP 31-4
 - framing type 24-26
 - problems with 57-7
 - RIP mode 24-25
- IP address
 - changing in group 24-49
- ip** command 30-7
- IP protocol 30-3
- IP RIP Filters
 - adding "global" filters 30-33
 - adding specific filters 30-34
 - configuring 30-33
 - deleting filters 30-36
 - displaying all filters 30-37
 - displaying global filters 30-38
 - displaying specific filters 30-38
 - filter precedence 30-35
- IP Routing 24-24
 - adding an IP address to ARP table 30-9
 - adding IP static routes 30-17
 - Address Resolution Protocol 30-3
 - flushing the RIP Routing Table 30-32
 - Internet Control Message Protocol 30-3
 - Internet Protocol 30-3
 - Open Shortest Path First Protocol 30-2
 - PING command 30-22
 - PINGing a host 30-22
 - removing IP static routes 30-19
 - Routing Information Protocol 30-2
 - Simple Network Management Protocol 30-3
 - TELNET protocol 30-3
 - tracing an IP route 30-31
 - Transmission Control Protocol 30-3
 - User Datagram Protocol 30-3
 - viewing ICMP statistics and errors 30-20
 - viewing IP statistics and errors 30-12
 - viewing RIP statistics and errors 30-26
 - viewing TCP statistics 30-27
 - viewing the Address Translation Table 30-8
 - viewing the IP routing table 30-15
 - viewing the IP-to-MAC Table 30-39
 - viewing the TCP Connection Table 30-29

- viewing the UDP listener table 30-25
 - viewing UDP statistics and errors 30-24
 - ipdirbcst** command 30-41
 - ipf** command 30-37
 - ipmac** command 30-39
 - ipr** command 30-15
 - ips** command 30-12
 - IP-to-MAC Table
 - displaying all entries 30-39
 - displaying specific entries 30-40
 - flushing entries 30-40
 - IPX
 - address mapping 23-9
 - routing over ATM 24-43, 24-45
 - Token Ring 23-14
 - triggered RIP and SAP 24-41
 - VLANs 29-4, 29-7
 - ipx** command 32-4
 - IPX RIP
 - description of protocol 32-2
 - IPX RIP/SAP Filtering
 - adding global filters 32-19
 - adding specific filters 32-20
 - configuring NetWare for WAN links 32-33
 - default setting of filters 32-18
 - deleting filters 32-22
 - displaying all filters 32-23
 - displaying global filters 32-24
 - displaying specific filters 32-24
 - filter precedence 32-25
 - uses for filters 32-18
 - IPX routing
 - adding an IPX static route 32-12
 - configuring IPX Serialization Packet Filtering 32-26
 - configuring IPX Watchdog Spoofing 32-28
 - configuring NetWare for WAN links 32-33
 - configuring SPX Keepalive Spoofing 32-30
 - disabling IPX Router Complex 32-14
 - displaying IPX Routing Table 32-5
 - enabling IPX Router Complex 32-14
 - flushing RIP/SAP tables 32-15
 - GNS Output filters 32-18
 - PINGing an IPX node 32-16
 - removing IPX static routes 32-13
 - RIP Input filters 32-18
 - RIP Output filters 32-18
 - RIP/SAP Filters
 - configuring 32-18
 - SAP Input filters 32-18
 - SAP Output filters 32-18
 - the IPX submenu 32-4
 - viewing IPX statistics 32-8
 - viewing SAP Bindery 32-10
 - IPX Serialization Packet Filtering
 - configuring 32-26
 - IPX static routes
 - removing 32-13
 - IPX Watchdog Spoofing
 - configuring 32-28
 - ipxdrt** command 32-38
 - ipxext** command 32-37
 - ipxf** command 32-23
 - ipxfilter** command 32-19
 - ipxflush** command 32-15
 - ipxoff** command 32-14
 - ipxping** command 32-16
 - ipxr** command 32-5
 - ipxs** command 32-8
 - ipxsap** command 32-10
 - ipxserialf** command 32-26
 - ipxspool** 32-28
 - ipxt** command 32-36
 - ipxtimer** command 32-35
 - ISDN
 - Basic Rate Interface (BRI) 48-4
 - isdn** command 52-3
 - ISDN Ports
 - accessing the ISDN menu 52-3
 - deleting an ISDN configuration entry 52-5
 - displaying ISDN configuration entry status 52-7
 - modifying an ISDN configuration entry 52-4
 - viewing an ISDN configuration entry 52-6
 - isdnd** command 52-5
 - isdnm** command 52-4
 - isdns** command 52-7
 - isdnv** command 52-6
 - iupgfpa** command 43-33
- ## K
- kill** command 8-39
 - Kodiak Ethernet Modules 19-5

L

- LAN Emulation (LANE) 36-4, 36-26, 36-67, 37-6
 - back-off timers 36-7
 - BUS 36-65
 - default translations 23-18
 - dynamic 24-5
 - Ethertype translation 23-19, 23-23
 - LECS 36-65
 - LES 36-65
 - SNAP translation 23-21
 - Token Ring 36-5
- LAN Emulation Clients, see LEC
- LANE Service Menu (LSM) 35-4
- layer 3 forwarding engine 37-4
- lb** command 11-8
- LE_ARP table 36-67
- leak monitor 13-19
- leakdumpall** command 13-19
- leakstart** command 13-19
- Leaky Bucket 40-2, 41-19, 41-22, 42-55
 - dual 41-21
- learning 23-40
- LEC
 - Token Ring 36-5, 36-67
- LECS
 - adding ELANs 35-17
 - adding policies to ELANs 35-20
 - ATM address 42-36
 - creating 35-13
 - displaying ELANs 35-42
 - displaying policies assigned to an ELAN 35-43
 - displaying statistics 35-39
 - displaying the configuration 35-41
 - displaying the status 35-38
 - Well-Known Address 42-36
- LEDs 7-16
 - amber 57-9, 57-10
 - OK2 57-9
 - STA 57-10
 - TEMP 57-10
- LES/BUS Pair
 - configuration overview 35-5
 - creating 35-7, 35-8
 - displaying LE Client information 35-36
 - displaying registered MAC addresses 35-34
 - displaying statistics 35-26
 - displaying the configuration 35-32
 - displaying the registered route descriptor 35-35
 - displaying the status 35-24
- Line Interface Unit (LIU) 53-5, 53-9
- Line Layer 39-4
- link** command 51-2
- linkadd** command 51-3, 51-4
- linkdelete** command 51-11
- linkmodify** command 51-9
- linkstatus** command 51-15
- linkview** command 51-12
- LLC 23-6, 23-22
- load** command 9-4
- loadfrmi** command 38-19
- logical port
 - clear channel 56-36
 - configuration 56-33, 56-36
 - configuration and statistics 56-40
 - protocol configuration 56-43, 56-46
 - protocol configuration and statistics 56-50, 56-54
 - statistics and errors 56-42, 56-59
- login accounts 8-37, 12-2
- login alert banner 8-35
- logout** command 8-20
- lookup** command 8-29
- lpadd** command 56-33
- lpcls** command 56-42
- lpdel** command 56-39
- lpfradd** command 56-60
- lpfrdel** command 56-61
- lpmod** command 56-36
- lppcls** command 56-59
- lppmod** command 56-43, 56-46
- lppview** command 56-50, 56-54
- lpview** command 56-40
- ls** command 9-4, 11-3
- lslb** command 35-23
- lsmcfg** command 35-5
- lvpt** command 42-30, 42-32, 47-3, 47-8, 47-11

M

- m013** command 56-10
- M013 module
 - application examples 56-4
 - configuration 56-70
 - configuration overview 56-8
 - DS1 channel 56-24
 - DS1 channel configuration and statistical parameters 56-32
 - DS1 channel statistics and errors 56-26, 56-28, 56-29, 56-31
 - DS3 port 56-14
 - DS3 port statistical parameters 56-22
 - DS3 port statistics and errors 56-19, 56-20
 - DS3 port statistics and errors 56-17
 - frame relay DLCI 56-60, 56-61
 - logical configuration 56-12
 - logical port 56-39
 - logical port configuration 56-33, 56-36
 - logical port configuration and statistics 56-40
 - logical port protocol configuration 56-43, 56-46
 - logical port protocol configuration and statistics 56-50, 56-54
 - logical port statistics and errors 56-42, 56-59
 - management menu 56-10
 - physical configuration 56-11
 - router interface configurations 56-63
 - router interfaces 56-62, 56-64
 - service configuration 56-67, 56-69
 - services 56-65, 56-67
 - supported physical interfaces 56-3
 - technical specifications 56-6
- m013cas** command 56-65
- m013cfgdel** command 56-70
- m013das** command 56-67
- m013mas** command 56-69
- m013vas** command 56-67
- MAC 22-16, 22-17
- MAC addresses
 - configuring 18-6
 - restoring 18-6
- MAC devices
 - VLAN membership 25-26, 27-30
- main menu 8-19
- Mammoth 19-2
- map** command 33-8, 33-46
 - CSM ports 41-29
 - IISP ports 47-1
 - VPI bits 47-4
- mas** command 20-14, 36-49
 - 1483 routed format services 36-59
 - 1483 scaling services 36-57
 - ATM Trunking 36-50
 - Classical IP 36-51
 - Frame Relay 49-62
 - LAN Emulation 36-49
 - PTOP Bridging 36-54
 - VLAN Clusters 36-55
- maskta** command 58-7
- masrt** command 42-36
- Maximum Burst Size (MBS) 33-21, 41-43, 42-12
 - ASM2 and ASX modules 33-69
- mbwg** command 33-68
- mclk** command 45-10
- mcvl** command 28-13
- MD5 16-4
- media access control - see MAC
- Medium Layer 39-4
- memory management 13-20
- memory threshold 15-5
- memory utilization statistics 13-19
- memstat** command 13-20
- Mobile Groups 24-1, 24-5
 - aging out devices 24-12
 - AutoTracker policies 24-38
 - configuring 24-30
 - def_group 24-12
 - default group 24-12
 - dynamic LANE 24-16
 - dynamic port assignment 24-5
 - Ethernet and Token Ring ports 24-2
 - move_from_def 24-13
 - move_to_def 24-12
 - multiple 24-2
 - policies 25-1, 25-24
 - ports in 24-5
 - primary group 24-13
 - static port assignment 24-5
 - viewing 25-23
- modatvl** command 25-6, 25-7, 25-21, 25-22, 27-24
- modem port 6-7, 10-3
- modmcvl** command 28-9, 28-12
- modules
 - removing 7-9

- modvl** command 24-25, 24-48, 27-4, 27-19
- modvp** command 13-32, 24-53, 24-68
 - translations 23-16
- move_from_def** variable 24-13
 - set in `mpm.cmd` 24-13
- move_to_def** variable 24-12
- MPC 37-4
- MPC components 37-4
- mpccfg** command 37-10, 37-11
- MPM 4-3, 5-18
 - Boot prompt configuration A-10
 - file corruption 6-4
 - hot swap warning 6-4
 - OK1 LED 6-4
 - OK2 LED 6-4
 - power down warning 6-4
- mpm** command 10-9
- MPM Module 4-1, 4-4, 4-11, 4-13, 4-15, 4-17, 6-1, 6-3, 6-11, 6-15
 - configuring 10-1
 - LEDs 57-9
 - redundancy 10-9
 - resetting a secondary 10-19
- MPM-1G 4-3, 4-7, 5-18, 6-2, 6-3
 - Boot prompt configuration A-10
- MPM-1GW 4-5
- MPM-C 6-2, 6-3, 40-23, 40-28
 - ATM services 40-29
 - Boot prompt configuration A-7
 - Ethernet management port 40-27
 - file corruption 6-5, 40-25
 - hot swap warning 6-5, 40-25
 - OK1 LED 6-5, 40-25
 - OK2 LED 6-5, 40-25
 - power down warning 6-5, 40-25
 - redundancy 40-28
 - serial ports 40-28
 - wide chassis required 40-23
- mpmget** command 10-17
- MPM-II 4-3, 5-18, 6-1, 6-3
 - Boot prompt configuration A-10
- MPM-III 6-2, 6-3, 6-6
 - Boot prompt configuration A-7
 - Ethernet management port 6-10
- mpmload** command 10-12
- mpmreplace** command 10-12
- mpmrm** command 10-13
- mpmstore** command 10-11
- MPOA 37-1
 - configuring a client 37-11
 - egress cache table 37-20
 - functionality 37-1
 - ingress cache table 37-19
 - management menu 37-10
 - requirements 37-4
 - viewing client status 37-14
 - viewing servers 37-21
 - viewing statistics 37-15
- MPOA Client, see MPC
- MPOA Network 37-8
- MPOA Server, see MPS
- MPS 37-5
- MPS components 37-5
- MPX 1-10, 1-13, 2-7
 - Boot prompt configuration A-7
 - configuring 10-1
 - file corruption 2-2
 - hot swap warning 2-2
 - OK1 LED 2-2
 - OK2 LED 2-2
 - power down warning 2-2
 - redundancy 2-9
 - resetting a secondary 10-19
- MTU 30-42
- multicast claiming 13-32
- Multicast VLANs 27-1, 28-1
 - creating 28-4
 - deleting 28-11
 - device assignment in 28-2
 - frame flooding in 28-3
 - modifying 28-9
 - multicast addresses 28-6
 - multicast claiming, compared 28-2
 - policies 28-12
 - recipients 28-1, 28-7
 - viewing 28-13
- multiple spanning tree 20-4
- multiple user sessions 8-37
- Multi-Protocol Over ATM, see MPOA
- mux
 - virtual path 42-25
- mva** command 33-25
- mvc** command 33-22, 41-53
- mvpt** command 42-35

N

- names** command 18-1
- nb** command 11-10
- net** command 55-2
- NetBIOS relays 31-11
- network address policy 27-7
 - precedence 25-2
- Network Time Protocol 16-1
- networking** command 8-19, 30-6
- newfs** command 11-15, 13-22
- Next Hop Clients, see NHC
- Next Hop Resolution Protocol, see NHRP
- Next Hop Server, see NHS 37-5
- NHC 37-6
- NHRP 37-6
- nisuf** command 10-14
- NoCLPNoSCR 33-20, 41-41, 42-9
- NoCLPSCR 33-20, 41-42, 42-10
- noecho** command 8-35
- non-Ethernet ports 24-32
- Non-mobile Groups 24-1, 24-18
- ntaccess** command 16-5, 16-36
- ntadmin** command 16-5, 16-33
- ntconfig** command 16-5
- ntinfo** command 16-5, 16-15
- NTP
 - advertised precision 16-14
 - client/server 16-8
 - client/server authentication 16-9
 - current leap second 16-30
 - event timer subsystem 16-28
 - I/O subsystem 16-27
 - key ID 16-34
 - key type 16-35
 - list of peers 16-15
 - local server information 16-21
 - local server statistics 16-23
 - loop filter information 16-26
 - packet count statistics 16-29
 - peer associations 16-12, 16-14
 - peer memory usage 16-26
 - peer summary information 16-16
 - primary receive timeout 16-33
 - reset subsystem counters 16-28
 - server statistics 16-24
 - specify password 16-34
 - system flag 16-35
 - trusted list 16-37
 - version number 16-20
- ntpaddpeer** command 16-12
- ntpaddserv** command 16-13
- ntpauth** command 16-38
- ntpbcast** command 16-13
- ntpckey** command 16-37
- ntpcres** command 16-39
- ntpctlk** command 16-37
- ntpctlstat** command 16-29
- ntpctrap** command 16-41
- ntpdelay** command 16-33
- ntpdisable** command 16-35
- ntpdkey** command 16-38
- ntpdres** command 16-41
- ntpdtrap** command 16-42
- ntpenable** command 16-35
- ntpiconfig** command 16-6, 16-8
- ntpinfo** command 16-21
- ntpio** command 16-27
- ntpkeyid** command 16-34
- ntpkeytype** command 16-35
- ntpleap** command 16-30
- ntploop** command 16-26
- ntplpeers** command 16-15
- ntpmem** command 16-26
- ntplmst** command 16-31
- ntpmmon** command 16-31
- ntpmres** command 16-41
- ntppasswd** command 16-34
- ntppeers** command 16-16
- ntpprec** command 16-14
- ntppreset** command 16-28
- ntppstat** command 16-24
- ntpreqk** command 16-36
- ntppreset** command 16-28
- ntpshowpeer** command 16-18
- ntpstat** command 16-23
- ntptimeo** command 16-33
- ntptimer** command 16-28
- ntpunconfig** command 16-14
- ntpvvers** command 16-20
- ntpvkey** command 16-37
- ntpvres** command 16-40
- ntpvtrap** command 16-42
- ntstats** command 16-5, 16-23

O

OC-12 3-48, 3-51, 7-53, 7-56
OC-3 3-40, 3-42, 3-45, 7-36, 7-42, 7-47, 7-50
OK2 LED 57-9
Omni Switch/Router 1-1, 2-7
 HRE-X 1-26
 - see also OmniS/R
Omni-3wx 4-2, 4-3, 4-5
Omni-5 4-11, 4-15
Omni-5e 4-3, 4-15
Omni-5wx 4-2, 4-7, 4-11, 4-15, 4-19
Omni-5x 4-2, 4-19
Omni-9 4-13, 4-17
Omni-9wx 4-2, 4-9, 4-13, 4-17, 4-21
Omni-9wxp 4-10
Omni-9wx-PLUS 4-10
Omni-9x 4-2, 4-3, 4-21
OmniChannel 19-1, 19-11
 creating 19-13
 Ethernet 19-11
 ports 19-15
 primary/secondary ports 19-16
OmniS/R 1-1
 DHCP 31-4
OmniS/R-3 1-8
OmniS/R-5 1-10
OmniS/R-9 1-13
OmniS/R-9P 1-13
OmniSwitch 4-1, 6-11, 7-1, 24-1, 40-28
 as ATM switch 40-1, 40-8, 40-14
 as hybrid switch 40-1, 40-7, 40-13
 as LAN switch 33-6, 40-1, 40-6, 40-12
 DHCP 31-4
optimized bridge mode 24-32
Optimized Ports
 ESM/ESX-K Series Modules 19-5
OSPF protocol 30-2
output translations 23-41

P

padj command 46-73
Partial Packet Discard (PPD) 40-2
partition management 12-11, 12-19
password 8-37, 12-2
 changing 12-2
Path Layer 39-3
path MTU discovery 30-42

pbstats command 46-85
PBX
 in circuit emulation 34-4
pcalls command 46-83
pdtl command 46-84
 summary form 46-84
Peak Cell Rate (PCR) 33-20, 41-43, 42-12
 ASM2 and ASX modules 33-68
Peer Group
 ID 46-13
 multiple 46-7
 single 46-6
pestats command 46-86
PGA files 6-11
pgcfg command 46-32
pginfo command 46-53
phalt command 46-88
Phase-Lock Loop 45-2
Physical Layer Convergence Protocol (PLCP)
 54-23, 54-32, 54-33
ping command 30-22
pinouts
 Ethernet modules 3-16
 Token Ring modules 3-34
 WAN modules 3-61
PLCP 3-55, 3-58, 7-59, 7-62, 7-68, 7-71, 40-57,
 45-3, 54-23, 54-32, 54-33
plink command 46-66
 summary form 46-68
pmap command 46-77
 diagram 46-79
 summary form 46-78
pmapcr command 24-20
pmapdel command 24-20
pmapmod command 24-20
pmapv command 24-20
pmcfg command 24-70
pmdelete command 24-72
pmon command 24-71
pmpause command 24-72
pmstat command 24-73
PMTU 30-42
pnbrs command 46-62
 summary form 46-63
pncfg command 46-40
pninfo command 46-56
pnmap command 46-80
 summary form 46-82
PNNI - See Private Network-to-Network
 Interface (PNNI)

- PNNI node
 - ATM address 46-56, 46-57
 - ID 46-56
 - node level 46-41, 46-57
- PNNI route addresses
 - configuring 47-9
 - viewing 47-15
- PNNI route properties
 - configuring 47-3
 - deleting 47-8
 - viewing 47-13
- PNNI static route addresses
 - deleting 47-11
- PNNI static routes
 - administrative weight 47-5
 - attributes 47-18
 - Cell Delay Variation (CDV) 47-5
 - Cell Transmit Delay (CTD) 47-5
 - configuring 47-3
 - metrics 47-18
 - reachable addresses 47-6, 47-15
 - route addresses 47-9
 - route property 47-3
 - scope 47-4
 - to nodes 47-17
 - Transit networks 47-6
- PNNI statistics
 - error 46-86
 - port 46-85
 - PTSE 46-87
- PNNI Topology State Elements (PTSEs)
 - 46-21, 46-53, 46-87
 - database 46-69
 - statistics 46-87
 - timers 46-43, 46-60
- PNNI Topology State Packets (PTSPs)
 - timer 46-43, 46-61
- Point to Multipoint connections on switch
 - viewing 41-100
- point-to-multipoint
 - ATM virtual circuits 41-38
 - intelligent multicast replication 42-56
- Point-to-Point Protocol (PPP)
 - accessing the PPP menu 50-6
 - adding a PPP entity 50-9
 - deleting a PPP entity 50-20
 - displaying PPP entity status 50-17
 - modifying a PPP entity 50-14
 - setting global parameters 50-7
 - viewing PPP entity configurations 50-15
- policies
 - AutoTracker 25-1
 - configuring 25-4
 - DHCP 25-29
 - DHCP example 25-27
 - DHCP MAC address 25-3
 - DHCP port 25-3
 - IP 27-7
 - IPX 27-7
 - MAC address 25-2
 - network address 25-2, 27-7
 - port 25-2, 27-9
 - port binding 25-2
 - protocol 25-2
 - user-defined 25-2
- port connection statistics
 - displaying for CSMS 42-51
- port mapping 24-20
 - example 24-74
 - operation of 24-75
 - relationship to policies 24-74
 - subset of ports 24-75
- port mirroring 24-36, 24-65
 - disabling 24-68
 - enabling 24-68
 - operation of 24-65
 - RMON probe 24-66
- port monitoring 24-69
 - menu 24-69
 - starting a session 24-71
 - statistics 24-73
- port monitoring resources 24-70
- Port partitioning
 - Ethernet modules 19-5
- port policies 27-9
 - backbone connections 27-12
 - inactive VLANs 27-12
 - silent stations 27-12
 - usefulness 27-12
 - with VAP 26-9
- Port switching 21-33
 - deleting mapped ports 21-38
 - mapping between Token Ring Ports 21-36
 - mapping ports 21-35
 - mapping to ATM PTOPT PVC Service 21-36
 - services supported by 21-35, 21-36
 - support for 21-33
 - viewing mapped ports 21-37

- port tests 58-13
 - cabling 58-39
 - cabling requirements 58-14, 58-22, 58-23
- ports 24-58
 - assignment to Group 24-2
 - Frame Relay 49-1
 - information 24-58
 - optimized (Ethernet modules) 19-5
 - spanning tree 22-30
 - statistics 24-61
 - translations 23-29
- power cords 5-29
- power supply 1-8, 1-11, 1-14, 4-1, 4-5, 4-7, 4-10, 4-11, 4-13, 4-15, 4-17, 4-19, 4-21, 5-1, 5-3, 5-8
 - connecting a DC power source 1-28, 1-31, 5-23
 - installing 5-22
 - removing 5-22
 - replacing (9-slot chassis) 5-2
 - replacing fuse 5-27
- ppcfg** command 46-50
- ppinfo** command 46-13, 46-64
 - summary form 46-65
- ppp** command 50-6
- pppadd** command 50-9
- pppdelete** command 50-20
- pppglobal** command 50-7
- pppmodify** command 50-14
- pppstatus** command 50-17
- pppview** command 50-15
- ppstats** command 46-87
- pptse** command 46-69
- pradd** command 47-9
- prdel** command 47-8, 47-11
- preset** command 46-90
- prestart** command 46-89
- priority
 - ATM virtual circuits 41-45, 42-14
- Private Network-to-Network Interface (PNNI) 46-1
 - address summarization 46-41, 46-57
 - adjacencies 46-73
 - administrative submenu 46-30
 - administrative weight 46-16
 - alternate routing 46-26
 - ATM address 46-5
 - attributes 46-16
 - border nodes 46-7
 - CAC & Call Overbooking 46-2
 - Call Admission Control (CAC) 46-26
 - calls 46-83
 - Cell Delay Variation (CDV) 46-16, 46-34
 - Cell Transfer Delay (CTD) 46-16, 46-34
 - command help for Multiple-peer group
 - version 46-31
 - complex representation 46-10, 46-46
 - configuration information 46-91
 - configuring 46-1, 46-4
 - configuring multi-peer group operation 46-39
 - Connect message 46-27
 - connections diagram 46-79
 - crankback 46-26
 - database summary packets 46-15, 46-63, 46-85
 - default ATM node addresses 46-13
 - defined 46-1
 - Designated Transit List (DTL) 46-6, 46-24, 46-39, 46-54, 46-84
 - discards 46-86
 - E.164 addresses 47-4
 - errors 46-54, 46-86
 - establishing a connection 46-22
 - FCSM I guidelines 46-96
 - general information submenu 46-29
 - halting 46-88
 - Hello packets 46-15
 - hello protocol 46-20
 - Hello states 46-66
 - hello timers 46-44
 - hierarchy level 46-7
 - horizontal link inactive timer 46-47
 - image files 46-4
 - load balancing 46-2
 - logical group nodes 46-39, 46-46
 - map table 46-77
 - maximum nodes 46-36
 - maximum paths 46-37
 - menu 46-28
 - metrics 46-16
 - neighbor nodes 46-20
 - neighbor states 46-62, 46-64
 - network 46-6
 - network initialization 46-19
 - nodal map table 46-80
 - node 46-6
 - operations limits 46-35
 - parent ATM address 46-58
 - parent node ID 46-58

parent peer group ID 46-59
 parent peer group leader node ID 46-59
 path limitations 46-3
 path selection 46-24
 peer group 46-7, 46-57
 peer group ID 46-13
 peer group leader election 46-9, 46-48
 peer group leader priority 46-46, 46-58
 peer group leader state 46-58
 peer groups 46-6
 PNNI Topology State Elements (PTSEs)
 46-6, 46-15
 PNNI Topology State Packets (PTSPs)
 46-6, 46-15
 point-to-multipoint calls 46-54
 point-to-point calls 46-53
 port information 46-64
 port type 46-4
 preferred peer group leader 46-58
 PTSE statistics 46-87
 public networks 42-24
 redundancy 46-93
 resetting statistics 46-90
 restarting 46-89
 route addresses 47-1
 Route Management menu 47-2
 route properties 47-1
 Routing Control Channel (RCC) 46-39,
 46-51
 Setup Message 46-25
 Shortest Path First (SPF) algorithm 46-21,
 46-53
 static route prefixes 47-14
 static route submenu 46-29
 static routes 46-5, 47-1
 static routes and VP tunnels 47-3
 statistics 46-87
 statistics submenu 46-30
 summarization 46-3, 46-18, 46-23
 summary address 46-14, 46-41, 46-58
 summary form of commands 46-31
 Switched Virtual Circuit Channel
 Connection (SVCC) interval timer
 46-47
 topology database 46-6, 46-21, 46-23
 UI menus 46-28
 unusable links 46-79
 verifying routes 46-92
 viewing statistics 46-85, 46-86
prmcfg command 46-91

probes 18-3
probes command 18-4
proutea command 47-15
 summary form 47-16
prouten command 47-17, 47-18
prp command 47-13
prpadd command 47-1, 47-3
prt command 47-14
prtst command 46-92
prty_disp command 24-20
prty_mod command 24-20
psmap command 46-74
ptinfo command 46-60
 PTOp Bridging 36-36
pvcfg command 46-91
 PVCs 34-17, 40-1, 40-15
 ATM access 33-8
 configuring 33-15
 deleting 33-23, 41-53
 modifying 33-22, 41-53
 viewing 41-63
pw command 8-29, 12-2
pwd command 11-2

Q

Quality of Service (QoS) 40-2, 41-10
 ATM virtual circuits 41-40, 42-8
quit command 8-20

R

rb command 11-8
 reboot 12-3
 - see also boot
reboot command 12-3
 receive threshold 15-3
 redundancy
 FCSM I 40-19
 MPM 4-4, 4-7, 4-9, 4-11, 4-13, 4-15, 4-17,
 6-15, 10-9
 MPX 1-7, 1-10, 1-13, 2-9
 power supply 1-11, 1-14, 4-7, 4-10, 4-11,
 4-13, 4-15, 4-17, 4-19, 4-21, 5-1, 5-5, 5-6,
 5-7, 5-8, 5-9, 5-10, 5-11
 re-executing commands 8-30
 Reference Timing
 derived clock 45-2
 reg_port_rule variable 27-9

relayc command 31-2, 31-3
relays command 31-23
remote trunking stations 22-18
renounce command 10-14
res command 18-1
reset command 58-6
Resource Management 41-12
resource thresholds 15-2
riadd command 56-62
ridel command 56-63
RIF stripping
 and UDP relay 31-1
rimod command 56-63
Ring switching 21-31
 limitations 21-31
RIP protocol 30-2
ripflush command 30-32
rips command 30-26
ripxsr command 32-13
risr command 30-19
riview command 56-64
rm command 2-8, 6-14, 9-4, 11-4
rmatvl command 27-4, 27-26
rmgp command 24-51
rmmcvl command 28-11
RMON 18-3
rmvp command 24-54
router interface 56-62, 56-64
 configuration 56-63
routing 23-1
 default VLAN 29-8
 Frame Relay 49-56
Routing Control Channels (RCCs) 46-53

S

sampling interval 15-6
SAP
 description of protocol 32-2
SAP Bindery
 viewing the, 32-10
saveconfig command 13-33
SC connectors
 proper handling 3-5
SCR 33-69
scvc command 42-3, 42-15, 42-17, 42-18
SDH 39-1
Search Command. See UI Table Filtering
secapply command 12-7

secdefine command 12-4
seclog command 12-10, 14-13
secreset command 10-19
secs command 39-22
Section Layer 39-4
security 12-1
security command 8-19
sedm command 39-9
seds command 39-11
segment buffers
 relation to Virtual Circuits 33-11
Segmentation and Reassembly (SAR) 33-11
selgp command 22-7
ser command 6-8, 9-4, 10-2, 10-3
serial port
 connections 6-7
 DCE 6-7
 DTE 6-7
service configuration
 M013 module 56-67, 56-69
service registry table
 adding ATM addresses to 42-38
services 36-1
 Classical IP 36-12
 LAN Emulation 36-4
 M013 module 56-65, 56-67
 PTOP Bridging 36-14
 VLAN Clusters 36-56
services command 8-19, 36-20
Service-Specific Connection Oriented
 Protocol (SSCOP) 33-27, 41-69
ses command 39-7
sess command 39-24
Shortest Path First (SPF) algorithm 46-21
single spanning tree 20-4
SLIP 10-3, 57-10
slot command 2-9, 6-15, 13-14, 40-19, 40-21
slot table 13-14
sls command 10-11
smon command 39-5
SNAP 23-6, 23-20
SNMP protocol 30-3
SNMP statistics 17-8
SNMP traps 17-8
snmpc command 17-2
snmps command 17-8
soft PVCs 34-17, 41-7
 broadband bearer 42-18
 configuring 42-3
 deleting 41-53

- modifying 41-53
- point-to-multipoint 42-5, 42-15
- priority 42-4
- retries 42-18
- terminating ATM address 42-4
- viewing 42-21
- software
 - installation problems 57-5
 - switch 2-7, 6-11
- SONET 39-1
- sonet** command 39-6
- SONET error collection 39-1
 - clearing statistics 39-22
 - commands 39-6
 - disabling 39-5
 - displaying collection status 39-5
 - displaying error statistics tables 39-11
 - enabling 39-5, 39-7
 - intervals 39-3
 - Line Layer 39-4
 - Line Table statistics 39-14
 - LTE 39-4
 - Medium Layer 39-4, 39-9
 - Medium Layer Table statistics 39-9
 - Path Layer 39-3
 - Path Table statistics 39-15
 - protocol layers 39-3
 - PTE 39-4
 - Section Layer 39-4
 - Section Table Statistics 39-13
 - STE 39-4
 - summary statistics 39-24
- source routing 21-4, 21-8
 - and DHCP 31-5
 - hop count 21-4
 - parameters 21-15, 21-18
 - virtual rings 21-15
- Spanning Tree 22-28, 24-32
 - non-mobile group 24-19
 - parameters 22-25, 22-28, 22-32
 - ports 22-30
- Speedy Tree Protocol
 - description 22-35
- split clocking 48-28, 48-32
- SPVC 34-17
- SPX
 - description of protocol 32-2
- SPX Keepalive Spoofing
 - configuring 32-30
 - SPX-Packet tolerance counting 32-30
- spxspoof** 32-30
- srs** command 21-18
- SRTB 21-12
- SRTS clocking 34-8
- STA LED 57-10
- static bridge address 22-13
 - configuring 22-10
- static port assignment 24-2
- static routes
 - adding IP 30-17
 - removing IP 30-19
- statistics
 - module level 15-7
 - port level 15-8
 - port monitoring 24-73
 - resetting 15-8
 - switch level 15-6
- STATUS ENQUIRIES
 - Frame Relay 38-30, 49-7, 49-24, 49-25
- stc** command 22-25, 22-38, 22-39
- STM-1 39-1
- sts** command 22-28, 22-38, 22-39
- STS-1 39-1
- summarization 46-18
- summary** command 8-19, 13-1
- Sustainable Cell Rate 33-21, 41-43, 42-12
 - ASM2 and ASX modules 33-69
- SVCs 40-1, 40-15
 - ATM access 33-8
 - configuring a cell switch 41-46
- svvc** command 42-21
- swap** command 10-20
- swap on** command 40-19
- swch** command 23-29, 23-30
- switch
 - software 2-7, 6-11
- switch** command 8-19, 23-24
- switch menu 23-24
- switch software
 - Boot prompt 9-5
 - loading with FTP 9-2
 - loading with ZMODEM 9-4
- switching modules 2-7, 3-7, 3-16, 3-25, 3-31, 3-34, 3-40, 3-61, 4-1, 6-11, 7-1, 7-13, 7-17, 7-36, 7-74, 7-100, 40-28, 48-13, 48-18
 - disabling 58-6
 - fiber optic 3-42, 3-45, 3-48, 3-51, 7-26, 7-42, 7-47, 7-50, 7-53, 7-56, 7-93, 7-112
 - hot swapping 7-10

- installing 7-7
- power consumption 1-19, 1-20, 1-21, 1-22, 1-23, 1-24, 5-18, 5-19, 5-20, 5-21
- removing 7-9
- resetting 58-6
- swlogc** command 14-6
- syncctl** command 10-15
- synchronous clocking 34-8
- syscfg** command 13-2, 13-23
- syslog** command 14-2
- sysstat** command 13-15
- system boot A-2
 - commands 9-6
 - see also boot
- system** command 8-19, 13-5
- system description 13-23
- system info 11-13
- system menu 11-13, 13-5
- system prompt 8-22
- system statistics 13-15

T

T1

- fractional 48-4
- framing 53-2
- T1/E1 menu 53-3
- T1/E1 ports 34-17, 43-21, 53-1
 - alarms 53-11
 - configuring 31 timeslots on a WAN E1 port 48-53
 - Extended Superframe 53-2, 53-4
 - facility datalink 53-6
 - in circuit emulation 34-1, 34-4, 34-12, 34-23
 - line coding 53-5, 53-10
 - Line Interface Unit (LIU) 53-5, 53-9
 - loopback 43-23, 43-27, 53-7, 53-10
 - remote statistics 53-20
 - signaling 53-7, 53-10
 - statistics 53-17
 - Superframe 53-2, 53-4
 - yellow alarms 53-7, 53-14
- Table Filtering. See UI Table Filtering
- takeover** command 10-18
- task utilization statistics 13-17
- taskshow** command 13-17
- taskstat** command 13-17
- TCP protocol 30-3
- tcpc** command 30-29

- tcps** command 30-27
- te** command 53-3
- technical support 57-3
- telcs** command 53-18
- telis** command 53-19
- TELNET command
 - using 30-30
- telnet** command 30-30
- telts** command 53-17
- temod** command 53-4, 53-8
 - configuring a T1 port 53-4
 - configuring an E1 port 53-8
- TEMP LED 57-10
- temperature masking 58-7
- temperature sensor 13-15
- tercs** command 53-21
- teris** command 53-21
- terts** command 53-20
- tes** command 53-11, 53-13, 53-15
 - viewing a T1 port 53-13
 - viewing an E1 port 53-15
- test** command 58-8
- testcfg** command 58-30, 58-37
- testdisp** command 58-29
- time 13-8
- Time Division Multiplexing (TDM) 34-1
- time slot 53-2
- time zone 13-8
 - configuring 13-9
- Timing
 - local 45-3
 - loop 45-3
- tok** command 21-13
- Token Ring
 - Bytex hubs 21-22
 - copy bit stamping 21-11
 - default translations 23-18, 23-27
 - IBM hubs 21-22
 - LEC 36-5, 36-67
 - ODS 836J 21-22
 - port mirroring 24-65
 - port switching 21-33
 - ring switching 21-31
 - Synoptics hubs 21-22
- Token Ring modules 3-34, 7-74, 7-85
 - configuring tests 58-32
 - pinouts 3-34
 - TSM-C-6 7-76
 - TSM-CD-16W 7-85
 - LEDs 7-87

- TSM-CD-6 7-82
- TSM-F-6 7-78
- TSX-C-32W 3-35
- TSX-CD-16W 3-37
- Token Ring ports
 - configuring 21-24
 - mapping 21-35
- Token Ring switching
 - enabling/disabling 21-31
- tpcfg** command 3-35, 3-37, 7-82, 21-11, 21-24, 21-25, 21-27
- tperrs** command 21-46
- tpers** command 21-39
- tpvc** command 21-44
- traceroute** command 30-31
- traffic descriptor names 41-17
- Traffic Descriptors
 - Maximum Burst Size (MBS) 33-69, 41-16
 - Peak Cell Rate (PCR) 33-68, 33-70, 41-16
 - Sustainable Cell Rate (SCR) 33-69, 41-16
- Traffic Enforcement
 - congestion-based 41-18
 - static 41-18
- traffic shaping
 - ASM2 and ASX modules 33-60
 - bandwidth groups 33-60
 - configuration using the CLI 42-65
- Transit networks 47-6
- translations 23-1
 - ATM LANE 23-18
 - automatic 23-39
 - default options 23-16
 - Ethernet 23-17
 - Ethertype 23-19
 - FDDI 23-17
 - LLC 23-22
 - SNAP 23-20
 - Token Ring 23-18
- transmission states
 - XMAP 26-3
- transmit credit 24-34
- transmit/receive threshold 15-3
- traps
 - configuring 17-2
- trdef** command 23-27
- troubleshooting 57-1
- trportsw** command 21-33
- trsw** command 21-31

- Truncating Tree Timing
 - description 22-35
- tsc** command 7-82, 21-21, 21-41
- TSM-C-6 5-20, 7-76
- TSM-CD-16W 7-85
- TSM-CD-6 5-20, 7-82
- TSM-CD-6W 5-20
- tsmcfg** command 21-29, 21-30
- TSM-F-6 5-20, 7-78
 - fiber optic power budget 7-78
- tsmvc** command 21-42
- TSX-C-32W 3-35
- TSX-CD-16W 3-37

U

- UDP 30-3
- UDP relay 31-1
- udpl** command 30-25
- udps** command 30-24
- UI Table Filtering 8-42
 - Filter Command 8-45
 - combining Search Command with 8-46
 - more** mode and 8-42
 - Search Command 8-43
 - combining Filter Command with 8-46
 - more** mode and 8-42
 - renewing a search 8-44
 - wildcards and 8-48
- uic** command 8-21-8-28, 8-34, 11-1, 13-5
- Universal Serial Port 48-4
- Universal Time Coordinate (UTC) 13-8
- Unspecified Bit Rate (UBR) 41-9, 41-25, 46-38
- User Interface 8-1, 8-20
- user login 8-37, 12-2
- useradd** command 12-12
- userdel** command 12-20
- usermod** command 12-16, 12-20
- userview** command 12-12
- USP. See Universal Serial Port.
- UTC 13-8

V

VAP

- configuring 26-9
- databases 26-8
- relation to port policies 26-9

vap command 33-26, 41-63

Variable Bit Rate (VBR) 46-38

- non-real-time 41-8, 41-24
- real-time 41-8, 41-24

vas command 20-18, 36-62

- Frame Relay 49-61

vat command 36-70

vbwg command 33-70

VCI bits 41-30, 41-68

vclk command 45-8

vclka command 45-9

vcrs command 33-55, 42-54

vcs command 33-52, 33-53, 33-54, 42-46,
42-48, 42-49, 42-50

vcst command 42-51

vcts command 33-57

ve command 24-63

velan command 35-42

verbose 8-26

vgptovc command 36-72

vi command 23-23, 24-58

via command 24-55

viatrl command 25-24, 27-28

view command 11-6

vigl command 24-14

vimcrl command 28-14, 28-15

viqs command 20-19

virtual channel connection

- modifying 33-22, 33-25

Virtual Channel Identifier (VCI) 41-5

virtual channels

- statistics 33-52, 33-55, 33-57
- status 33-36, 38-40
- viewing 33-35

virtual circuits

- viewing 41-82

Virtual Path (VP) Tunneling 42-24

Virtual Path Identifier (VPI) 41-5

virtual path mux 42-25

Virtual Path Tunnels 46-50

virtual ports 24-18

- adding 24-52
- deleting 24-54
- errors 24-63
- format 24-34

information on 24-55

modifying 24-53

statistics for 24-58, 24-61

VLAN membership 27-29

VLAN/group membership 25-25

virtual rings

- setting up 21-7

virtual router ports 27-19

- creating 24-24

viwl command 25-25, 27-29

VLAN Advertisement Protocol
see VAP

VLAN Clusters 36-38

- 1483 encapsulation 36-39

vlan command 8-19, 24-20

VLAN policies

- deleting 27-25, 28-10
- modifying 27-26, 28-11
- viewing 25-24, 27-28, 28-14

VLANs 24-18, 27-1

- application examples 29-1

backbone 29-10

Banyan Vines 27-31

bridges 22-4

creating 27-16

deadlocked 57-6

default 27-4

deleting 27-26

deleting policies in 27-25, 28-10

frame flooding in 27-15

IP routing in, 30-4

IPX networks 29-4, 29-7

logical policies 29-2

modifying 27-24

multicast 28-1

network address policies 29-2

policies 25-2, 27-3

port policy 27-9, 27-18

router ports 27-15

router traffic in 27-7

secondary traffic 27-6

translated frames 29-7

trunking 36-9

viewing 25-23, 27-27

vlap command 26-9
vlat command 36-67
vlb command 35-24
vlbc command 35-32
vlbs command 35-26
vlec command 35-33, 35-36
vlecs command 35-38
vlecsc command 35-41
vlecss command 35-39
vlrs command 33-46, 42-41
vls command 33-45, 42-39
vlts command 33-50
vmac command 35-34
vmpe command 37-10, 37-14
vmpece command 37-10, 37-20
vmpci command 37-10, 37-19
vmpcs command 37-10, 37-21
vmpcst command 37-10, 37-15
vnac command 33-59, 41-100
vnape command 33-59, 41-100
 VP switching 41-51
 VP Tunnels
 caution 42-27
 creating 42-26
 deleting 42-35
 modifying 42-35
 route addresses 47-9
 viewing 42-30
 VPI bits 41-30, 41-68
vpis command 54-28
vpolicy command 35-43
vps command 54-17
vs command 24-61
vss command 36-63, 36-64, 36-68, 36-71,
 36-74
vtsmap command 21-37
vva command 33-43
vvc command 33-35, 41-82

W

wan command 48-24
 WAN Links
 accessing the LINK menu 51-2
 adding a link record 51-3
 deleting link records 51-11
 displaying link status 51-15
 modifying a link record 51-9
 viewing link records 51-12
 WAN modules 3-61, 48-13, 48-18
 cables B-1
 pinouts 3-61
 WSM-BRI 48-18
 WSM-FT1/E1 48-15
 WSM-S 48-13
 WSX-BRI-SC 3-75
 WSX-FT/E1-SC 53-1
 WSX-FT1/E1-SC 3-71
 WSX-S-2W 3-66
 WSX-SC 3-68
 WAN routing 24-22, 24-39
 warning
 hot swapping and file corruption 2-2, 6-4,
 6-5, 40-25
 power down and file corruption 2-2, 6-4,
 6-5, 40-25
wb command 11-10
 well-known address
 for LECS 42-36
who command 8-38
wpmodify command 48-24
wpstatus command 48-46
wpview command 48-36
write command 8-39
 WSM 5-20
 back-to-back configuration 48-6
 back-to-back configurations 48-6
 cables 48-21
 data compression 48-22
 port configuration 48-24
 statistics 48-46
 viewing parameters 48-36
 WSM-FT1/E1 53-1
 WSX-BRI-SC 3-75
 WSX-FT1/E1-SC 3-71, 53-1
 WSX-S-2W 3-66
 WSX-SC 3-68

X

X802.1Q 20-1, 20-4

X-LANE 36-15

xlat command 30-8

XMAP

adjacency 26-2

and remote switches 26-4

common transmission time 26-7

configuring 26-5

discovery transmission time 26-6

transmission states 26-3

well-known MAC address 26-3

xmapcmntime command 26-7

xmapdisctime command 26-6

xmapls command 26-5

xmapst command 26-5

Z

ZMODEM 9-1, 9-4, A-1