

# ATLAS 800<sup>PLUS</sup> User Manual

Part Number 1200226L1 Part Number 1200228L1

#### **TRADEMARKS**

Windows is a registered trademark of Microsoft Corporation. DMS 100 is a registered trademark of Northern Telecom. 5ESS is a registered trademark of AT&T. AT&T is a registered trademark.



901 Explorer Boulevard P.O. Box 140000 Huntsville, AL 35814-4000 (256) 963-8000

© 2000 ADTRAN, Inc. All Rights Reserved. Printed in U.S.A.

### FCC regulations require that in this manual the following information be provided to the customer:

- 1. This equipment complies with Part 68 of the FCC rules. The required label is affixed to the bottom of the chassis.
- 2. An FCC-compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack which is Part 68-compliant. See Chapter 2, *Installing the ATLAS 800PLUS*, for details.
- 3. If your telephone equipment (ATLAS) causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice isn't practical, you will be notified as soon as possible. You will be advised of your right to file a complaint with the FCC.
- 4. Your telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of your equipment. If they do, you will be given advance notice to give you an opportunity to maintain uninterrupted service.
- 5. If you experience trouble with this equipment (ATLAS), please contact ADTRAN at (256) 963-8000 for repair/ warranty information. The telephone company may ask you to disconnect this equipment from the network until the problem has been corrected or until you are sure the equipment is not malfunctioning.
- 6. This unit contains no user-serviceable parts.
- 7. The following information may be required when applying to your local telephone company for leased line facilities.

Service Type	REN/SOC	FIC	USOC
1.544 Mbps - SF	6.0N	04DU9-BN	RJ-48C
1.544 Mbps - SF and B8ZS	6.0N	04DU9-DN	RJ-48C
1.544 Mbps - ESF	6.0N	04DU9-1KN	RJ-48C
1.544 Mbps - ESF and B8ZS	6.0N	04DU9-1SN	RJ-48C
ISDN	6.0N	04DU9-ISN	RJ-48C

#### Federal Communications Commission Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a 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 instruction manual, may cause harmful interference to radio frequencies. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Shielded cables must be used with this unit to ensure compliance with Class A FCC limits.



Change or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

#### **Affidavit Requirements for Connection to Digital Services**

- An affidavit is required to be given to the telephone company whenever digital terminal equipment
  without encoded analog content and billing protection is used to transmit digital signals containing encoded analog content which are intended for eventual conversion into voiceband analog signals and transmitted on the network.
- The affidavit shall affirm that either no encoded analog content or billing information is being transmitted or that the output of the device meets Part 68 encoded analog content or billing protection specifications.
- End user/customer will be responsible for filing an affidavit with the local exchange carrier when connecting unprotected customer premise equipment (CPE) to 1.544 Mbps or subrate digital services.
- Until such time as subrate digital terminal equipment is registered for voice applications, the affidavit requirement for subrate services is waived.

# Affidavit for Connection of Customer Premises Equipment to 1.544 Mbps and/or Subrate Digital Services

For the work to be performed in the certified territory of	(telco name)
State of	
County of	
I, (name),	(business address),
(telephone number) being duly sworn, state:	
I have responsibility for the operation and maintenance of the terminal equipment 1.544 Mbps and/or subrate digital services. The terminal equipment plies with Part 68 of the FCC rules except for the encoded analog content and bifications. With respect to encoded analog content and billing protection:	to be connected com-
( ) I attest that all operations associated with the establishment, maintenance, a digital CPE with respect to analog content and encoded billing protection in ously complies with Part 68 of the FCC Rules and Regulations.	
( ) The digital CPE does not transmit digital signals containing encoded analog information which is intended to be decoded within the telecommunication	
( ) The encoded analog content and billing protection is factory set and is not u customer.	under the control of the
I attest that the operator(s)/maintainer(s) of the digital CPE responsible for the nance, and adjustment of the encoded analog content and billing information has to perform these functions by successfully having completed one of the following blocks):	as (have) been trained
( ) A. A training course provided by the manufacturer/grantee of the equipmanalog signals; or	nent used to encode
( ) B. A training course provided by the customer or authorized representative rials and instructions provided by the manufacturer/grantee of the equal analog signals; or	
( ) C. An independent training course (e.g., trade school or technical institution manufacturer/grantee of the equipment used to encode analog signals;	
( ) D. In lieu of the preceding training requirements, the operator(s)/maintain control of a supervisor trained in accordance with (circle one	

	(telco's name) with proper documentation to demonstrate provided in the preceding paragraph, if so requested.
	_Signature
	_Title
	_ Date
Transcribed and sworn to before me	
This, 199	_
Notary Public	-
My commission expires:	

#### **Canadian Equipment Limitations**



The Industry Canada Certification label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic waterpipe system, if present, are connected together. This precaution may be particularly important in rural areas.



Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or an electrician, as appropriate.

The Load Number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the equipment that the total of the LNs of all devices does not exceed 100.

The ringer equivalence number (REN) assigned to each terminal adapter is used to determine the total number of devices that may be connected to each circuit. The sum of the RENs from all devices in the circuit should not exceed a total of 5.0.

#### LIMITED PRODUCT WARRANTY

ADTRAN warrants that for five (5) years from the date of shipment to Customer, all products manufactured by ADTRAN will be free from defects in materials and workmanship. ADTRAN also warrants that products will conform to the applicable specifications and drawings for such products, as contained in the Product Manual or in ADTRAN's internal specifications and drawings for such products (which may or may not be reflected in the Product Manual). This warranty only applies if Customer gives ADTRAN written notice of defects during the warranty period. Upon such notice, ADTRAN will, at its option, either repair or replace the defective item. If ADTRAN is unable, in a reasonable time, to repair or replace any equipment to a condition as warranted, Customer is entitled to a full refund of the purchase price upon return of the equipment to ADTRAN. This warranty applies only to the original purchaser and is not transferable without ADTRAN's express written permission. This warranty becomes null and void if Customer modifies or alters the equipment in any way, other than as specifically authorized by ADTRAN.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, THE FOREGOING CONSTITUTES THE SOLE AND EXCLUSIVE REMEDY OF THE CUSTOMER AND THE EXCLUSIVE LIABILITY OF ADTRAN AND IS IN LIEU OF ANY AND ALL OTHER WARRANTIES (EXPRESSED OR IMPLIED). ADTRAN SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING (WITHOUT LIMITATION), ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THIS EXCLUSION MAY NOT APPLY TO CUSTOMER.

In no event will ADTRAN or its suppliers be liable to Customer for any incidental, special, punitive, exemplary or consequential damages experienced by either Customer or a third party (including, but not limited to, loss of data or information, loss of profits, or loss of use). ADTRAN is not liable for damages for any cause whatsoever (whether based in contract, tort, or otherwise) in excess of the amount paid for the item. Some states do not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to Customer.

#### **About this Manual**

The ATLAS 800<sup>PLUS</sup> system consists of the Base Unit and one or more option modules. (Each option module includes its own user manual which contains specific information about installing, configuring, and testing the option module; insert the option module manuals into this binder.) This ATLAS User Manual provides the information you need to install, configure, test, and troubleshoot the ATLAS 800<sup>PLUS</sup> system; when applicable, this manual refers you to the individual option module user manual. The arrangement of this user manual allows you to quickly and easily find the information you need. An overview of the contents of this manual follows:

#### Introduction

• Chapter 1, *Introducing the ATLAS 800PLUS*, familiarizes you with the ATLAS 800<sup>PLUS</sup> Base Unit and provides some sample ATLAS 800<sup>PLUS</sup> applications.

#### **Getting Started**

- Chapter 2, *Installing the ATLAS 800PLUS*, describes the rear panel layout and how to install the ATLAS 800<sup>PLUS</sup>.
- Chapter 3, *Operating the ATLAS 800PLUS*, describes the front panel layout and different ways to operate the ATLAS 800<sup>PLUS</sup>.

#### **Reference Information**

- Chapter 4, *Using the Front Panel*, describes how to use the front panel. This chapter also describes each menu option that is accessible through the front panel.
- Chapter 5, Navigating the Terminal Menu, describes how to navigate the terminal menu.
- Chapter 6, Terminal Menu and System Control, describes the terminal menus used for system control.
- Chapter 7, *Modules Terminal Menu*, describes the terminal menus used for module and T1/PRI port control.
- Chapter 8, *Dedicated Maps Terminal Menu*, describes the terminal menus used for Dedicated Maps and provides some examples.
- Chapter 9, Dedicated Circuit Backup and Circuit Status, describes the terminal menus used for Circuit Status.
- Chapter 10, *Dial Plan Terminal Menu*, describes the terminal menus used for Dial Plans and provides some examples.

#### Working with the ATLAS $800^{PLUS}$

- Chapter 11, *Updating Firmware*, provides step-by-step instruction on how to update the ATLAS 800<sup>PLUS</sup> firmware.
- Chapter 12, SNMP Management, describes how to control the ATLAS 800 PLUS via SNMP.
- Chapter 13, ADTRAN Utilities, describes the SysLog, Telnet, VT-100, and TFTP Server programs delivered with the ATLAS 800<sup>PLUS</sup>.

#### **Appendices**

- Appendix A, System Event Logging, describes the events monitored by the ATLAS 800<sup>PLUS</sup>.
- Appendix B, Troubleshooting, describes how to diagnose different problems you may experience.
- Appendix C, Warranty and Technical Support Information, describes your warranty and how to contact technical support.
- Appendix D, Acronyms and Abbreviations, lists acronyms and abbreviations used for the ATLAS 800<sup>PLUS</sup> and its option modules.
- Appendix E, *Glossary*, defines terms used with ATLAS 800 PLUS and its option modules.



Notes provide additional useful information.



Cautions signify information that could prevent service interruptions.



Warnings provide information that could prevent damage to the equipment or endangerment to human life.

# **Table of Contents**

List of Figures	xxiii
List of Tables	xxv
Chapter 1 Introducing the ATLAS 800PLUS	1-1
Product Overview	
ATLAS 800PLUS Base Unit	1-1
ATLAS 800PLUS Features	1-6
Chapter 2 Installing the ATLAS 800PLUS	2-1
Inspect the ADTRAN Shipment	
Contents of ADTRAN Shipments	
Check the Power Connection	
AC Powered Unit	
DC Powered Unit	
Grounding Instructions	
Review the Rear Panel Design	
Control/Chain In Port	
Connection	
Control/Chain Out Port	
Connection	
Network Connection	
Connection	
Ethernet 10BaseT Connection	
Connection	
MON	
Option Slots	
Install Any Option Modules	
Power-Up	
	0.4
Chapter 3 Operating the ATLAS 800PLUS	
Methods of Operating the ATLAS 800PLUS	
Using The Terminal Menu	
Using Telnet	
Starting a Telnet Session	
Using VT-100 Terminal Emulation	
Using T-Watch PRO	3-5
Chapter 4 Using the Front Panel	
Operation Keys	
Front Panel Menu Structure	
Front Panel Main Menu	4-6
Menus	4-7

Submenus	4-7
Sub-submenus	4-7
Status	4-7
S0 System	4-7
Ethernet Status	
Chain Port Status	
S1—S8	
Config	
S0 System	
Ethernet	
Chain Port	
S1—S8	
Util	
Time/Date	
Software Rev	
Selftest	
Run Selftest	
Show Results	
Clear Results	
Set Passcode	
Password Reset	
ALRM Menu	4-11
Active Alarms	4-11
View History	4-12
Clear History	4-12
Chapter 5 Navigating the Terminal Menu  Terminal Menu Window  Menu Path	5-1
Window Panes	5-2
Window Pane Navigation	
Right Window Pane Notation	
Additional Terminal Menu Window Features	
Navigating Using the Keyboard Keys	
Moving through the Menus	
Session Management Keystrokes	
Configuration Keystrokes	
Getting Help	
Getting Ticip	J-J
Chapter 6 Terminal Menu and System Control	6-1
Selecting the Appropriate menu	
Security Levels	
v	
Menus	
Submenus	
Sub-submenus	
System Info	0.0
System Name	
Contain I and an	6-3
System Location	6-3 6-3
System Contact	
System Contact Firmware Revision	
System Contact	
System Contact Firmware Revision System Uptime Startup Mode	
System Contact	

	Serial Number	.6-3
	Boot ROM Rev	.6-3
Syst	em Status	6-3
Ü	Event Log	.6-4
	Clear System Event Log	.6-4
	Ethernet Port	.6-5
	Clear System LED	.6-5
	System Alarms	
	System Timing Source	
	Resource Usage	
	Data Tables	
	Configuration	
	Trunk Usage	
	Data Tables	
	Chain Port Signal Leads	
	Chain Port Tx Bytes	
	Chain Port Rx Bytes	
	Chain Port Overrun Errs	
	Chain Port Framing Errs	
	Clear Chain Port Countrs	
	em Config	
	Primary Timing Source	
	Backup Timing Source	
	ADLP Address	
	Session Timeout	
	Max Telnet Sessions	
	Ethernet Port	
	Chain Port	
	Port Name	
	Port Type	
	Port Speed	
	Modem Initialization String	
	Initialize Modem	
	Flow Control	
	SNMP	
	SNMP Access	
	SNMP Communities	
	Trap Transmission	
	Authen Trap Transmission	
	Traps Destination $\epsilon$	
	System Event Logging $\epsilon$	
	Syslog Setup	
	Transmission6	3-10
	Host IP Address6	3-10
	Host Facility6	3-10
	Real Time Clock6	3-10
	Current Time/Date6	3-10
	Auto Daylight Savings6	6-10
	Access Passwords6	
	Label6	3-11
	Access Rights6	3-11
	Password	
	Active6	
	Bonding Config6	

TXINIT Timer	6-12
TXFA Timer	6-12
TXADD01 Timer	6-12
TXDEQ Timer	
TANULL Timer	
TCID Timer	
Call Stagger	
System Utility	
Update Firmware	
Module Slot	
Module Type	
Transfer Method	
Restart Schedule	
Current Update Status	
Previous Update Status	
Begin Firmware Update	
Update Status	
Config Transfer	
Transfer Method	
TFTP Server IP Address	
TFTP Server Filename	
Current Transfer Status	
Previous Transfer Status	
Load and Use Config	
Save Config Remotely	
System Utilization	
System Selftest	
Selftest Run	
Status	
View Selftest Log	
Clear Self-test Log	
Ping	
IP Address	
Count	
Size	
Timeout	
Round trip min	
Round trip avg	
Round trip max	
Tx Stats	
Reset Stats	
Start/Stop	
Reboot System	
Factory Default System	6-20
Chapter 7 Modules Terminal Menu	
Menus	
Submenus	
Sub-submenus	7-1
Modules	7-1
Slt	
Type	
Menu	
Alarm	7-2

Test	7-2
State	7-2
Status	7-3
Rev	7-3
Modules (Quad T1/PRI) Menu	7-3
Controller Info	7-3
Alarm Status	7-3
DS0 Status	7-4
DS0 Alarms	7-4
Sig Status	7-4
Performance: Current	7-5
Performance: 15 Min	7-5
Performance: 24 Hr.	7-5
Configuration	7-5
Test	7-6
Chapter 8 Dedicated Maps Terminal Menu	8-1
Overview	
Menus	
Submenus	8-1
Sub-submenus	
Activate Map	
Auto	
Maps 1—5	
Current Map	
Create / Edit Maps	
#	
Map Name	
Sort TO/FROM	
Connects	
#	
FROM Slt	
Port	
TO Slot	
Port	
From Config	
To Config	
RBS	
Activate Time	
Enbl Day	
Designing a Dedicated map	
Configuring the Ports	
Defining the Connections	8-8
Chapter 9 Dedicated Circuit Backup and Circuit Status	
Overview	
Dedicated Circuit Dial Backup Setup	
Configuration	
Menus	
Submenus	
Sub-submenus	
Interface Configuration	
Originate/Answer	
Outgoing Call Type	9-3

Source ID	
Outdial Number	
Force Mode	
Backup Criteria	
Restore Criteria	9-3
Startup Delay	9-3
Backup Delay	9-3
Restore Delay	9-4
Max Num Redials	9-4
Redial Timer	9-4
Enable Schedule	
Test Call	
Min Num DS0s	
Max Num DS0s	
Circuit Status Menu	
From	
MAN (Manual Backup)	
BKUP Status (Backup Status)	
Line Status	
Delay	
Test	
Last Run Time	
Next Run Time	
Last Test Status	
Pass : Fail	
Test Now	9-7
CI . 40 D. I.D 114	40.4
Chapter 10 Dial Plan Terminal Menu	
Overview	
Network Term	
Slot/Svc	
Port/PEP	
Sig	
Out#Accept	
Src ID	
Accept Numbers	
Search	
Data 64K, Data 56K	
Out#Rej	
Reject Number	10-5
Data 64K, Data 56K, Audio, and Speech	
Ifce Config	
User Term	
Slot/Svc, Port/PEP	
Sig	
In#Accept	
Source ID	
Accept Numbers	
Search	
Data 64K, Data 56K	
Out#Rej	
Reject Number	
Data 56K, Data 64K, Audio, Speech	
Ifce Config	10-7

Global Param	10-8
End of Number Timeout	10-8
Area Code	10-8
Nbr Complete Templates	10-8
Number Type Templates	10-8
Automatic Routeback Rejection	
Quad T1/PRI Module Interface Configuration	10-9
Quad T1/PRI Module (Network Termination/PRI)	10-9
Switch Type	
First DS0	
Number of DS0s	10-10
Outgoing Number Conversion	10-10
Strip MSD	
Netwrk Spec. Fac Voice	
Netwrk Spec Fac. Data	
Called Digits Transferred	10-10
Outgoing Caller ID	
Source ID	
Swap ANI/DNIS	
Quad T1/PRI Module (Network Termination/RBS)	10-12
First DS0	10-12
Number of DS0s	10-12
DS0s Available	10-12
Signaling Method	10-12
Direct Inward Dialing	10-13
Trunk Number	10-13
Strip MSD	10-13
Source ID	10-13
Quad T1/PRI Module (User Termination/PRI)	10-14
Switch Type	10-14
First DS0	10-14
Number of DS0s	10-14
Strip MSD	10-14
Network Specific Facility Voice	10-14
Network Specific Facility Data	10-14
Called Digits Transferred	10-15
Outgoing Caller ID	
ID Presentation	10-15
ID Number	
Source ID	
Swap ANI/DNIS	
Quad T1/PRI Module (User Termination/RBS)	
First DS0/Number of DS0s	
DS0s Available	
Signaling Method	
Direct Inward Dialing	
Caller ID Number	
Strip MSD	
Source ID	
Quad Nx56/64 Module (User Termination)	
Ports Available	
Number of Ports	
Number to dial	
Call Type	10-18

Source ID	
Max DS0s	10-18
	10-18
Octal BRI Module (Network Termination)	
Switch Type	
SPID List	
Strip MSD	
Source ID	
Octal BRI Module (User Termination)	
Switch Type	
SPID List	
Strip MSD	
Source ID	
Outgoing Caller ID	
ID Presentation	
ID Number	
Creating Dial Plans—Examples	
Understanding Dial Plan Configurations	10-21
Charter 11 Hardathar Firman	11 1
Chapter 11 Updating Firmware	
Overview	
XMODEM Firmware Updates	
Updating Firmware using XMODEM	
TFTP Firmware Updates	
Updating Firmware using TFTP	11-4
Chapter 12 SNMP Management	19-1
SNMP	
Basic Components	
Network Manager	
Agent	
15011	
	12-1
MÏB	
MÏBSNMP Traps	12-2
MIBSNMP TrapsTrap Destination List	12-2 12-2
MIBSNMP TrapsTrap Destination List Configuring a Trap Destination List Via Terminal Menu	12-2 12-2 12-2
MIBSNMP TrapsTrap Destination ListConfiguring a Trap Destination List via Terminal MenuFiltering (Disabling) Traps	12-2 12-2 12-2
MIBSNMP TrapsTrap Destination ListConfiguring a Trap Destination List via Terminal MenuFiltering (Disabling) TrapsStandard Traps	
MIBSNMP TrapsTrap Destination ListConfiguring a Trap Destination List via Terminal MenuFiltering (Disabling) TrapsStandard TrapsStandard TrapsDS1 Traps	
MIBSNMP TrapsTrap Destination ListConfiguring a Trap Destination List via Terminal MenuFiltering (Disabling) TrapsStandard TrapsDS1 TrapsDS1 TrapsDS1 Alarm Traps	
MIBSNMP TrapsTrap Destination ListConfiguring a Trap Destination List via Terminal MenuFiltering (Disabling) TrapsStandard TrapsStandard TrapsDS1 Traps	
MIB	
MIBSNMP TrapsTrap Destination ListConfiguring a Trap Destination List via Terminal MenuFiltering (Disabling) TrapsStandard TrapsDS1 TrapsDS1 TrapsDS1 Alarm Traps	
MIB	
MIB	12-2 12-2 12-2 12-3 12-3 12-3 12-3 12-4 13-1 13-1
MIB	12-2 12-2 12-2 12-3 12-3 12-3 12-4 13-1 13-1 13-2
MIB  SNMP Traps  Trap Destination List  Configuring a Trap Destination List via Terminal Menu  Filtering (Disabling) Traps  Standard Traps  DS1 Traps  DS1 Alarm Traps  DS1 Alert Traps  Chapter 13 ADTRAN Utilities  Overview  SysLog Host Daemon  SysLog GUI	
MIB	
MIB  SNMP Traps  Trap Destination List  Configuring a Trap Destination List via Terminal Menu  Filtering (Disabling) Traps  Standard Traps  DS1 Traps  DS1 Alarm Traps  DS1 Alert Traps  Chapter 13 ADTRAN Utilities  Overview  SysLog Host Daemon  SysLog GUI  Monitor.  Menu Bar	12-2 12-2 12-2 12-3 12-3 12-3 12-3 12-4 13-1 13-1 13-2 13-2 13-3
MIB  SNMP Traps  Trap Destination List  Configuring a Trap Destination List via Terminal Menu  Filtering (Disabling) Traps  Standard Traps  DS1 Traps  DS1 Alarm Traps  DS1 Alert Traps  Chapter 13 ADTRAN Utilities  Overview  SysLog Host Daemon  SysLog GUI  Monitor  Menu Bar	12-2 12-2 12-3 12-3 12-3 12-3 12-3 12-4 13-1 13-1 13-2 13-2 13-3 13-3 13-3
MÏB  SNMP Traps  Trap Destination List	12-2 12-2 12-3 12-3 12-3 12-3 12-3 12-4 13-1 13-1 13-1 13-2 13-3 13-3 13-3 13-3
MIB SNMP Traps Trap Destination List Configuring a Trap Destination List via Terminal Menu Filtering (Disabling) Traps Standard Traps DS1 Traps DS1 Alarm Traps DS1 Alert Traps  Chapter 13 ADTRAN Utilities Overview SysLog Host Daemon SysLog GUI Monitor Menu Bar. File Display Log Files	12-2 12-2 12-3 12-3 12-3 12-3 12-3 12-4 13-1 13-1 13-2 13-3 13-3 13-3 13-4 13-4

Clear Red Events	13-4
Help	13-4
Telnet Utility	13-4
Session Menu	13-6
Connect	13-6
Host Name	13-6
Port	13-6
Edit Entry	13-6
Add New	13-6
Delete	13-6
Connect	13-6
Disconnect	13-6
Transfer Cfg	13-7
Exit	
Edit Menu	
Options Menu	
Colors	
Local Echo	
AutoRepeat	
Capture Menu	
File	
Start Cfg Capture	
Stop Cfg Capture	
Buffer Size	
Save Buffer As	
Screen Capture	
Help Menu	
Contents	
IP Status	
About	
VT-100 Utility	
Session Menu	
Connect	
Disconnect	
File Transfer	
XMODEM CRC	
ASCII Cfg Files	
Edit Menu	
Port Menu	
Options Menu	
Refresh Screen	
Connect	
Transmit Wakeup	
Transmit Refresh	
Colors	
Local Echo	
AutoRepeat	
Capture Menu.	
Help Menu	
Contents	
About	
TFTP Server	
Server Menu	
Enable	13-11

Disable	13-11
Abort	13-11
Exit	13-11
Print Log	13-11
to Clipboard	13-11
to Printer	13-11
Clear Log	13-11
Help	13-12
Contents	13-12
About	13-12
Status Field	13-12
Meter Field	13-12
Log Field	
Saving the Current Configuration to a TFTP Server	13-12
Successful Transfer	
Unsuccessful Transfer	13-13
Retrieving the Configuration from a TFTP Server	13-13
Appendix A System Event Logging	A-1
Appendix B Troubleshooting	B-1
Appendix C Warranty and Technical Support Information	C-1
Appendix D Acronyms and Abbreviations	D-1
Appendix E Glossary	E-1
Index	Index-1

# List of Figures

Figure 1-1.	Point-to-Point Circuit	1-2
Figure 1-2.	Frame Relay Circuit	1-3
Figure 1-3.	Digital Access Cross-Connect System (DACS)	1-4
	T1 Bandwidth Management	
Figure 1-5.	WAN Overbooking	1-6
Figure 2-1.	AC Powered ATLAS 800 <sup>PLUS</sup> Rear Panel	2-3
Figure 2-2.	DC Powered ATLAS 800PLUS Rear Panel	2-4
Figure 2-3.	ATLAS 800 <sup>PLUS</sup> Slot Designation (Rear View)	2-8
Figure 3-1.	Front Panel LCD	3-1
Figure 3-2.	Example of Basic Front Panel Menu Navigation	3-2
Figure 4-1.	ATLAS 800 PLUS Front Panel Layout	4-1
Figure 4-2.	Front Panel LCD	4-4
Figure 4-3.	Front Panel Menu Tree	4-6
Figure 5-1.	Top-level Terminal Menu Window	5-1
Figure 6-1.	System Information Menu	6-2
Figure 6-2.	System Status Menu	6-4
Figure 6-3.	System Configuration Menu	6-7
Figure 6-4.	System Utility Menu	6-13
Figure 6-5.	View Self-test Log	6-18
Figure 7-1.	Modules Menu	7-1
Figure 8-1.	Dedicated Maps Menu Tree	8-1
Figure 8-2.	Trunk Conditioning	8-6
Figure 8-3.	Dedicated Map Overview Example	8-6
Figure 8-4.	Slot 0 Module Configuration Menu	8-8
Figure 8-5.	Completed Dedicated Map	8-10
Figure 9-1.	Dedicated Circuits Backup Configuration	9-1
Figure 9-2.	Interface Config Menu	9-2
	Circuit Status Menu	
Figure 10-1	. Dial Plan Menu	10-1
Figure 10-2	. Dial Plan Menu Tree	10-2
Figure 10-3	. PSTN Connection	. 10-21
Figure 10-4	. Point-to-Point	. 10-22
Figure 10-5	. Remote Access and Video Conferencing Setup	. 10-22
	. Completed Network Map	
_	. Completed User Map	
Figure 11-1	. Update Firmware Menu Interface	11-3
Figure 11-2	. Update Firmware Menu Interface	11-6
Figure 13-1	. ATLAS SysLog Host GUI	13-2

Figure 13-2. SysLog Menu Tree for the Menu Bar	13-3
Figure 13-3. Telnet Menu Tree	13-5
Figure 13-4. VT-100 Menu Tree	13-8
Figure 13-5. TFTP Server Interface Menu Tree	13-10
Figure 13-6. TFTP Server Interface	13-11

# List of Tables

Table 2-1.	Control/Chain In Pinout	2-5
Table 2-2.	Control/Chain Out Pinout	2-5
Table 2-3.	Network Pinout	2-6
Table 2-4.	Ethernet 10BaseT Pinout	2-7
Table 4-1.	ATLAS 800 PLUS Front Panel Description	4-2
Table 4-2.	LED Descriptions	4-3
Table 4-3.	Operation Keys	
Table 6-1.	Password Security Levels	6-2
Table 6-2.	Call Stagger Values	6-13
Table 8-1.	Connections and Ports	8-7
Table 10-1.	Network and Attached Equipment Provisioning	10-24
Table 10-2.	Network Terminations	10-24
Table 10-3.	User Terminations	10-25
Table 11-1.	TFTP Upload Messages	11-5
Table 12-1.	Trap Destination List	12-2
Table 12-2.	Standard Traps	12-3
Table 12-3.	DS1 SNMP Traps	12-4
Table 12-4.	DS1 Current Alert SNMP Traps	12-4
Table 12-5.	Total Alert Traps	12-5
Table A-1.	Source: System	A-2
Table A-2.	Source: Switchboard	A-3
Table A-3.	Source: Nx 56/64	A-4
Table A-4.	Source Time	A-5
Table A-5.	Source: Ethernet	A-6
Table A-6.	Source: ISDN	A-7
Table A-7.	ISDN Cause Codes	A-10
Table A-8.	Cause Code Log Entries	A-12
Table A-9.	Source: ISDN L2 Messages	A-12
Table A-10.	Source: ISDN Call Control Messages	A-12
Table A-11.	Source: ISDN Information Elements	A-13

## Chapter 1 Introducing the ATLAS 800 PLUS

#### PRODUCT OVERVIEW

The ATLAS 800<sup>PLUS</sup> is a modular, highly scalable platform that provides robust solutions for the wide area communication needs of medium-to-large corporations and network access providers. ATLAS is an Integrated Access System with the most extensive support of dedicated bandwidth management and access switching in the industry.

The ATLAS  $800^{PLUS}$  is a high performance version of the ATLAS 800. The ATLAS  $800^{PLUS}$  contains a high-performance CPU, more memory, and powerful communications drivers which allow the support of optional applications such as frame relay.

With the ATLAS  $800^{PLUS}$ , you can consolidate your voice, data, and video applications into a single platform while optimizing wide area bandwidth and reducing equipment costs. The ATLAS  $800^{PLUS}$  architecture and the chassis' eight expansion slots allow for a variety of modules, making it one of the most versatile access systems on the market. With the appropriate modules installed, the ATLAS  $800^{PLUS}$  functions as follows:

- A Frame Relay Switch
- A Digital Access Cross-Connect System (DACS)
- A T1 Bandwidth Manager
- An ISDN Access Switch
- A Remote Access Manager

#### ATLAS 800 PLUS BASE UNIT

The ATLAS  $800^{PLUS}$  architecture includes a packet switching and a circuit switching bussing scheme. The result is a highly scalable system capable of supporting bandwidth requirements up to 34~T1/E1 or Primary Rate ISDN (PRI) circuits. Designed for standalone or rackmount installations, the ATLAS  $800^{PLUS}$  Base Unit provides two network interfaces, each independently configurable for T1, DSX-1, or PRI operation. Eight expansion slots accommodate hot-swappable modules for a variety of applications. A 10BaseT connection for remote access and network management is standard with the ATLAS  $800^{PLUS}$  Base Unit.

The modules include the following:

- Quad Nx 56/64 Module
- Quad T1/PRI Module
- Octal Basic Rate ISDN Module
- T3 Module
- Async-232 Module
- Modem-16 Module

#### Frame Relay

Frame relay is a packet-switched service that allows efficient transfer of bursty traffic in a WAN environment. It offers lower-cost data transfer when compared to typical point-to-point applications. Using virtual connections within the frame relay network and combining those into a single physical connection at each location results in lower cost. Frame relay providers use a frame relay switch to route the data on each virtual circuit to the appropriate destination. Figures 1-1 and 1-2 illustrate a conversion from a typical point-to-point application to a frame relay application.

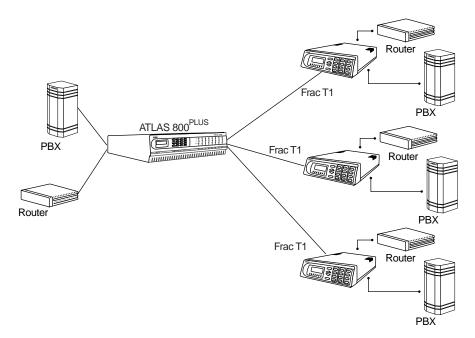


Figure 1-1. Point-to-Point Circuit

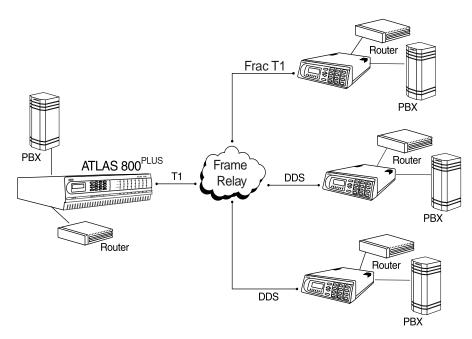


Figure 1-2. Frame Relay Circuit

The Frame Relay/Router upgrade option adds the capability for the ATLAS series of Integrated Access Devices to act as a voice/data FRAD, a frame relay switch, and an IP router in addition to the current available bandwidth manager and switch applications.

#### **Dedicated and Switched Connection Maps in a Single Platform**

The ATLAS  $800^{PLUS}$  allocates dedicated bandwidth according to any of up to five unique connection maps. Any DS0 on any T1 circuit can be mapped to any other DS0 on up to 34 T1 circuits in the system. Dedicated Connection Maps can be invoked manually or implemented automatically based on the time of day and day of the week.

Additionally, the ATLAS 800 PLUS can be configured to switch dialup calls to specific ports or DS0s based on the number that is dialed. Switched connection mapping is supported for dial calls placed over basic rate ISDN, primary rate ISDN, or channelized T1.

#### Signaling Conversion for Maximum Interoperability

The ATLAS 800<sup>PLUS</sup> can convert between Robbed Bit Signaling and ISDN D channel signaling, giving you the flexibility to get the speed and reliability of ISDN, while preserving your investment in non-ISDN equipment. ATLAS can also convert between D4 and ESF frame formats as well as AMI and B8ZS line coding, providing interoperability with legacy equipment.

#### Flexible Network Management and Maintainability

Several network management methods are available for the ATLAS  $800^{PLUS}$ , including SNMP support. VT 100 and Telnet are also of-

fered, providing detailed system configuration through an easy-to-use menu system. The terminal interface is secured by six levels of password protection with varying degrees of management privileges. The terminal interface is accessed locally or remotely using either the EIA-232 Chain In port on the rear of the unit or the Telnet interface. The 10BaseT interface on the Base Unit provides an Ethernet connection for SNMP and Telnet connections.

Additionally, T-Watch PRO, ADTRAN's Microsoft<sup>®</sup> Windows<sup>®</sup>-based GUI management system can allow end-to-end management with downstream ADTRAN T1 products. User configurations can be preserved in non-volatile memory and duplicated for managing multiple ATLAS implementations. ATLAS also supports FLASH upgrades for future enhancements. You can remotely download software using TFTP or XMODEM.

The front panel contains a 2x16 character backlit LCD display and an extensive array of LEDs for alarm and status information pertaining to the system and the individual modules. A front panel keypad allows navigation through the menu system and access to system testing.

Several test capabilities allow you to diagnose the health of your T1, PRI, or BRI circuits without additional test equipment. Standard Bantam test jacks located on the rear panel also allow you to use external test equipment to monitor traffic. Tests include local, remote, and V.54 loopbacks utilizing the 511, QRSS, all zeros, and all ones test patterns.

#### **Digital Access Cross-Connect System (DACS)**

Inherent in the ATLAS 800<sup>PLUS</sup> architecture is the ability to cross connect, or DACS, up to thirty-four T1 circuits. DACSing allows the assignment and redistribution, or grooming, of any DS0 on any T1 circuit to any other DS0 on any of the thirty-four T1 circuits in the system. For optimizing network resources, any of five dedicated connection maps can be invoked manually or automatically, based on the time of day and day of the week (see Figure 1-3).

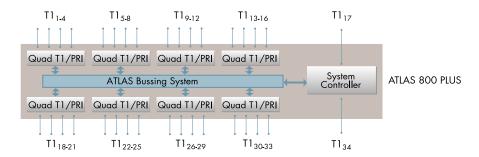


Figure 1-3. Digital Access Cross-Connect System (DACS)

61200226L1-1

#### T1 Bandwidth Manager

1-4

As a T1 Bandwidth Manager, ATLAS 800<sup>PLUS</sup> combines the functions of a T1 CSU/DSU, an intelligent channel bank, a T1 Multiplexer, and DACS into a single platform. The Bandwidth Manager supports a wide range of data ap-

plications including T1 "drop and insert," channel grooming, and wide area data transport. ATLAS is ideal for point-to-point configurations or access to public networks. For optimization of existing equipment and network resources, ATLAS can be paired with ADTRAN's TSU product offerings to support a variety of data and analog voice applications (see Figure 1-4).

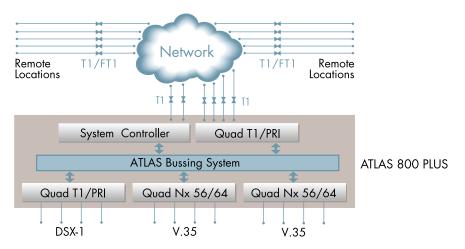


Figure 1-4. T1 Bandwidth Management

#### **ISDN Access Switch**

The ATLAS 800 PLUS includes an advanced access architecture for switching dial-up calls to specific ports or DS0s. As an access switch functioning in a user-to-user network and user-to-user mode, ATLAS consolidates multiple basic rate ISDN (BRI) connections onto T1/PRI access lines. Additionally, BRI-to-BRI, BRI-to-PRI, and PRI-to-PRI switching are supported. ATLAS also converts between ISDN D channel (PRI or BRI) and T1 robbed bit signaling, allowing a non-ISDN PBX to access a more efficient ISDN facility. For network optimization, when bandwidth is not being used for switched applications such as video conferencing, switched connection mapping dynamically allocates bandwidth to the PB for voice traffic. Call Filtering allows you to program the call types that will be answered and/or originated on a per-user basis.

#### **WAN Overbooking**

The WAN Overbooking feature of ATLAS 800 PLUS allows you to oversubscribe switched bandwidth for situations where simultaneous access to the network by every subscriber is not required. WAN Overbooking reduces telecommunications expenses while still giving your subscriber base the connectivity they require. Local subscriber-to-subscriber connections are made without accessing the network at all, resulting in even more efficient use of wide area bandwidth Figure 1-5 on page 1-6.

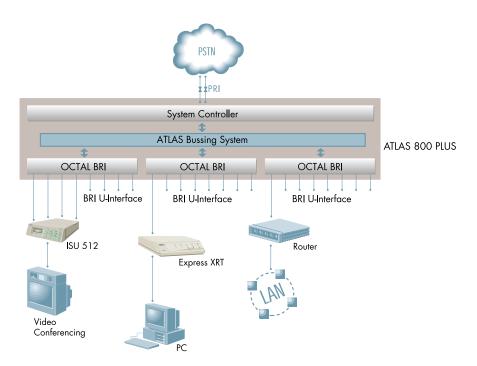


Figure 1-5. WAN Overbooking

#### ATLAS 800<sup>PLUS</sup> FEATURES

#### **Configuration and Management**

- VT 100 Emulation
- T-Watch PRO, Microsoft Windows based GUI
- SNMP, per MIB II (RFC1213), DS1 MIB (RFC1406), and ADTRAN private MIBs
- Telnet
- LCD Front Panel
- Six levels of password protection and privileges

#### **Software Upgrade**

- Flash Memory
- TFTP Download
- XMODEM via control port

#### **Signaling Support**

- ISDN D Channel
- Robbed bit, E&M, Ground Start, Loop Start
- · Convert between Robbed Bit Signaling and ISDN D Channel
- Direct Inward Dialing

#### **ISDN Switch Types**

• 5ESS™, DMS-100™, National ISDN, 4ESS™

#### **Dedicated Connection Maps**

- Up to five connection maps
- Time of day/day of week configurable
- · Preserves signaling through cross-connect
- No effect on non-configured channels

#### **Switched Connection Maps**

Inbound and outbound call filtering and blocking

#### **Testing**

- Local and remote: payload/line, V.54
- Patterns: 511, QRSS, all ones, all zeros

#### **Performance Monitoring**

- Reports: Information stored for last 24 hours in 15 minute increments
- Performance statistics per TR54016, T1.403, RFC1406
- Alarm reporting per TR54016, T1.403

# Chapter 2 Installing the ATLAS 800 PLUS

#### INSPECT THE ADTRAN SHIPMENT

Before installing the ATLAS 800<sup>PLUS</sup>, carefully inspect the ATLAS 800<sup>PLUS</sup> Base Unit for shipping damage. If you suspect damage, file a claim immediately with the carrier and then contact ADTRAN Technical Support (see *Warranty and Technical Support Information* on page C-1). If possible, keep the original shipping container for returning the ATLAS 800<sup>PLUS</sup> for repair or for verification of damage during shipment.

#### **CONTENTS OF ADTRAN SHIPMENTS**

Your ADTRAN shipment includes the following items:

- The ATLAS 800<sup>PLUS</sup> Base Unit
- The ATLAS 800<sup>PLUS</sup> User Manual
- Power cord (AC unit only) ADTRAN P/N 3127031
- Network cables (2) ADTRAN P/N 3125M008
- Rackmount brackets (left and right)
- RJ45—DB-25 adapter (modem and direct)
- RJ-45 control port cable (1) ADTRAN P/N 3127004
- DSX-1 crossover cable (1) ADTRAN P/N 3125M010
- RJ48—DB15 adapter (1)
- ADTRAN Utilities diskettes (3)



Customers must supply the 10BaseT cable.

#### CHECK THE POWER CONNECTION

Check the power connection appropriate to your power supply (AC or DC.)

#### **AC Powered Unit**

The AC powered ATLAS 800<sup>PLUS</sup> (P/N 1200226L1) comes equipped with a detachable 8-foot power cord with a three-prong plug for connecting to a grounded power receptacle.



Power to the ATLAS 800<sup>PLUS</sup> must be from a grounded 115 VAC, 60 Hz or 220 VAC, 50-60 Hz source.

#### **DC Powered Unit**

The DC powered ATLAS  $800^{PLUS}$  (P/N 1200228L1) comes equipped with a terminal block on the rear of the unit. The power source should be connected to the terminal block according to the polarity markings on the unit. For example, a -48 V source would be connected with the -48V return connected to the (+) terminal and the -48VDC attached to the (-) terminal. Power must be from a DC power source in the range of 42 to 57 VDC, capable of delivering up to 7 A of current.



The branch circuit overcurrent protection shall be a fuse or circuit breaker rated minimum 48 V, maximum 20A.

A readily accessible disconnect device that is suitably approved and rated shall be incorporated into the fixed wiring.

#### **GROUNDING INSTRUCTIONS**

This section provides grounding instruction information from the Underwriters' Laboratory UL 1459 Standard for Safety: Telephone Equipment, of September 20, 1993.

An equipment grounding conductor that is not smaller in size than the ungrounded branch-circuit supply conductors is to be installed as part of the circuit that supplies the product or system. Bare, covered, or insulated grounding conductors are acceptable. Individually covered or insulated equipment grounding conductors shall have a continuous outer finish that is either green, or green with one or more yellow stripes. The equipment grounding conductor is to be connected to ground at the service equipment.

The attachment-plug receptacles in the vicinity of the product or system are all to be of a grounding type, and the equipment grounding conductors serving these receptacles are to be connected to earth ground at the service equipment.

A supplementary equipment grounding conductor shall be installed between the product or system and ground that is in addition to the equipment grounding conductor in the power supply cord.

The supplementary equipment grounding conductor shall not be smaller in size than the ungrounded branch-circuit supply conductors. The supplementary equipment grounding conductor shall be connected to the product at the terminal provided, and shall be connected to ground in a manner that will retain the ground connection when the product is unplugged from the receptacle. The connection to ground of the supplementary equipment grounding conductor shall be in compliance with the rules for terminating bonding jumpers at Part K or Article 250 of the National Electrical Code, ANSI/NFPA 70. Termination of the supplementary equipment grounding conductor is permitted to be made to building steel, to a metal electrical raceway system, or to any grounded item that is permanently and reliably connected to the electrical service equipment ground.

# **REVIEW THE REAR PANEL DESIGN**

The ATLAS 800<sup>PLUS</sup> rear panel contains eight slots for housing option modules which provide a variety of additional resources and data ports. All slots are functionally identical, except slots 7 and 8. These slots can also accommodate an optional power supply for redundancy Figure 2-1 (AC powered unit) and Figure 2-2 (DC powered unit).

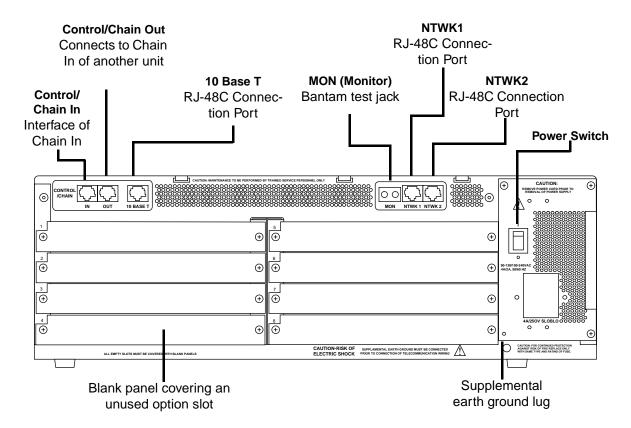


Figure 2-1. AC Powered ATLAS 800 PLUS Rear Panel

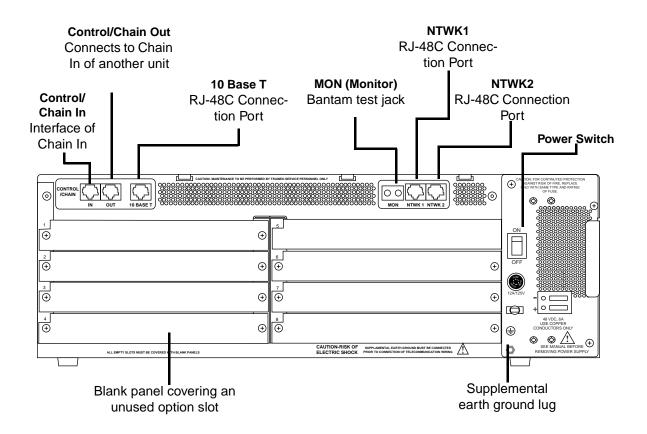


Figure 2-2. DC Powered ATLAS 800 PLUS Rear Panel

# Control/Chain In Port

The Control In/Chain In port (EIA-232) connects to a computer or modem (Control In) or to another ATLAS  $800^{PLUS}$  Base Unit (Chain In). The control port input provides the following functions:

- Accepts EIA-232 input from a PC or a modem for control of the ATLAS  $800^{PLUS}$ .
- Attaches to another ATLAS 800<sup>PLUS</sup> (chain input).
- Operates at 2400, 9600, 19200, or 38400 bps.
- Acts as input for PC control or as input for a chained connection.
- Acts as an interface for flash memory software downloads using XMODEM.

#### Connection

The Control/Chain In connection follows, with the pinout shown in Table 2-1 on page 2-5.

**Connector type** RJ-48C

Part number AMP# 555164-2

Table 2-1. Control/Chain In Pinout

PIN	NAME	DESCRIPTION
1	GND	Ground - connected to unit chassis
2	RTS	Request to send - flow control
3	RXDATA	Data received by the ATLAS 800 <sup>PLUS</sup>
4	DTR	Data terminal ready
5	TXDATA	Date transmitted by the ATLAS 800 <sup>PLUS</sup>
6	CD	Carrier detect
7	UNUSED	_
8	CTS	Clear to send - flow control

# **Control/Chain Out Port**

The Control/Chain Out port (RJ-48C) connects to another ATLAS  $800^{PLUS}$ Chain In connector. The Control/Chain Out port output provides the following:

- EIA-232 output to chain control to other ATLAS  $800^{PLUS}$  Base Units
- 2400, 9600, 19200, or 38400 bps operation
- Automatic setup; no user input required

#### Connection

The Control/Chain Out connection follows, with the pinout shown in Table 2-2.

**Connector type** RJ-48C

Part number AMP# 555164-2

Table 2-2. Control/Chain Out Pinout

PIN	NAME	DESCRIPTION
1	GND	Ground - connected to unit chassis. Connects to GND of next unit (pin1).
2	UNUSED	_
3	TX DATA	Data transmitted to chained units by the ATLAS. Connect to RX DATA of the next unit (Chain In pin 3).
4	UNUSED	_

Table 2-2. Control/Chain Out Pinout (Continued)

PIN	NAME	DESCRIPTION
5	RX DATA	Data received from chained units by the ATLAS. Connect to TX DATA of the next unit (Chain In pin 5).
6,7,8	UNUSED	_

# **Network Connection**

The two eight-pin modular jacks labeled **NTWK 1** and **NTWK 2** provide the network connection. The two Network Interface (NI) ports comply with the applicable ANSI and  $AT\&T^{@}$  standards. The NIs provide the following functions:

- AMI or B8ZS coding
- · Manual line build out
- D4 or ESF framing
- · Network performance monitoring and reporting
- · Test loopbacks with QRSS generation and checking
- Extensive self-testing

#### Connection

The network connection follows, with the pinout shown in Table 2-3 on page 2-6.

Connector type (USOC) RJ-48C Part number AMP# 555164-2

**Table 2-3. Network Pinout** 

PIN	NAME	DESCRIPTION
1	R1 RXDATA-RING	Receive data from the network
2	T1 RXDATA-TIP	Receive data from the network
3	UNUSED	_
4	R TXDATA-RING	Send data toward the network
5	T TXDATA-TIP	Send data toward the network
6, 7, 8	UNUSED	_

# **Ethernet 10BaseT Connection**

The 10BaseT Ethernet port (RJ-48C) provides an Ethernet LAN connection, which is used for TFTP, SNMP, and Telnet connection.

#### Connection

The network connection follows, with the pinout shown in Table 2-4.

Connector type (USOC) RJ-48C

Part number AMP# 555164-2

Table 2-4. Ethernet 10BaseT Pinout

PIN	NAME	DESCRIPTION
1	TX1	Transmit Positive
2	TX2	Transmit Negative
3	RX1	Receive Positive
4 & 5	UNUSED	_
6	RX2	Receive Negative
7 & 8	UNUSED	_

# MON

The MON (monitor) test jack provides a bridged access jack for non-intrusive monitoring of the T1 circuits receiving data. When connected to this jack, the test equipment should be configured for a bridged termination.

# **Option Slots**

Figure 2-3 shows the option slot numbering designation, as viewed from the rear of the ATLAS  $800^{PLUS}$ . All slots are functionally identical except slots seven and eight, which can also accommodate an optional power supply for redundancy.

SLOT 1	SLOT 5	PPLY
SLOT 2	SLOT 6	SU
SLOT 3	SLOT 7	WER
SLOT 4	SLOT 8	РО

Figure 2-3. ATLAS 800<sup>PLUS</sup> Slot Designation (Rear View)

# **INSTALL ANY OPTION MODULES**

After installing the base ATLAS  $800^{PLUS}$  Base Unit and connecting the required cables, you can install your choice of option modules. Instructions for installing option modules are given in the user manuals for the chosen modules

# **POWER-UP**

As shipped, the ATLAS  $800^{PLUS}$  is set to factory default conditions. After installing the Base Unit and any option modules, the ATLAS  $800^{PLUS}$  is ready for power-up.



You can also run a full self-test, set a pass code (UTIL menu), and set the unit ID (CONFIG menu) from the Front Panel. Please see Chapter 4 for detailed information on the Front Panel, Unit ID on page 4-9 and Set Passcode on page 4-11 for details.

# Chapter 3 Operating the ATLAS 800 PLUS

# METHODS OF OPERATING THE ATLAS 800 PLUS

You can access basic setup functions from the ATLAS  $800^{PLUS}$  Front Panel. However, to access all of the ATLAS  $800^{PLUS}$  functions, set up a Telnet session or use a VT-100 terminal emulation. In addition, T-Watch PRO provides limited configuration control. The following sections provide an overview of these methods of operating the ATLAS  $800^{PLUS}$ . After you understand the different ways to operate the ATLAS  $800^{PLUS}$ , you will be ready to configure the unit.

# **USING THE FRONT PANEL**

With the ATLAS 800<sup>PLUS</sup> powered-up, the Front Panel LCD window displays four menu items (see Figure 3-1). To select a menu item, either press the corresponding number on the Front Panel keypad or press the Front Panel up and down arrows to scroll to the menu selection. For detailed information on the Front Panel menus, see

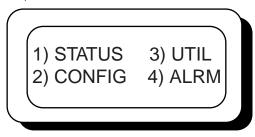


Figure 3-1. Front Panel LCD

# Example 1 Using Front Panel Menu CONFIG to Set Up the Unit ID

Figure 3-2 shows the path you would follow to set up the Unit ID from the Front Panel. The following Step/Action table provides step-by-step instructions to do the same.

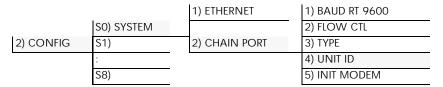


Figure 3-2. Example of Basic Front Panel Menu Navigation

Setting Up the Unit ID using the Front Panel Menu, CONFIG		
Step	Action	
1	Activate <b>CONFIG</b> by pressing the Front Panel <b>arrow keys</b> or by pressing the number <b>2</b> on the Front Panel. (The cursor flashes on the number next to the activated selection.) Press <b>Enter</b> on the Front Panel.	
2	Use the Front Panel <b>Arrow Keys</b> to view the submenu items.	
3	Select S0) System. Press Enter on the Front Panel.	
4	Activate 2) Chain Port using the Arrow Keys or by pressing 2. Press Enter on the Front Panel.	
5	Activate 4) Unit Id using the Arrow Keys or by pressing 4. Press Enter on the Front Panel.	
6	The <b>Unit Id</b> field displays. Type the new Unit ID in this field and press <b>Enter</b> on the Front Panel. The new Unit ID is now set.	

# **USING THE TERMINAL MENU**

The terminal menu provides a primary means of monitoring and configuring the ATLAS 800 PLUS. The terminal menu interface uses the full capabilities of the VT-100 terminal to provide the quickest and most intuitive operation possible. To receive the full benefit of the terminal menu interface, you should use a fully VT-100 compatible client. The ADTRAN Utilities floppy disks (that you can install on a PC) contain both a VT-100 client and a customized Telnet program. See ADTRAN Utilities on page 13-1 for details on the available programs. You can access the terminal menu using a VT-100 terminal or a computer running VT-100 terminal-emulation software.

The two basic connection methods supported by the ATLAS  $800^{PLUS}$  are a a Telnet session and a direct connection through the EIA-232 Chain In port. The following sections describe using both of these methods.

# **Using Telnet**

To connect to the ATLAS  $800^{PLUS}$  via Telnet, define the IP address, set the subnet mask, and, typically, wet the default gateway IP address. The following Step/Action tables provide instructions for performing these tasks.



You must define the IP address before attempting to connect via Telnet.

Instructions for Defining the IP Address			
Step	Action		
1	Obtain an IP address for the ATLAS 800 <sup>PLUS</sup> from your LAN administrator.		
2	From the Front Panel, select 2) CONFIG, then S0) SYSTEM, then 1) ETHERNET.		
3	When the submenu displays, select 1) IP ADDRESS.		
4	Enter the IP address by entering each number followed by <b>Enter</b> to move to the next field.		
5	Press Enter after keying in the entire IP address.		

Instructions for Setting the Subnet Mask		
Step	Action	
1	Obtain a subnet mask address from your LAN administrator.	
2	From the Front Panel, select 2) CONFIG, then S0) SYSTEM, then 1) ETHERNET.	
3	When the submenu displays, select 2) SUBNET MASK.	
4	Enter the subnet mask by entering each number followed by <b>Enter</b> to move to the next field.	
5	Press <b>Enter</b> after keying in the entire subnet mask address.	

Instructions for Setting the Gateway IP Address		
Step	Action	
1	From the Front Panel, select 2) CONFIG, then S0) SYSTEM, then 1) ETHERNET.	
2	When the submenu displays, select 3) DEF GATEWAY.	
3	Enter the default gateway by entering each number followed by <b>Enter</b> to move to the next field.	
4	Press <b>Enter</b> after keying in the entire address.	
NOTE	You will need a default gateway if the LAN contains multiple segments. Contact your LAN administrator for the appropriate address.	

# **Starting a Telnet Session**

When you begin the Telnet session, you will be prompted for a password. The default password is **password** (which is a Level 0 superuser password). You can change this password using the **Access Passwords** option, which is only accessible through the terminal menus. See *Access Passwords* on page 6-11 for details. The Telnet session will time out and display the Login prompt after a pre-defined time that is set in the **Session Timeout** option (see *Session Timeout* on page 6-8 for details).



Use the Max Telnet Sessions option to define the number of Telnet sessions that can be active at one time (see Max Telnet Sessions on page 6-8 for details).



Microsoft Telnet version 1.0 does not implement full VT-100 emulation. However, many commercial Telnet clients for Microsoft Windows exist which fully implement VT-100. In addition, a freeware client which is recommended for optimum performance is delivered with the ATLAS 800<sup>PLUS</sup>. See VT-100 Utility on page 13-8 for details.

# **Using VT-100 Terminal Emulation**

An EIA-232 serial connection is available via the Chain In port on the rear panel of the ATLAS  $800^{PLUS}$ . The ATLAS  $800^{PLUS}$  provides the Front Panel menus to a VT-100 type terminal. The following Step/Action table provides instructions for setting up the ATLAS  $800^{PLUS}$  for VT-100 terminal mode.

Instructions for Setting Up an ATLAS 800 for VT-100 Terminal Mode		
Step	Action	
1	Set the baud rate on the VT-100 terminal to 9600 baud (8/N/1).	
2	Use the Front Panel to set the ATLAS 800 <sup>PLUS</sup> baud rate to match the terminal baud rate. Select <b>2) CONFIG, S0) SYSTEM, 2) CHAIN PORT,</b> then <b>1) BAUD RATE</b> .	
3	Use the ADTRAN-provided VT-100 terminal adapter to connect the COM port of a VT-100 compatible terminal, or equivalent, to the eight-pin modular jack labeled <b>CONTROL</b> on the rear of the unit. This connection provides both local and remote configuration.	
4	Repeatedly press <b>Enter</b> on the Front Panel until the <b>Login</b> Menu appears.	

After connecting a VT-100 terminal or a computer running VT-100 terminal-emulation software to this port, you may need to press Ctrl-R to refresh the display.

When you begin the VT-100 session, you will be prompted for a password. The default password is **password** (which is a Level 0 superuser password). You can change this password using the **Access Passwords** option, which is only accessible through the terminal menu. See *Access Passwords* on page 6-11 for details.

# **Using T-Watch PRO**

T-Watch PRO is the ADTRAN Microsoft Windows management software program designed to control TSU units from a remote PC. It provides limited control over the configuration of the ATLAS 800<sup>PLUS</sup> using a graphic interface. Currently, you can choose ATLAS 800<sup>PLUS</sup> from a list of products, and T-Watch PRO automatically initiates a Telnet session by which you can connect to and manage the ATLAS 800<sup>PLUS</sup> Base Unit. Currently, T-Watch PRO automatically receives SNMP traps from an ATLAS 800<sup>PLUS</sup>.

# Chapter 4 Using the Front Panel

Use the Front Panel to select and set up the method of connectivity for controlling the ATLAS 800<sup>PLUS</sup> Base Unit and to monitor the operation and status of the Base Unit. Figure 4-1 identifies the display panels and the operation keys located on the Front Panel.

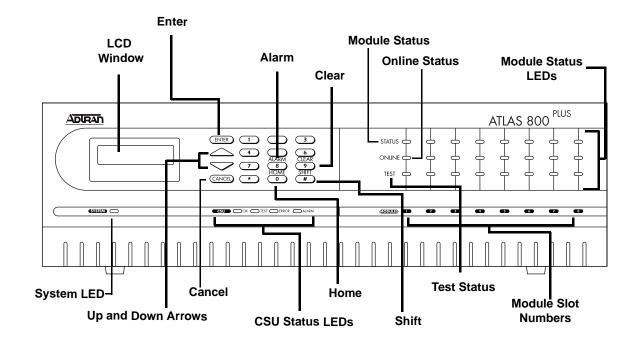


Figure 4-1. ATLAS 800<sup>PLUS</sup> Front Panel Layout

Table 4-1 on page 4-2 provides a brief description of the Front Panel features; Table 4-2 on page 4-3 provides detailed information about the LEDs; and Table 4-3 on page 4-4 provides information on operation keys.

Table 4-1. ATLAS 800<sup>PLUS</sup> Front Panel Description

Feature	Description
LCD Window	Displays menu items and messages in two lines by sixteen characters in a backlit liquid crystal display (LCD). It also displays alarm and status information.
Enter	Selects active menu items. To select a menu item, press the number of the item. The menu item flashes, indicating it is activated. Press <b>Enter</b> to select the menu item.
Alarm	Provides quick access to the active alarm display menus.
Clear	Clears data/results fields.
Module Status	Displays the operational condition of modules installed in the option slots.
Online Status	Indicates that the module is available for use or is currently in use. If the module is manually taken offline, this LED is turned off.
Module Status LEDs	Displays, by row, the operational condition ( <b>Status</b> , <b>Online</b> , and <b>Test</b> ) of each module installed in the option slots.
Module Slot Numbers	Illuminates to indicate that option modules are installed in the corresponding slot.
Test Status	Indicates that one or more ports within a module is in test.
Shift	Activates the Front Panel operation keys ( <b>Alarm</b> , <b>Clear</b> , and <b>Home</b> ). First, press <b>Shift</b> on the Front Panel. The next section describes all of the available operation keys. If you press a key without using <b>Shift</b> , the numbered item becomes active instead of the operation key.
Home	Returns to the main menu.
CSU Status LEDs	Indicates the status of both network interfaces.
Cancel	Stops the current activity and returns to the previous menu. (To return to a previous menus, repeatedly press the <b>Cancel</b> key until you reach the desired menu level.)
Up and Down Arrows	Use to scroll through and activate the submenu items available in the current menu. When the submenu items are scrolled, the flashing cursor indicates the active parameter.
System LED	Indicates the status of the entire ATLAS $800^{PLUS}$ . The System LED indicates the general status of the entire ATLAS $800^{PLUS}$ . A green light indicates that conditions are normal. A red light indicates a system problem or alarm condition.
Numeric Keypad	Contains the numbers 0 through 9, which you use to activate menu items and enter information (such as the IP address).

Table 4-2. LED Descriptions

For these LEDs	This color light	Indicates that
System	Green (solid)	No diagnosed system faults were found.
	Green (fast blink)	Flash download is in progress.
	Yellow (solid)	Fault was diagnosed, but the condition no longer exists. The condition will be recorded in the system log.
	Red (solid)	An error condition is present with either the power supply or temperature.
	Red (fast blink)	A fatal error occurred during flash download.
	Off	Power is not currently applied to the system.
CSU Status	OK (green)	Both network interfaces are operating normally with error-free operation. If either interface experiences alarms, the <b>OK</b> LED remains off.
	Test (yellow)	One of the interfaces is operating in a test mode. This includes a self-test, a test pattern, or a test loopback. When illuminated, this LED also indicates that normal data flow is not occurring in at least one of the module ports.
	Error (flashing red)	The <b>Error</b> LED indicates an error such as <b>BPV</b> (bipolar violation), <b>OOF</b> (out of frame), or <b>CRC</b> (cyclic redundancy check).
	Alarm (red)	An alarm condition has been detected. When the alarm condition is no longer valid, the <b>OK</b> LED illuminates. To view an alarm condition, select the active alarm menu item or select <b>Alarm</b> by pressing <b>Shift + 8</b> . If the alarm conditions have been corrected, you can view the alarm which caused the activation of the <b>Alarm</b> LED under the <b>View History</b> menu.
Module Status	Green (solid)	The module is OK.
	Green (blinking)	The module has been disabled by the user.
	Red (solid)	At least one port on the module has an alarm.
	Red (blinking)	The module is enabled, but is not responding to the system controller.
	Off	No module occupies the slot.
Module Online		The module is available for use or is currently in use. If the module is manually taken offline, this LED is turned off.
Module Test	Yellow (solid)	One or more ports in a module is in test.

# **OPERATION KEYS**

Operation keys are ATLAS 800 Front Panel keys that perform alternate functions. To activate an operation key, simultaneously press the Front Panel **Shift** key and the operation key that you want to activate, as shown in Table 4-3.

Table 4-3. Operation Keys

To do this	Press these keys
Access the active alarm display menus.	Shift + Alarm
(This function can be activated while any other menu item is in use.)	
Clear data/result fields in various menus.	Shift + Clear
Return to the <b>Main</b> menu from any menu location.	Shift + Home

# FRONT PANEL MENU STRUCTURE

The ATLAS  $800^{PLUS}$  uses a multilevel menu structure containing both menu items and data fields. All menu operations and data display in the LCD window. However, you only have access to limited configuration options through the Front Panel; to access all of the ATLAS  $800^{PLUS}$  options, use the Terminal menu.

The Front Panel opening menu (**Main** menu) is the access point to all other operations. Each **Main** menu item has several functions and submenus to identify and access specific parameters.

The Front Panel LCD of the **Main** menu contains the submenu options **STATUS**, **CONFIG**, **UTIL**, and **ALRM** (see Figure 4-2).

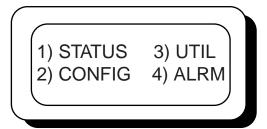


Figure 4-2. Front Panel LCD

Selecting Front Panel Menus		
To do this	Go to this menu	See also page
Display the status of the ATLAS 800 <sup>PLUS</sup>	STATUS	4-7
Display the card type in each slot	STATUS	4-7
Perform limited configuration of the ATLAS 800 <sup>PLUS</sup>	CONFIG	4-7
Monitor and modify miscellaneous settings	UTIL	4-9
View a log of system events	ALRM	4-11

Using the Front Panel Menus		
Menu Item/Activity	Comments	
Data Field	Menu items followed by a colon (:) indicate a data field that you can edit, for example, changing the baud rate. See also <i>Editing a Data Field</i> on page 4-5.	
Status Field	Menu items followed by an equal sign (=) indicate the state of the item, for example, Online.	
Select and Activate a Menu Item	To select a menu item, place the cursor on the menu item  1. by pressing the number corresponding to the menu item or 2. by highlighting the menu item with the <b>up</b> or <b>down arrows</b> .	
Exit any Menu Field Operation or Display	Press Cancel as many times as required to return to the desired menu level. or Press Home to return to the Main menu.	

Editing a Data Field		
Step	Action	
1	With the cursor positioned on the submenu item number, press <b>Enter</b> on the Front Panel. The cursor moves to the data field (to the right of the submenu item name).	
2	Use the Front Panel <b>arrows</b> to scroll and scan the available value settings. (The value settings display one at a time.)	
3	When the desired value displays, press <b>Enter</b> on the Front Panel to set the value. (When the value is set, the cursor moves back to the submenu item position, indicating the operation is complete.)	

	Editing a Data Field (Continued)		
Step	Action		
4	Select another data field to edit, or press Cancel to return to the submenu.		
NOTE	Pressing <b>Cancel</b> prior to pressing <b>Enter</b> voids any data changes. The original data value is restored and the cursor returns to the submenu field.		

# FRONT PANEL MAIN MENU

The Front Panel **Main** menu provides limited configuration and control of the ATLAS 800<sup>PLUS</sup>. Figure 4-3 shows the submenu options provided.

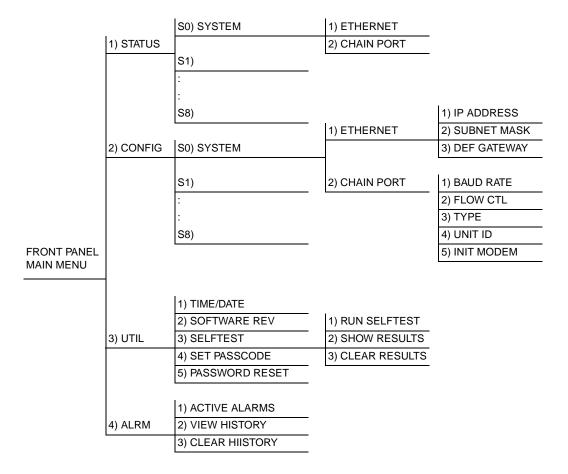


Figure 4-3. Front Panel Menu Tree

To help you follow the terminal menu hierarchy, the following notations are used.

- > MENUS
- » Submenus
- »» Sub-submenus

# > STATUS

The **Status** menu branch lets you view the status of the ATLAS 800<sup>PLUS</sup> Base Unit and any installed modules.

» S0 System

Displays status options that are available for the ATLAS 800<sup>PLUS</sup> Base Unit. Choose from **Ethernet** (see *Ethernet Status* on page 4-7) or **Chain Port** (see *Chain Port Status* on page 4-7).

»» Ethernet Status

Shows the status of the 10BaseT Ethernet connection port. The following port status options display in the LCD window. An asterisk (\*) indicates activity for the item.

TX Data is being transmitted from the 10BaseT port on the system controller.

**RX** Data is being received on the 10BaseT port.

**LNK** The current status of the 10BaseT link integrity test is indicated (*LNK* should always be on when the unit is connected to a functional 10BaseT hub).

#### »» Chain Port Status

Indicates the status of the Chain Port. The following port status options display in the LCD window. An asterisk (\*) indicates activity for the item. (Read-only.)

**RTS** Request to send.

CTS Clear To send.

**DTR** Data terminal ready.

**DCD** Data carrier detect.

## » S1—S8

Displays the current status of installed modules. **S1** corresponds to slot 1, **S2** to slot 2, and so on. When you select one of these options, an expanded description of the card status displays. The status types include **ON** (Online), **OFF** (Offline), **NRSP** (No Response), **NRDY** (Not Ready), and **RST** (Restarting).

## > CONFIG

The **Config** (Configuration) menu branch provides limited configuration control of the ATLAS 800 *PLUS*.

» S0 System

Displays configuration options that are available for the ATLAS 800<sup>PLUS</sup> Base Unit. Choose from **Ethernet Configuration** (see *Ethernet* on page 4-8) or **Chain Port Configuration** (see *Chain Port* on page 4-8).

#### »» Ethernet

Allows you to create and change configuration settings for the 10BaseT Ethernet connection.

#### IP Address

Uniquely identifies the ATLAS 800<sup>PLUS</sup> on a TCP/IP network. This address is composed of four decimal numbers, each in the range of 0 to 255, separated by periods. This value is set to 0.0.0.0 by default. The IP address is used for the 10BaseT Ethernet interface. Obtain the correct IP address from your LAN administrator. Enter the IP address by entering each number followed by **Enter** to move to the next field.



You must define the IP address before attempting to use a Telnet program.

#### Subnet Mask

Defines which part of a destination IP address is the Network number. This address is composed of four decimal numbers, each in the range of 0 to 255, separated by periods. This option is used along with the ATLAS 800<sup>PLUS</sup> IP address to determine which nodes must be reached through the default IP gateway. Enter the subnet mask address by entering each number followed by **Enter** to move to the next field.

#### **Def Gateway**

Allows you to define or change the default gateway. You will need a default gateway if the LAN contains multiple segments. This address is composed of four decimal numbers, each in the range of 0 to 255, separated by periods. This value is set to 0.0.0.0 by default. Contact your LAN administrator for the appropriate address. Enter the default gateway address by entering each number followed by **Enter** to move to the next field.

#### »» Chain Port

The **Chain Port** configuration menu option modifies selected items in its menu branch.

**Baud Rate** Displays and changes the baud rate. The supported

baud rates for the chain port include 2400 and 9600 bps. If **Type** is set to **Dial**, make sure this field matches the

modem baud rate.

**Flow Ctl** Sets the flow control for the chain port. You can config-

ure the chain port flow control for **OFF** or **H/W** (hard-

ware).

Type Sets the Port Type to either Direct or Dial. Select Direct

to connect to a local VT 100 and select Dial to connect via

a modem.

#### **Unit ID**

Accesses the current Unit ID setting, which is the system identifier used for ADTRAN Data Link Layer Protocol (ADLP) configuration control (such as using T-Watch PRO).

Editing or changing the Unit ID requires the use of a passcode if a passcode is defined. See *Set Passcode* on page 4-11 for details on working with passcodes. Unit Identification numbers must be between 2 and 9999. The number 1 is reserved for the PC.

Press **Enter** to record the Unit ID number and establish its availability when operating by remote control. Press **Cancel** at any time to end the editing process.

#### **Init Modem**

Provides the option to send the modem initialization string (e.g., ATE0V1&D2S0=1) from the chain port to a modem connected to the chain port. Configure this string in the terminal menus. See *Modem Initialization String* on page 6-9 for details on how to change this field.



The Init Modem option is only used if Type is set to Dial.

#### » S1—S8

Displays the current configuration options of installed modules. **S1** corresponds to slot 1, **S2** to slot 2, and so on. When you select one of these options, you can enable or disable the selected module. The current status, **ENA** (Enabled) or **DIS** (Disabled), displays next to the module name. Set this field to **DIS** (Disable) prior to removing a module from the ATLAS 800<sup>PLUS</sup> unit.

#### > UTIL

The **Utility** menu allows miscellaneous settings to be displayed or modified.

#### » Time/Date

Displays and/or edits the current time and date. The ATLAS 800<sup>PLUS</sup> maintains the time and date during power off conditions.

After any numeric change, press **Enter** to record the entry and move to the next editing position. You can also move to a different field to edit by pressing **Enter** at the editing position without making any change, or by using the **up** and **down arrow keys**. Press **Cancel** at any time to end the editing process.

#### » Software Rev

Displays the current software revision level loaded into the Base Unit controller. This information is required when requesting assistance from ADT-RAN Technical Support or when updates are needed. Press **Cancel** to exit this option.

#### » Selftest

Executes a system self-test, and the LCD displays the **Pass** or **Fail** when the test is complete. Options include Run Selftest, Show Results, and Clear Results.

NOTE The Selftest option disrupts data flow.

#### »» Run Selftest

Initiates a self-test. When you select this option, the prompt **Selftest**, **Are You Sure Y/N?** displays. To initiate the self-test, select **Y** and press **Enter**. Select **N** and press **Enter** to cancel the self-test.

If you select **Y** and proceed with the self-test, the LCD displays the message **Selftest in progress....** When the self-test is complete with no failures detected, the **OK** LED illuminates and the LCD momentarily displays **Self-Test Passed.** If failures are detected, a list of failures displays in the LCD window.

The full self-test procedure consists of the following steps:

- 1. Board-level tests. An on-board processor executes a series of tests checking the circuitry on the board.
- 2. RAM tests; EPROM checksum.
- 3. TDM map tests.
- 4. **On-board data path.** Sending a known test pattern through an onboard loop.
- 5. **Board-to-board interface test.** Verifies the data path, clocks, and control signals. A test pattern is sent from the controller through a loopback on all other boards and checked on the controller.

During a self-test, ATLAS  $800^{PLUS}$  checks data integrity and verifies processor control to each port. Each port is looped back and a data pattern is sent and tested.

#### »» Show Results

Displays the types of tests performed during a self-test, as well as the results of the tests. Each item in the list displays either **Passed** or **Failed**. A RAM test failure indicates a controller board problem. If a slot fails, the module in the slot may have a problem. The following items display:

NVRAM	Non-volatile RAM
DSP RAM	Digital signal processor RAM
RTC RAM	Real time clock RAM
TDM MAP	TDM time slot mapping RAM
DRAM	Dynamic program memory used for program execution
Slot 1—8	Data path test to individual modules

#### »» Clear Results

Resets the self-test log that you access with the **Show Results** option. When you select this option, the message **Self-Test Log Clearing** displays. After the command is finished executing, the message **Self-Test Log Cleared** displays.



If you clear the message log, you cannot retrieve the data.

#### » Set Passcode

Provides security for Front Panel access. You can change or set the Front Panel passcode at any time or eliminate it altogether through the **Set Passcode** option. By default, the Front Panel does not have a passcode.

The passcode can only be entered by using numbers (any number except zero). After entering the desired passcode, press **Enter**. The prompt **Verify Passcode** displays. Enter the passcode again and press **Enter**.

Set a null passcode by pressing **0** and then pressing **Enter**. When the **Verify Password** prompt displays, press **0** and **Enter** again. A null passcode grants unlimited access to Front Panel options.

#### » Password Reset

Creates a list of system passwords with the terminal menus (see *Access Passwords* on page 6-11 for details). If you forget the password and are unable to log in to the terminal menus, use the **Password Reset** option. When you select this option, two items display in the LCD window: **CHALLENGE** # and **RESPONSE** #.

Call ADTRAN technical support, and tell them the challenge number. They use this to generate a random response number. Enter this response number in the **RESPONSE** # field, and ATLAS  $800^{PLUS}$  inserts a default password into the system password list. You can then use the new default password to log into the terminal menus.

# > ALRM MENU

From the **ALRM** (alarm) menu you can view a log of system events. To control the types of events logged, a series of filters have been defined for each event source (System, T1/PRI, ISDN, Ethernet, etc.). Any event with a severity greater than or equal to the threshold defined in the event logging filter list is logged to the system event log. Events that do not appear in the event log do not appear in the Front Panel alarm lists. Therefore, the event logging filters are applied to both the terminal and the Front Panel menu lists. See *System Event Logging* on page 6-10 for details on setting the thresholds for event logging.

# » Active Alarms

Displays a list of current alarms reported by the base controller. If no alarms are current, this menu item displays **End of List**. If there are current alarms, this display includes two lines of text. The top line is the alarm source. The bottom line is the alarm message.

» View History Displays a time and date-stamped list of the alarms that have occurred in the

ATLAS  $800^{PLUS}$ . Some alarm types include **-A** to indicate the alarm is active and **-I** to indicate the alarm is inactive.

» Clear History Clears the alarm history log.



When you clear the alarm history log, you cannot retrieve the data.

# Chapter 5 Navigating the Terminal Menu

# **TERMINAL MENU WINDOW**

The ATLAS  $800^{PLUS}$  uses a multilevel menu structure that contains both menu items and data fields. All menu items and data fields display in the terminal menu window, through which you have complete control of the ATLAS  $800^{PLUS}$  (see Figure 5-1).

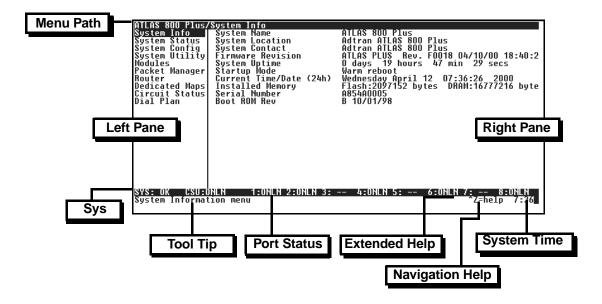


Figure 5-1. Top-level Terminal Menu Window

# Menu Path

The first line of the terminal menu window (the menu path) shows the session's current position (path) in the menu structure. For example, Figure 5-1 shows the top-level menu with the cursor on the **System Info** submenu; therefore, the menu path reads **ATLAS 800/System Info**.

# **Window Panes**

When you first start a terminal menu session, the terminal menu window is divided into left and right panes. The left pane shows the list of available submenus, while the right pane shows the contents of the currently selected submenu.

# **Window Pane Navigation**

Use the following chart to assist you in moving between and within the two window panes.

To move	Press one of these keys
From left pane to right pane	Tab Enter Left arrow Right arrow
From right pane to left pane	Tab Escape Left arrow Right arrow
Within each pane	Up arrow Down arrow Left arrow Right arrow

## **Right Window Pane Notation**

The right window pane shows the contents of the currently selected menu. These contents can include both submenu items and data fields. Some submenus contain additional submenus and some data fields contain additional data fields. The following chart explains the notation used to identify these additional items.

This notation	Means that
[+]	More items are available when selected.
[DATA]	More items are available when selected.
<+>	An action is to be taken, such as activating a test.
Highlighted menu item	You can enter data in this field.
Underlined field	The field contains read-only information.

# **Additional Terminal Menu Window Features**

**Sys** Describes the status of the ATLAS base unit (system).

**Tool Tip** Provides a brief description of the currently selected

(highlighted) command.

**Port Status** Displays status information, such as OK, WARN, or

ALRM, about ports 1—8.

**Extended Help** Displays information about selected commands

(Ctrl-A).

**Navigation Help** Lists characters used for navigating the terminal menu

(Ctrl-Z). See also Moving through the Menus on page 5-3

**System Time** Displays current time. See *Current Time/Date (24h)* on

page 6-3 for details on editing the time.

# **NAVIGATING USING THE KEYBOARD KEYS**

You can use various keystrokes to move through the terminal menu, to manage a terminal menu session, and to configure the system. Press **Ctrl-Z** to activate a pop-up screen listing the navigation keystrokes.

# Moving through the Menus

To do this	Press this key
Return to the home screen.	Н
Jump between two menu items.	J
Press <b>J</b> while the cursor is located on a menu item, and you jump back to the main screen.	
Go to another menu item, press <b>J</b> , and you jump back to the screen that was displayed the first time you pressed <b>J</b> .	
Press $oldsymbol{J}$ anytime you want to jump between these items.	
Select items.	Arrows
Edit a selected menu item.	Enter
Cancel an edit.	Escape
Close pop-up help screens.	Escape
Move between the left and right panes.	Tab Arrows
Move to the top of a screen.	A

Move to the bottom of a screen.	Z
Ascend one menu level.	Backspace

# **Session Management Keystrokes**

To do this	Press this
Log out of a session.	Ctrl-L
Invalidate the password entry and return to the login screen.	Ctrl-S
Refresh the screen.	Ctrl-R
To save time, only the portion of the screen that has changed is refreshed. This option should only be necessary if the display picks up incorrect characters.	
The System Status bar can toggle to a full view of the current value highlighted by the cursor. Ctrl-V toggles between the extended data view and the System Status view.	Ctrl-V
While in the extended data mode, if the cursor highlights an element with no useful information, the System Status is displayed.	

# **Configuration Keystrokes**

To do this	Press this key
Restore factory default settings.	F
This setting restores the factory defaults based on the location of the cursor. If the cursor is on a module line (in the <b>Modules</b> menu), then only the selected module is updated to factory defaults.	
Copy selected items to the clipboard.	С
The amount of information you can copy depends on the cursor location when you press <b>C</b> :	
If the cursor is over an editable field, only that item is copied.	
<ul> <li>If the cursor is over the index number of a list, then all of the items in the row of the list are copied. For example, if the cursor is over the Slot # field in the Modules screen, all of the information associated with the slot is copied.</li> </ul>	

To do this	Press this key
Paste the item stored in the clipboard, if the information is compatible.	Р
You must confirm all pastes—except those to a single editable field.	
Increment the value of certain types of fields by one when you paste information into those fields.	>
Decrement the value of certain types of fields by one when you paste information into those fields.	<
Insert a new list item.	I
For example, add a new item to the <b>Dedicated Map</b> connection list by pressing <b>I</b> while the cursor is over the index number.	
Delete a list item.	D
For example, delete an item from the <b>Dedicated Map</b> connection list by pressing <b>D</b> while the index number is active.	

# **Getting Help**

The bottom line of the terminal menu window contains context-sensitive help information. When the cursor is positioned over a set of configuration items, a help message displays (when available) providing a description of the item. When more detailed help is available for a particular item, ^A displays at the bottom of the window. At this point, if you press Ctrl-A, a popup help screen displays with information about the item.

Press **Ctrl-Z** to activate a help screen that displays the available keystrokes you can use to navigate the terminal menu.

# Chapter 6 Terminal Menu and System Control

# **SELECTING THE APPROPRIATE MENU**

The terminal menu is the access point to all other operations. Each terminal menu item has several functions and submenus that identify and provide access to specific operations and parameters. Use the chart below to help you select the appropriate terminal menu.

To do this	Go to this menu	For more info
Review and monitor general system information for the ATLAS 800 PLUS.	System Info	See page 6-2.
Review and monitor system status for the ATLAS 800 <sup>PLUS</sup> .	System Status	See page 6-3.
Set up the operational configuration for the ATLAS 800 <sup>PLUS</sup> .	System Config	See page 6-7.
Update settings, transfer files, perform system diagnostics, and reboot the ATLAS 800 <sup>PLUS</sup> .	System Utility	See page 6-13.
Review and configure settings for each installed module, including the ATLAS 800 <sup>PLUS</sup> Base Unit.	Modules	See page 7-1.
Assign dedicated connections between any two ports in the ATLAS $800^{PLUS}$ .	Dedicated Maps	See page 8-1.
View the status of all Dedicated Circuit backups that may be configured.	Circuit Status	See page 9-1.
Set global ATLAS $800^{PLUS}$ switch parameters or set individual parameters for each port in ATLAS $800^{PLUS}$ that handles a switched call.	Dial Plan	See page 10-1.

# **SECURITY LEVELS**

To edit terminal menu items, you must have a password and the appropriate security level. Table 6-1 describes the six security levels. See *Access Passwords* on page 6-11 for additional information on working with passwords.

Description Security Level 5 Read-only permission for all menu items—minimum rights. 4 Read permission for all menu items and permission to use test commands. 3 Access to all commands except passwords, flash download, authentication methods, and interface configurations. 2 Access to all commands except passwords, flash download, and authentication methods. 1 Access to all commands except passwords. 0 Permission to edit every menu item, including creating and editing passwords—maximum rights.

**Table 6-1. Password Security Levels** 

To help you follow the terminal menu hierarchy, the following notations are used.

- > MENUS
- » Submenus
- »» Sub-submenus

# > SYSTEM INFO

The **System Info** menu provides basic information about the unit as well as data fields for editing information. Figure 6-1 displays the submenus that are available when you select this menu item.



Figure 6-1. System Information Menu

### » System Name Security level: 3; Read security: 5

Provides a user-configurable text string for the name of the ATLAS 800<sup>PLUS</sup>. This name can help you distinguish between different installations. You can enter up to 40 alpha-numeric characters in this field, including spaces and special characters (such as an underbar). This name also displays on the LCD Front Panel.

# » System Location

## Security level: 3; Read security: 5

Provides a user-configurable text string for the location of the

ATLAS 800<sup>*PLUS*</sup>. This field is to help you keep track of the actual physical location of the unit. You can enter up to 40 alphanumeric characters in this field, including spaces and special characters (such as an underbar).

#### » System Contact

#### Security level: 3; Read security: 5

Provides a user-configurable text string for a contact name. You can use this field to enter the name, phone number, or email address of a person responsible for the ATLAS  $800^{PLUS}$  system. You can enter up to 40 alpha-numeric characters in this field, including spaces and special characters (such as an underbar).

#### » Firmware Revision

#### Read security: 5

Displays the current firmware revision level of the controller.

#### » System Uptime

#### Read security: 5

Displays the length of time the ATLAS  $800^{PLUS}$  system has been running. Each time you reset the system, this value resets to 0 days, 0 hours, 0 min and 0 secs.

#### » Startup Mode

#### Read security: 5

Displays details about the last system startup.

# » Current Time/Date

(24h)

## Security level: 3; Read security: 5

Displays the current date and time, including seconds. This field can be edited. Enter the time in 24-hour format (such as 23:00:00 for 11:00 pm). Enter the date in mm-dd-yyyy format (for example, 10-30-1998).

#### » Installed Memory

#### Read security: 5

Displays the type and amount of memory in use (including Flash memory and DRAM).

## » Serial Number

#### Read security: 5

Displays the serial number for the unit. The serial number of the  $\,$ 

ATLAS 800<sup>PLUS</sup> will automatically display in this field.

#### » Boot ROM Rev

#### Read security: 5

Displays the boot ROM revision.

# SYSTEM STATUS

The **System Status** menu provides information on the status of the unit. Figure 6-2 shows the submenu functions available in the **System Status** menu.

```
ATLAS 800 Plus/System Status
System Info
System Status
System Config
System Config
System Config
System Config
System Utility
Modules
Packet Manager
Router
Dedicated Maps
Circuit Status
Dial Plan

Chain Port Signal Leads
Chain Port Signal Leads
Chain Port System System
Chain Port System
Chain Port System
Chain Port Rx Bytes
Chain Port Countrs

Chain Port Countrs

Chain Port Countrs

System Status menu

Temp Fail[-] PS1 Fail[-] PS2 Fail[-]
PRIMARY: Locked
[+]
FINANCY
[+]
FINANCY
```

Figure 6-2. System Status Menu

# » Event Log

#### Read security: 5

Displays the last 350 warning or failure messages sent—including the day, date, and priority of the message. The most recent messages display at the top of the list. The following read-only fields are available to review:

Time Event Log/Time	Displays the date (in mm/dd format) and the time (in hh:mm:ss format) that the event occurred.
Category	Displays the severity of the event. The possible categories are Critical, Major, Minor, Warning, Normal, and Info. You can specify which types of errors you want the system to log with the System Event Logging option. See <i>System Event Logging</i> on page 6-10 for details.
Slot	Displays the slot number in which the event occurred. If this field displays a dash (—), the event occurred in the ATLAS $800^{PLUS}$ base unit.

**Port** Displays the port in which the event occurred.

**Description** Displays a description of the event.

# » Clear System Event Log

#### Write security: 3; Read security: 5

Clears the event log. When you select the command, the following prompt displays: This will clear the entire event log. Confirm (y/n). Select Y to clear the log or N to exit the command.



If you clear the event log, you cannot retrieve the data.

## » Ethernet Port Read security: 5

Displays status information about the Ethernet port. An asterisk (\*) indicates activity for the item. The following read-only fields are available to review:

**I/F Status** Indicates the current status of the 10BaseT port.

**Tx Frames** Indicates the number of frames transmitted from the

10BaseT port since system startup.

**Rx Frames** Indicates the number of frames received on the 10BaseT

port since system startup.

# » Clear System LED Write security: 3; Read security: 5

Changes the color of the system LED on the front panel from yellow (indicating a previous error) to green (OK). The system LED turns red if the ATLAS  $800^{PLUS}$  detects a major system failure. If the failure condition clears, the LED turns yellow and remains yellow to warn of the past failure.

# » System Alarms Read security: 5

Indicates the status of major system components. An asterisk (\*) indicates activity for the items. The following read-only fields display in this field:

**Temp Fail** The system's internal temperature is outside normal limits.

**PS1 Fail** The main power supply is not functioning correctly.

**PS2 Fail** The backup power supply is not functioning correctly.

## » System Timing Source

#### Read security: 5

Indicates which timing source (primary or backup) is currently being used by ATLAS and if ATLAS is locked onto this source. If the display does not indicate locked, the ATLAS 800<sup>PLUS</sup> does not have a valid source of timing and cannot reliably transfer data. Review the current setting for system timing source in the **System Config** menu. See *Primary Timing Source* on page 6-7 and *Backup Timing Source* on page 6-7 for details.

#### » Resource Usage

#### Write security: 4; Read security: 5

Indicates resource use (analog modems; digital modems; voice compression).

#### » Data Tables

**Resource Type** Displays the system resources list.

**Current** Shows the number of resources available (not in use)

and the total number of resources. If a resource is tak-

en off line, it is not included in the total.

**Average** Shows the average number of resources available

since the statistics were last reset.

**Minimum** Shows the fewest number of resources available since

the last reset.

0 (zero) available Provides a count of the number of times the quantity

of available resources reached 0.

**Hour Data** Shows availability information by hour for a 24-hour

period.

Reset Activates the reset of all accumulated availability sta-

tistics.

» Configuration Write security: 4; Read security: 5

Configures the statistics displayed under data tables.

**Display Formt** Selects the statistics display format—Raw Data or %.

Reset Mode Selects the mode for resetting statistics—Manual, Dai-

ly, or Weekly.

» Trunk Usage Write security: 4; Read security: 5

This provides DS0 usage tracking for Dial Plan connections.

» Data Tables

**Trunk Type** Displays the types of trunks in the system.

Current Shows the number of DS0s available (not in use) and

the total number of DS0s.

**Average** Shows the average number of DS0s available since the

statistics were last reset.

**Minimum** Shows the fewest number of DS0s available since the

last reset.

0 (zero) available Provides a count of the number of times the quantity

of available resources reached 0.

SIt/Prt Displays the usage data broken down by slots and

ports.

Reset Activates the reset of all accumulated availability sta-

tistics.

» Chain Port Signal

Leads

Read security: 5

Displays the state of the following options (these fields are read-only). An asterisk (\*) indicates activity for the item.

**RTS** Request to send.

CTS Clear to send.

**DTR** Data terminal ready.

DCD Data carrier detect. » Chain Port Tx
Read security: 5

**Bytes** Displays the number of transmitted data bytes.

» Chain Port Rx Read security: 5

**Bytes** Displays the number of received data bytes.

» Chain Port Read security: 5

**Overrun Errs** Displays the number of overrun errors.

» Chain Port
Read security: 5

**Framing Errs** Displays the number of received framing errors.

» Clear Chain Port

Countrs

Clears all chain port counters. Press **Y** to activate command.

# > SYSTEM CONFIG

The **System Config** menu allows you to set up the ATLAS operational configuration. Figure 6-3 shows the items included in this menu.

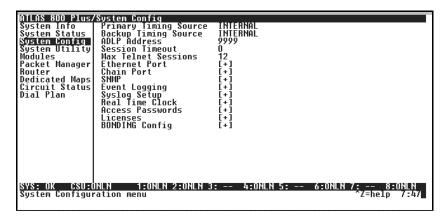


Figure 6-3. System Configuration Menu

» Primary Timing Source

Source

Write security: 3; Read security: 5

Selects the primary timing source. You can select either INTERNAL or a port from one of the installed modules.

» Backup Timing Write secu

Write security: 3; Read security: 5

Selects the secondary timing source. You can select either INTERNAL or a port from one of the installed modules. ATLAS  $800^{PLUS}$  uses the backup timing source if the primary timing source goes into alarm. The <code>Backup Timing Source</code> should be different from the <code>Primary Timing Source</code>.

» ADLP Address

Write security: 2; Read security: 5

Shows the system ADTRAN Data Link Layer Protocol (ADLP) address for connecting remote devices to management software (such as T-Watch PRO). The allowable range is between 2 and 65520. Enter a value not used by any of the TSU units controlled by the management software.

### » Session Timeout

### Write security: 3; Read security: 5

Defines the number of seconds the terminal session must remain idle before the session times out. You can enter zero to deactivate this option (the session will never time out).

### » Max Telnet Sessions

### Write security: 3; Read security: 5

Defines the maximum number of Telnet sessions that can be active at the same time. Enter a number between 0 and 100 in this field.



If you enter zero in this field, you will not be able to use Telnet. Only enter zero if you want to completely lock out Telnet access.

### » Ethernet Port

### Write security: 2; Read security: 5

Provides a way to configure various settings for the Ethernet port. The following options are available for review and editing:

**Port Name** Defines the name of the Ethernet port. You can leave this

field blank.

**IP Address** Lists the address assigned to the base Ethernet port. This

address is composed of four decimal numbers, each in the range of 0 to 255, separated by periods. This value is set to 0.0.0.0 by default. The IP address is used for the 10BaseT Ethernet interface. Obtain the correct IP address from your

LAN administrator.

### Default Gateway

Defines or changes the default gateway. Enter the default gateway address by entering a decimal number into the appropriate field and then pressing **Enter** to move to the next field. You will need a default gateway if the LAN contains multiple segments. This address is composed of four decimal numbers, each in the range of 0 to 255, separated by periods. This value is set to 0.0.0.0 by default. Contact your LAN administrator for the appropriate address.

### Subnet Mask

Defines which part of a destination IP address contains the network number. This address is composed of four decimal numbers, each in the range of 0 to 255, separated by periods. This value is set to 0.0.0.0 by default. This part of the destination IP address is used along with the ATLAS  $800^{PLUS}$  IP address to determine which nodes must be reached

through the default IP gateway.

### » Chain Port

### Write security: 2; Read security: 5

Accepts input for configuring the chain-in port.

### »» Port Name

### Write security: 2; Read security: 5

Defines the name of the chain port. Type in an alpha-numeric name up to 57 characters long. The name can include spaces and special characters.

»» Port Type Write security: 2; Read security: 5

Specifies whether you use **Direct** or **Dial** mode.

»» Port Speed Write security: 2; Read security: 5

Specifies the baud rate of the port. Select either 2400, 9600, 19200, or 38400. If you are using **Dial** for **Port Type**, ensure that the **Port Speed** setting

matches the modem baud rate.

»» Modem Write security: 2; Read security: 5

**Initialization String** Specifies the initialization string for a modem. Refer to your modem docu-

mentation for acceptable initialization strings.

»» Initialize Modem Write security: 4; Read security: 5

Sends the Modem Initialization string to the modem. When you select this command, the following message displays: Please verify a modem is connected to the chain port before continuing. Confirm (y/n). Ensure that a

modem is connected before selecting Y.

»» Flow Control Write security: 2; Read security: 5

This option sets the flow control for the chain port. You may configure the

chain port flow control for OFF or H/W (hardware).

» SNMP Write security: 3; Read security: 5

Provides a way to configure SNMP access for the ATLAS 800<sup>PLUS</sup>. For detailed information on SNMP, refer to *SNMP Management* on page 12-1.

The following options are available for review and editing:

**»» SNMP Access** Write security: 3; Read security: 5

Defines whether SNMP access to the ATLAS 800<sup>PLUS</sup> is enabled or disabled.

Select the appropriate option.

»» SNMP Communities Write security: 3; Read security: 5

Defines SNMP manager(s) characteristics as follows:

**IP Address** Specifies the IP address of the network manager.

**Privileges** Defines Get (read-only) and Get/Set (read and write) privi-

leges.

**Get Name** Defines the community name for Get access. This value

must match the Get name defined on the network manage-

ment station. Public is the default name.

**Set Name** Defines the community name for Set access. This value must

match either the Get or Set name defined on the network

management station. Public is the default name.

»» Trap Transmission Write security: 3; Read security: 5

Enables and disables SNMP trap transmission.

»» Authen Trap Write security: 3; Read security: 5

**Transmission** Enables and disables the authentication failure trap.

### »» Traps Destination

### Write security: 3; Read security: 5

Defines the destination for SNMP traps as follows:

**IP Address** Identifies the IP address to which the network manager

sends traps.

**Community** Defines the community name for trap destinations.

This name must match the community name defined at

the network management station.

**Trap Filtering** Sets the minimum severity level required for a system

event to generate an SNMP trap.

If a trap event occurs and if the trap's severity level is equal to or more severe than the trap type's current threshold setting, that event is sent as an SNMP trap. (Refer to the ATLAS  $800^{PLUS}$  MIB for a listing of all

traps and their severity levels.)

You can set the following threshold levels for the available selections: disabled, critical, major, minor, warn-

ing, normal, and info.

### » System Event Logging

### Write security: 3; Read security: 5

Sets the system event severity level threshold for each of the

ATLAS  $800^{PLUS}$  system event types. Whenever a system event occurs, that event is logged if the event's severity level is equal to or more severe than the event type's current threshold setting. See *System Event Logging* on page

A-1 for detailed information on the system events.

### » Syslog Setup

### Write security: 3; Read security: 5

Configures the ATLAS Syslog client for use with a Syslog server (supplied on ADTRAN /Utility disk or available on most UNIX platforms).

**»» Transmission** Enables or disables the transmission of log events to the external Syslog

server.

»» **Host IP Address** Lists the IP address of the external server that is running the Syslog host dae-

mon.

**»» Host Facility** Specifies the facility destination of log events. Facilities are located on the

host and are managed by the Syslog host daemon running on either a UNIX

machine or a PC.

» Real Time Clock Write security: 3; Read security: 5

Provides access to the following two options that you can review and edit:

»» **Current Time/Date** Displays the current date and time, including seconds. To edit this field, enter the time in 24-hour format (such as 23:00:00 for 11:00 pm), and enter the

date in mm-dd-yyyy format (for example, 09-23-1998).

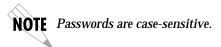
»» Auto Daylight Savings When enabled, automatically updates the time and date when Daylight Sav-

ings Time starts and, also, when Standard Time starts.

## » Access Passwords Write security: 0; Read security: 5

Provides a way to edit passwords and, also, to add new users and passwords. All menu items are protected by passwords of varying security levels. By assigning different passwords to different security levels, the ATLAS system administrator can control which users can change various menu items. You can assign multiple passwords at the same access level. This way, different users with the same access privileges can have different passwords.

Each of the six password security levels are described in Table 6-1 on page 6-2.



Instructions for Adding/Deleting Passwords	
To add a new password	Select the first column (0) and press I
To delete a password	select the first column (0) and press D.



If you lose or forget the ATLAS 800<sup>PLUS</sup> system administrator password, contact ADTRAN technical support for help in resetting the **NOTE** password. In order to reset the password, you must have access to the front panel. For details on resetting the password, see Password Reset on page 1-30.

### »» Label

### Write security: 0; Read security: 5

Defines a user name.

### »» Access Rights

### Write security: 0; Read security: 5

Defines the password level for the corresponding label. You can select from six different password levels (see also Table 6-1 on page 6-2).

### »» Password

### Write security: 0; Read security: 5

Allows you to change the password (the default password is password). The current password displays as a series of asterisks (\*\*\*\*\*\*\*).

**NOTE** Passwords are case-sensitive.

Instructions for Changing Passwords		
Step	Action	
1	Select the <b>Password</b> field—a new <b>Password</b> field displays.	
2	Type the new password in the <b>Enter</b> field.	
3	Type the new password again in the <b>Confirm</b> field.	
NOTE	The password can contain up to 12 alphanumeric characters. You can also use spaces and special characters in the password.	

### »» Active

### Write security: 0; Read security: 5

Displays the number of users for each label that are currently logged into the system.

### » Bonding Config

### Write security: 5; Read security: 5

Displays the configuration submenus available for the IMUX Nx56/64 modules. This configuration is shared among all IMUX modules.

### »» TXINIT Timer

### Write security: 3; Read security: 5

Specifies the length of time the originating endpoint attempts to detect the BONDING negotiation pattern from the answering endpoint before deciding the BONDING call has failed.

### »» TXFA Timer

### Write security: 3; Read security: 5

Specifies the length of time both endpoints attempt to detect the BONDING frame pattern when a call is connected before deciding the BONDING call has failed. When interoperating with other manufacturers' BONDING equipment, it may be necessary to change this time so that it matches TXADD01.

### »» TXADD01 Timer

### Write security: 3; Read security: 5

Specifies the length of time both endpoints wait for additional calls to be connected at the end of negotiation before deciding that the BONDING call has failed. The factory default setting is sufficient for most calls to connect, although when dialing overseas it may be necessary to lengthen this timer to allow for slower call routing.

### **»» TXDEQ Timer**

### Write security: 3; Read security: 5

Specifies the length of time both endpoints attempt to equalize the network delay between the bearer channels before deciding the BONDING call has failed.

### »» TANULL Timer

### Write security: 3; Read security: 5

Specifies the length of time the answering endpoint attempts to detect the BONDING negotiation pattern from the originating endpoint before deciding the BONDING call has failed. It may be necessary to shorten this timer if the DTE equipment using the BONDING module also has timer constraints for completing non-BONDING parameter negotiation.

# »» TCID Timer Write security: 3; Read security: 5

Specifies the length of time both endpoints attempt to negotiate an agreeable value for bearer channels and channel capacities before deciding the BONDING call has failed.

### »» Call Stagger

### Write security: 3; Read security: 5

Specifies the amount of delay between placing calls for outgoing BOND-ING sessions. Table 6-2 defines the call stagger values.

Table 6-2. Call Stagger Values

Display value	Meaning
No Stagger	There is no delay between the call dialing of a BONDING session.
500 ms	Wait approximately $\frac{1}{2}$ second between the call dialing of a BONDING session.
1 sec	Wait approximately 1 second between the call dialing of a BONDING session.
2 sec	Wait approximately 2 seconds between the call dialing of a BONDING session.

## > SYSTEM UTILITY

Use the **System Utility** menu to view and set the system parameters shown in Figure 6-4.

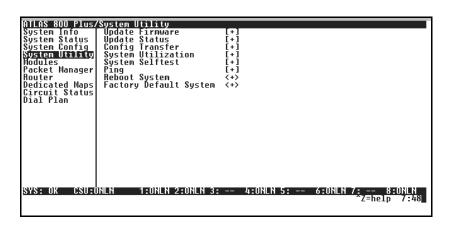


Figure 6-4. System Utility Menu

### » Update Firmware

### Write security: 1; Read security: 5

Updates firmware when ATLAS 800<sup>PLUS</sup> enhancements are released. Two transfer methods are available for use in updating any modules that contain Flash memory—including the ATLAS system controller.

The first transfer method uses the ATLAS serial Chain-In port of the system controller and XMODEM protocol. For detailed information on how to update firmware using this method, see *XMODEM Firmware Updates* on page 11-1.

The second transfer method uses the ATLAS built-in Ethernet port of the system controller and TFTP (Trivial File Transfer Protocol). For detailed in-

formation on how to update firmware using this method, see TFTP Firmware Updates on page 11-4.



The available update options vary depending on whether you select Slot 0, Slots 1 through 8, or All Modules of a Type.

### »» Module Slot

### Write security: 1; Read security: 5

Displays the slot you selected for firmware updating. When this option first appears, None Selected displays. When you move the cursor to this field and press Enter, a dialog box opens, allowing you to select Slot 0 through Slot 8 or All Modules of a Type. (All Modules of a Type is useful if several identical modules are installed in the ATLAS 800 PLUS).

### »» Module Type

### Write security: 1; Read security: 5

Reflects the module type selected in **Module Slot**. This is normally a readonly field; however, if you selected All Modules of a Type, you must select a particular module type to update all modules of that type. The selections only include upgradable modules.

#### »» Transfer Method

### Write security: 1; Read security: 5

Lists the two transfer methods for updating firmware: XMODEM and TFTP. XMODEM transfers files by connecting to a communications program that supports XMODEM uploads to the terminal interface. TFTP transfers files by specifying an appropriate server address and filename:

### TFTP Server Write security: 1; Read security: 5

**IP Address** 

Configures the IP address of the TFTP server on which the update file resides. ATLAS uses this field to locate the network server on which the update file resides.

TFTP Server Write security: 1; Read security: 5

Filename

Identifies the name of the update file to retrieve from the TFTP server. (Enter the full path name and filename for the file.)

### »» Restart Schedule

### Write security: 1; Read security: 5

Indicates when to restart the updated module to invoke the new code. The two options include Restart Immediately After Update and Restart at Specified Date and Time:

### Restart Immediately After Update

Automatically restarts the module immediately after the update is complete.

### Restart at Specified **Date and Time**

Lets you specify a date and time to automatically restart the updated module. (When you select this option, a new field called Restart Date and Time displays below the current field.)

### Restart Date and Time Write security: 1; Read security: 5

Defines the date and time to restart the system.

- Enter the time using a 24-hour format (i.e., 23:00:00 for 11:00 pm).
- Enter the date in mm-dd-yyyy format (i.e., 10-30-1998).



Restart at Specified Date and Time is only available for the System Controller— not for modules residing in expansion slots, since they are unable to maintain normal operation during the update process.

### »» Current Update Status

### Read security: 5

Indicates progress or problems encountered during the current update process. The field displays **Idle** if no update is in progress or when the update is successfully completed. At the end of a successful update, the contents of this field are copied into Previous Update Status.

If you are updating several modules at the same time (if **Module Slot** is set to All Modules of a Type), this option displays [+], indicating this field contains submenu items. The following submenus display:

SIt Indicates the slot number.

**Type** Defines the type of module for each slot.

Current Status Indicates the status of the current update.

Previous Indicates the status of the previous update. Status

**Previous Time** Indicates the time of the previous update.

During the TFTP upload process, various status messages are provided in **Current Update Status** (see Table 11-1 on page 11-5).

### »» Previous Update Status

### Read security: 5

Displays the status of the previous update. If a firmware update has not been attempted for a particular slot, this field reads, Has not been attempted. Following a successful update the field reads, Module Update Complete. If an update was unsuccessful, the appropriate error message displays.

### »» Begin Firmware Update

### Write security: 1; Read security: 5

Begins updating the firmware for the selected modules. To start this action, enter Y to begin or enter N to cancel. You can also cancel the operation after the update has begun. For XMODEM updates, cancel the process via the terminal emulation software (consult your documentation for information

on how to do this). For TFTP updates, you can cancel the process by selecting **Cancel Update** from this field.

### » Update Status

### Read security: 5

Displays the status of the current firmware update. These fields are identical to those defined in *Current Update Status* on page 6-15.

### » Config Transfer

### Write security: 3; Read security: 5

Used only with TFTP transfers. Sends a file containing the ATLAS 800<sup>PLUS</sup> configuration to a file on a TFTP server using the TFTP protocol through the 10BaseT Ethernet port. **Config Transfer** also lets you save the

ATLAS 800<sup>*PLUS*</sup> configuration as a backup file, so you can use the same configuration with multiple ATLAS 800<sup>*PLUS*</sup> units. In addition, **Config Transfer** can retrieve a configuration file from a TFTP server.

To support these transfers, ADTRAN delivers a TFTP program with ATLAS 800<sup>PLUS</sup> called *TFTP Server*. You can configure any PC running Microsoft Windows with this software, and store a configuration file. See *TFTP Server* on page 13-10 for details on how to use *TFTP Server*.



Before using Config Transfer, the ATLAS 800<sup>PLUS</sup> should have a valid IP address, subnet mask, and default gateway (if required), and should be connected to an Ethernet network.

Only one configuration transfer session (upload or download) can be active at a time. The TCP/IP parameters are not saved or overwritten as part of an ATLAS  $800^{PLUS}$  unit's transferred configuration; this way, identical configurations can be sent to multiple units.

### »» Transfer Method

### Write security: 3; Read security: 5

Displays the method used to transfer the configuration file to or from a server. Currently, you must use TFTP.

### »» TFTP Server IP Address

### Write security: 3; Read security: 5

Specifies the IP address of the TFTP server. Get this number from your system administrator.

# »» TFTP Server Filename

### Write security: 3; Read security: 5

Defines the name of the configuration file that you transfer to or retrieve from the TFTP server. The default name is **atlas.cfg**, but you can edit this name.

# »» Current Transfer Status

### Read security: 5

Indicates the current status of the update.

### »» Previous Transfer Status

### Read security: 5

Indicates the status of the previous update.

### »» Load and Use Config

### Write security: 3; Read security: 5

Retrieves the configuration file specified in the TFTP Server Filename field from the server. To start this command, enter  ${\bf Y}$  to begin or enter  ${\bf N}$  to cancel.



If you execute this command, the ATLAS 800<sup>PLUS</sup> retrieves the configuration file, reboots, then restarts using the new configuration.

# »» Save Config Remotely

### Write security: 3; Read security: 5

Saves the configuration file specified in **TFTP Server Filename** to the server identified in **TFTP Server IP Address**. To start this command, enter **Y** to begin or enter **N** to cancel.



Before using this command, you must have identified a valid TFTP server in TFTP Server IP Address.

### » System Utilization

### Write security: 0; Read security: 0

Displays statistics related to the ATLAS internal operating system. Please check with ADTRAN Technical Support before attempting to use this menu.

### » System Selftest

### Write security: 3; Read security: 5

Initiates a system self-test. The self-test consists of memory tests and data integrity tests for each installed module.



Self-tests disrupt data flow.

### »» Selftest Run

### Write security: 3; Read security: 5

Activates the self-test. To confirm self-test activation, press  $\mathbf{y}$ ; to cancel the self-test press  $\mathbf{n}$ .

### »» Status

### Security level: 3; Read security 5

Indicates a system self-test. The self-test consists of memory tests and data integrity tests for each installed module.

### »» View Selftest Log

### Read security: 5

Displays time-stamped log of the tests conducted and the Pass/Fail results. Self-tests verify data integrity and processor control to each port. Each port is looped back and a data pattern is sent and tested.

The result of the self-test on each installed port is listed with Pass/Fail results. A typical test log is shown in Figure 6-5. The log includes the following additional fields.

**Index** Index number of the log

**Time** Time and date of the log entry

SI ATLAS slot number

Pt ATLAS port number

**Event** Event description

**Result** Shows Pass/Fail results

The tests associated with the system controller include the following:

This event	Logs this result
Flash	Flash memory checksum verified.
BootRom	Boot ROM checksum verified.
DSP RAM	Memory associated with the DTMF DSP.
RTC RAM	Memory associated with the real time clock.
TDM RAM	Memory associated with mapping TDM bandwidth.
DRAM	Dynamic RAM used for program execution.

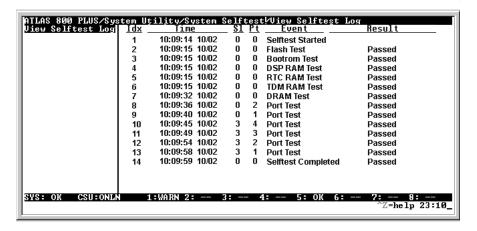


Figure 6-5. View Self-test Log

»» Clear Self-test Log Write security: 3; Read security: 5

Clears the self-test log.

» Ping Write security: 5; Read security: 5

Allows you to send pings (ICMP requests) to devices accessible via the net-

work.

NOTE

Only ping one session can be active at a time.

»» IP Address Write security: 5; Read security: 5

Specifies the IP address to ping.

»» Count Write security: 5; Read security: 5

Specifies the number of pings to send. The default number is, and the maxi-

mum value is 99.

»» Size Write security: 5; Read security: 5

Specifies the size in bytes of the data portion of the ping request. The

default value is 64 bytes, and the maximum size is 1024 bytes.

»» Timeout Write security: 5; Read security: 5

Specifies the time in milliseconds to wait for the ping reply before timing

out. The default timeout is three seconds, and the maximum timeout value

is ten seconds.

»» Round trip min Read security: 5

Displays the minimum round trip time of the ping request/reply of the cur-

rent set of pings.

»» Round trip avg Read security: 5

Displays the average round trip time of the ping request/reply of the cur-

rent set of pings.

»» Round trip max
Read security: 5

Displays the maximum round trip time of the ping request/reply of the cur-

rent set of pings.

»» Tx Stats Read security: 5

Displays the number of ping requests transmitted ( ${\bf n}$  txed), the number of

ping replies received (n rxed) and the number of ping requests that were

lost (n lost).

»» Reset Stats
Write security: 5; Read security: 5

Resets all ping statistics to zero. If the ping client is active, this menu will

stop it.

»» Start/Stop Write security: 5; Read security: 5

If the ping client is currently idle, this menu sends pings to the specified

address. If the ping client is active, the menu sends stops sending pings.

» Reboot System Write security: 2; Read security: 5

Reboots the ATLAS  $800^{PLUS}$ . When you select this command, the following message displays: \*\* WARNING \*\* This will reboot the entire system! Press y

to reboot the system, or  $\mathbf{n}$  to exit the command.

» Factory Default **System** 

Write security: 0; Read security: 0

Resets the entire system to the factory default settings. To reset the system,

press y; to cancel this command, press n.

# Chapter 7 Modules Terminal Menu

To help you follow the terminal menu hierarchy, the following notations are used.

- > MENUS
- » Submenus
- »» Sub-submenus

## > MODULES

### Write security:3; Read security:5

The **Modules** menu provides options that allow you to configure and control the installed option modules as well as the controller T1/PRI ports. Figure 7-1 shows the **Modules** menu.

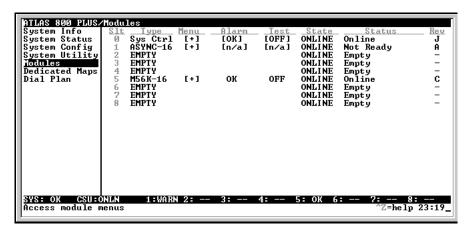


Figure 7-1. Modules Menu

The controller board (slot 0) has two T1/PRI interface ports. This section only describes the module options available for the T1/PRI interface ports. Individual module choices are described in the applicable module manuals. The ATLAS system controller automatically detects the presence of modules when they are installed in the system. To view the menus for the installed modules via the terminal menu, use the **arrow keys** to scroll to the appropriate menu and press **Enter.** You can then access the module choices.

### » SIt

### Write security:3; Read security:5

Identifies the slot number. Slot 0 refers to the ATLAS 800<sup>PLUS</sup> Base Unit.

### » Type

### Write security:3; Read security:5

Displays the type of module actually installed in the slot or the type of module you plan to install in the slot. The ATLAS 800<sup>PLUS</sup> automatically detects the type of module installed in each slot, and the **Type** field automatically defaults to the installed module type. You can also use this field to pre-configure a unit before actually installing modules by specifying the module that you want to install in each slot.

To use this option, navigate to the field you want to edit and press **Enter**. For empty slots, a list of all the available module types displays. Select the one you want and it displays in the **Type** field. If this field is already configured with a module, you can only set this field to **Empty**.



If you install a module in a slot, then want to install a different type of module in the slot, you must set this field to **Empty** before selecting another module type.



If a module is installed, the module type automatically shows the name of the installed module, and it cannot be set to any other option.

### » Menu

Displays additional status and configuration menus for the selected module. To access the submenus for this item, use the **Arrow Keys** to scroll to the **Menu** column for the module you want to edit, and press **Enter**. For detailed information on each submenu item, see *Modules (Quad T1/PRI) Menu* on page 7-3.

### » Alarm

### Read security:5

Displays whether there is an alarm condition on the ATLAS 800<sup>PLUS</sup> Base Unit. Press **Enter** to access the **Alarm** menu.

### » Test

### Read security:5

Displays whether the ATLAS 800<sup>PLUS</sup> is executing a test. To initiate a test, choose the **Menu** submenu on this screen. Then, select the **Test** option to access the screen that allows you to set up and initiate tests. See *Test* on page 7-2 for details. Press **Enter** to access the **Test** menu.

### » State

### **Read security:5**

Displays whether the module is online of offline. Even though a module is physically installed, it must be marked **Online** for it to be considered an available resource. This parameter allows an installed module to be marked **Offline**, which may be useful in system troubleshooting. If you choose **Offline**, the module will not be in alarm condition, but will display **Offline**.



Once a module is installed, you must change the state to Online in order for the ATLAS to utilize the module for any data bandwidth.

### » Status Read security:5

Displays status information on the ATLAS 800 PLUS T1/PRI ports and other installed modules as follows:

**Online** The module is enabled and is responding to the system

controller's status polls. This is the normal response of the

system.

**No Response** The module is enabled but is not responding to the sys-

tem controller's status polls. This response indicates a problem in the system or that the module is not installed.

**Empty** The system controller has not detected the presence of a

module in the system, nor has a module been manually

enabled for this option slot.

Offline The modules is installed but has been taken Offline by a

user. The module is still responding to controller polls.

**Offline/No** The module is installed but has been taken Offline by a

**Response:** user. The module is not responding to polls.

**Not Supported** The module is not supported by the current system con-

figuration.

### » Rev Read security:5

Displays the hardware revision of the ATLAS 800<sup>PLUS</sup>.

# Modules (Quad T1/PRI) Menu

This section provides detailed information on the **Modules/Menu** submenus. **Menu** provides access to commands that allow you to review the status of various options, change the configuration for general parameters, and initiate tests. This section *only* describes the menu options for the Quad T1/PRI controller port (the ATLAS 800 PLUS Base Unit). For details on menu options for individual modules, refer to the appropriate module manuals.

### »» Controller Info Read security:5

Displays general information about the ATLAS 800 PLUS Base Unit and Quad T1/PRI ports as follows:

Part Num Displays the part number of the ATLAS 800 PLUS.

**PLL Status** Indicates whether the clock is locked to its specific

(Phase Lock Loop) source.

### »» Alarm Status Read security:5

Displays any active alarms as follows:

**Prt** Port number displayed.

Loss of Signal

(LOS)

No signal detected on port interface.

**Red Alarm** Not able to frame data received on the port. Alternate-

(**RED**) ly referred to as Out of Frame (OOF).

Yellow Alarm (YELLOW)

Remote alarm indicator (RAI) being received on port.

Blue Alarm Receiving unframed all ones from the port alarm indi-

**(BLUE)** cator signal (AIS).

**D Channel Sync** (D-Chan) HDLC framing is operational on PRI D channel. This indication only applies when operating in PRI mode.

**Receive Level** Indicates the strength of the signal received on the port. (Rx Level)

### »» DS0 Status

### Read security:5

Indicates usage on a DS0 basis for each port as follows.

- \* Inactive
- A Active call on this DS0
- **D** Active D channel DS0
- **M** Maintenance DS0
- N Dedicated DS0
- Off hook detected
- R Ringing detected

### »» DS0 Alarms

### Read security: 5

Indicates alarms on a DS0 basis as follows:

- No alarm DS0
- **D** D channel alarm (ISDN)
- **F** Frame alarm (PACKET)
- TBOP alarm (PACKET)

### »» Sig Status

### **Read security:5**

Indicates signaling of all 24 DS0s. The A/B bits for Re and Tx DS0s are shown for each port.

### »» Performance: Current

### Write security:4; Read security:5

The performance fields – either current, 15 minute total, or 24 hour total – provide status on key performance measures as specified in ANSI T1.403 and AT&T TR54016 for each of the four T1/PRI ports as follows:

Prt Displays the port number.

**CLR** Clears information for the selected port. Press **Enter** when the cursor is over this field to clear the data.

ES Errored Seconds. An ES is a second with one or more error events or one or more Out Of Frame events or one or more Controlled Slips.

**BES** Bursty Errored Seconds. A BES is a second with more than one, but less than 320 error events.

**SES** Severely Errored Seconds. An SES is a second with 320 or more error events or one or more Out Of Frame events.

**SEFS** Severely Errored Frame Seconds.

**LOFC** Loss of Frame Count.

**CSS** Controlled Slip Seconds.

**UAS** Unavailable Seconds.

**LCV** Line Code Violations.

**RCV** Path Code.

**LES** Line Errored Seconds.

### »» Performance: 15 Min

### Write security:3; Read security:5

In the Performance 15 min. menu, the Performance data for the previous 15 minute window is stored. Refer to Performance: Current on page 7-5 for a detailed description.

### »» Performance: 24 Hr. Write security:3; Read security:5

In the Performance 24 hr. menu, the performance data for the previous 24 hour window is stored. Refer to Performance: Current on page 7-5 for a detailed description.

### »» Configuration

All of these configurable parameters depend on whether the port is connected to a Primary Rate ISDN circuit or a Channelized T1 circuit—dedicated or switched.

Read security:5 Prt

Identifies the port number.

**Port** Write security:3; Read security:5

Accepts any alphanumeric name up to 16 characters long to Name

uniquely identify each port.

**Frame** Write security:2; Read security:5

Matches the frame format of the circuit to which it is con-

nected (available from the network supplier).

Code Write security:2; Read security:5

Matches the line code of the circuit to which it is connected

(available from the network supplier).

Tx Yellow Write security:3; Read security:5

(Auto Tx Yellow Alarm) Enables and disables the transmit-

ting of yellow alarms.

Tx PRMs Write security:3; Read security:5

(Transmit PRMs) Enables and disables the sending of PRM data on the facility data link (FDL). The PRM data continues to be collected even if XMIT PRM is disabled (possible only

with ESF format).

LBO Write security:2; Read security:5

(Line Build Out) Depends on whether the circuit is provi-

sioned for DS1 by the telephone company.

LB Write security:3; Read security:5

**Accept** (Loopback Accept) Sets unit to accept or reject the in-band

loop up and loop down codes as defined in ANSI T1.403. This

is a line loopback.

Pulse Write security:3; Read security:5

**Density** Enables or disables the Pulse Density Enforcer for this T1 cir-

Enforcer cuit.

**"" Test** Initiates different types of tests and displays test results.



These **Test** commands temporarily disrupt service.

**Prt** Identifies the port number.

Loc LB Read security:5

(Local Loopback) Causes loopback on near-end port

Line Metallic loopback

Payld Payload loopback framing and clocking are

regenerated.

Remote LB Write security:4; Read security:5

(Remote Loopback) Sends a loopback code to a remote

CSU.

**ANSI FDL Line** (Requires ESF mode)

**ANSI FDL Pyld** (Requires ESF mode)

AT1 Inband line

Pattern Write security:4; Read security:5

Specifies the test pattern to be transmitted out the port.

All ones framed ones

All zeros framed zeros

QRSS 2 20-1 pseudorandom pattern with

suppression of excess zeros

QRSS/RLB Read security:5

Results (Test Pattern Results) Suppresses excess zeros—indica-

tion of sync and errors of received data pattern.

Clr Write security:4; Read security:5

(Test Pattern Results Clear) Clears current error counters

on test pattern results menu.

Inj Write security:3; Read security:5

(Test pattern Error Inject) Injects errors into transmitted

test pattern.

# **Dedicated Maps Terminal** Chapter 8 Menu

### **OVERVIEW**

The **Dedicated Maps** menu assigns dedicated connections between any two ports in the ATLAS 800<sup>PLUS</sup> Base Unit. This chapter describes the **Dedicated** Maps menu items (see Figure 8-1). In addition, step-by-step instructions are provided for setting up a sample dedicated map (see Creating A Dedicated Map on page 8-6).

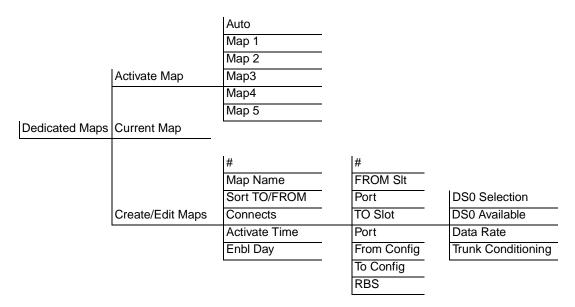


Figure 8-1. Dedicated Maps Menu Tree

To help you follow the terminal menu hierarchy, the following notations are used.

- > MENUS
- » Submenus
- »» Sub-submenus

# > ACTIVATE

## Write security:3; Read security:5

Activates a dedicated map—automatically or manually. You can have up to five different dedicated maps, each with an optionally specified name.

» Auto

Automatically activates a particular dedicated map at the time and day specified in **Activate Time** (see *Activate Time* on page 8-5).

### » Maps 1—5

Lets you manually activate a specific dedicated map.

	Instructions for Manually Activating a Dedicated Map	
Step Action		
1	Move the arrow keys to highlight the <b>Activate Map</b> field and press <b>Enter</b> .	
2	Move the arrow key to highlight the map of choice from the popup menu list and press <b>Enter</b> .	

### > CURRENT MAP

### Read security:5

Displays the name of the currently active dedicated map (read only).

## > CREATE / EDIT MAPS

Creates new maps and defines settings, as well as edits existing maps. To add a new map, position the cursor in the index column and press I. ATLAS automatically names the maps in the sequence in which they are created. You can change the names with **Map Name**.

» #

Index number of the available maps.

### » Map Name

### Write security:3; Read security:5

Displays the name of the dedicated map. The name can contain up to 57 alphanumeric characters, including spaces and special characters. To edit the name, press **Enter** and type in the new name.

### » Sort TO/FROM

### Write security:3; Read security:5

Specifies sort order based on the end points set in **Connects/From Config** and **Connects/To Config**. You can also turn **Off** this option. This sort feature is helpful when you are attempting to find a particular connection in a large connection list.

### » Connects

Enters the dedicated map connections. Press **Enter** to activate the submenus.



Some of the options available in this submenu change depending on the type of modules selected in the FROM or TO fields.

»»#

(Index Number) Displays the number of the dedicated map connection. If you press I in this field, ATLAS 800<sup>PLUS</sup> adds another dedicated map connection, numbered consecutively.

### »» FROM SIt

### Write security:3; Read security:5

(From Slot) Specifies the slot to use for the **FROM** connection. When you select this option, a list of all of the slots and the modules installed in the slots displays. Pick the appropriate slot and press **Enter**.

#### »» Port

### Write security:3; Read security:5

Specifies the port to use for the **FROM** connection. When you select this option, a list of ports and module types appears. Pick the appropriate port and module type, and press **Enter**.

#### »» TO Slot

### Security level: 3; Read security: 5

Specifies the slot to use for the second end of a connection. Select this option, and a list of all of the slots and the modules installed in the slots displays. Pick the appropriate slot.

### »» Port

### Security level: 3; Read security: 5

Selects the port used for the second connection. When you select this option, a list of all the slots and available modules displays. Select the appropriate slot.

### »» From Config

### Write security:3; Read security:5

Specifies the configuration for the **FROM** connection. The selections displayed in this field are based on the type of module selected in the **FROM SIt** option. You must input the following information—based on the module type.

# DS0

### Write security:3; Read security:5

### Selection

Defines DS0s for a T1 port. Use this field to define which DS0s will be used for this connection. You can enter the DS0s in several ways. For example, to enter DS0s one through five, enter 1-5. For DS0s one and five, enter 1,5.

### DS0 Available

### Read security:5

Indicates which DS0s of the T1 are assigned. DS0 assignment is based on the following items:

- digits 0—9 This DS0 is available. The digit that displays in this field represents the last digit of the DS0 number.
  - \* This port is requesting this DS0 for this connection, but the DS0 is not yet activated.
  - ! This DS0 is used by this port in this connection and is activated.
  - **s** This DS0 is used in the switched Dial Plan.
  - S This DS0 is used in the switched Dial Plan and conflicts with this connection.

- n This DS0 is already used in this Dedicated Map.
- N This DS0 is already used in this Dedicated Map and conflicts with this connection.

### Data Rate Write security:3; Read security:5

Defines the data rate per DS0. If **FROM SIt** is an Nx port, the data rate per DS0 must be set. You can choose from 64 kbps or 56 kbps.

# Trunk Conditioning

### Security level: 3; Read security: 5

Sets known values in the signaling bits and the data field for outgoing DS0s which are cross-connected to a T1 port experiencing alarms.

The trunk conditioning process consists of a 2.5-second transmission (indicating call termination), followed by a continuous transmission signaling the final condition as chosen by the user.

NOTE

Trunk conditioning only applies to RBS T1s in the

dedicated map.

Fault Signaling Defines to ATLAS the type of signaling being

used on the trunk:

E&M

LS/GS Network or User

SW56 Custom

NOTE

Fault signaling is only visible when RBS is turned

on.

**Fault State** Defines the final fault signaling state:

**Idle** - used for one-way trunks; that is, for outgoing *or* incoming calls only—not both.

**Seized** - used for two-way trunks. Prevents the PBX from attempting to use a failed trunk for an outgoing call.

Custom

Permits users to define the Fault Signaling to

use in the form of A/B set to 1/0.



See also the trunk conditioning example on page 8-5.

### »» To Config

### Security level: 3; Read security: 5

Specifies the configuration for the **To** connection. The selections that display in this field are based on the type of module selected in the **TO Slot** option. You must input the following information (based on the type). The same options for setting DS0s are available for this command as with the **FROM Config** option.

### »» RBS

### Security level: 3; Read security: 5

(Robbed Bit Signaling) Defines whether the connection has active RBS. Where RBS is not an option, ATLAS  $800^{PLUS}$  automatically assigns the correct setting. For example, a T1-to-Nx connection is set to **Off**.

**On** Preserves the signaling bits between the connections.

Off Ignores signaling bits.

### » Activate Time

### Security level: 3; Read security: 5

Sets the time when the map becomes active if you have selected **Auto** in the **Activate Map** field (see *Activate Map* on page 8-2). Enter this time in hh:mm:ss 24-hour format.

### » Enbl Day

### Security level: 3; Read security: 5

Specifies which days of the week the map is active.

# **Example 1** Setting Trunk Conditioning

The trunk conditioning process sets known values in the signaling bits and the data bits for outgoing DS0s which are cross connected to a T1 port experiencing alarms. The trunk conditioning process consists of a 2.5-second transmission, indicating call termination, followed by a continuous transmission signaling the final condition as chosen by the User.

Use the trunk conditioning menu items **Fault Signaling** (to set the state of the signaling bits) and **Fault Data Code** (to set the state of the data bits) for this process. You can set trunk conditioning for each end of each T1-to-T1 connection in a dedicated map. To simplify this procedure, use the copy command (press **C**). Connections to the Network and connections to User equipment (PBX) contain different signaling bit states.

For this example, assume voice traffic is received on T1-A, and T1-B is groomed onto T1-C to the PBX (see Figure 8-2). If T1-A fails, the DS0s which were cross-connected to T1-C will receive trunk conditioning.

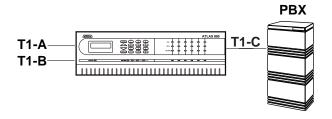


Figure 8-2. Trunk Conditioning

**Example:** Creating A Dedicated Map

A Dedicated Map defines connections for dedicated bandwidth between ports, and grooms and cross-connects bandwidth between T1 ports. Any ATLAS port supporting dedicated bandwidth can be mapped to any other port supporting dedicated bandwidth (see the example in Figure 8-3).

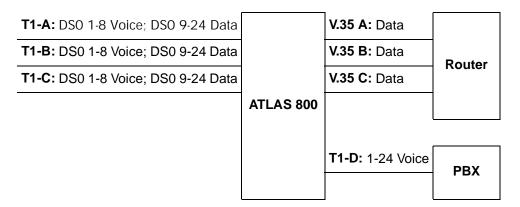


Figure 8-3. Dedicated Map Overview Example

61200226L1-1

The example shown in Figure 8-3 contains three T1s (T1-A, T1-B, T1-C) supporting dedicated bandwidth from three remote sites. Each T1 includes DS0s for data and voice. At the central site (ATLAS), each incoming DS0 carrying data is mapped to a separate V.35 port and connected to the router. DS0s carrying voice are collected together (groomed) and sent to the PBX over a single T1 (T1-D).

# Designing a Dedicated map

8-6

In designing a Dedicated Map, you must first determine what connections to make and which ports to involve. (For T1 ports, you must also decide which DS0s to use). Then, you must configure the ports. Finally, you must define the appropriate connections. The remainder of this chapter provides

step-by-step procedures for creating a sample Dedicated Map based on the connections and ports given in Table 8-1.

**Table 8-1. Connections and Ports** 

Name	ATLAS 800 <sup>PLUS</sup> Port	DS0s	Name	ATLAS 800 <sup>PLUS</sup> Port	DS0s
T1: Data A	Controller T1 Slot 0 Port 1	9-24 RBS Off	V.35 - A	Quad V.35 Slot 2/Port 1	N/A
T1: Data B	Controller T1 Slot 0/Port 2	9-24 RBS Off	V.35 - B	Quad V.35 Slot 2/Port 2	N/A
T1: Data C	Quad T1/PRI Slot 1/Port 1	9-24 RBS Off	V.35 - C	Quad V.35 Slot 2/Port 3	N/A
T1: Voice A	Controller T1 Slot 0/Port 1	1-8 RBS On	T1-D	Quad T1/PRI DSX Slot 1/Port 2	1-8 RBS On
T1: Voice B	Controller T1 Slot 0/Port 2	1-8 RBS On	T1-D	Quad T1/PRI DSX Slot 1/Port 2	9-16 RBS On
T1: Voice C	Quad T1/PRI Slot 1/Port 1	1-8 RBS On	T1-D	Quad/PRI DSX Slot 1/Port 2	17-24 RBS On

# **Configuring the Ports**

Begin by navigating to **Terminal Menu/Modules**. From this menu, configure the various ports to match the framing parameters of the T1 line provided by the telco.

	Instructions for Configuring the Ports	
Step	Action	
1	Select Slt / 0 (system controller T1/PRI port).	
2	Set the line framing parameters by selecting Menu / Configuration / Frame / ESF.	
3	Copy this configuration information for use with additional ports. (Navigate to <b>Prt</b> and press <b>C</b> .)	
4	Navigate to the port index number of the second port ( <b>Prt</b> ) and press <b>P</b> to paste the configuration information. Press <b>Y</b> to confirm paste.	
5	Repeat Step 4 for the first port of the T1/PRI card located in Slot 1.	
6	Navigate to the V.35 port <b>Configuration</b> submenu and repeat Step 2 for the first port, followed by a copy-and-paste to the second and third ports (see Figure 8-4).	

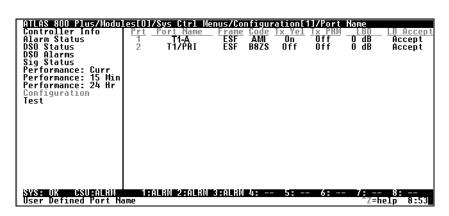


Figure 8-4. Slot 0 Module Configuration Menu

# **Defining the Connections**

Begin by navigating to **Dedicated Maps / Create/Edit Maps** and naming your map.

Navigate to **Dedicated Maps / Connects**. The **Connects** submenu defines the connections necessary to route the required bandwidth. Refer to Table 8-1 to define each of the necessary connections. For this procedure, first define the data connections, and then define the voice connections. The following Step/Action tables guide you through this process. (Figure 8-5 shows the completed map.)

	Instructions for Defining Data Connections	
Step	Action	
1	For Data A, select and define FROM Slot (i.e., 0 Sys Ctrl).	
2	Select and define "from" <b>Port</b> (i.e., port <b>1</b> for T1: Data A).	
3	Select and define From Config DS0s (i.e., DS0=9-24).	
4	Select and define <b>TO Slot</b> and "to" <b>Port</b> in the same way (i.e., <b>2 V.35Nx4</b> and <b>1</b> where 2 = Slot 2 and 1 = Port 1.)	
5	From <b>To Config</b> , set <b>V.35</b> to operate at <b>56k/64k</b> per DS0.	
6	Repeat for the remaining data connections (i.e., Data B and Data C) as follows:	
6a	Insert new connection lines by positioning the cursor over the index # of the first connection and pressing I.	
6b	Copy the first connection by positioning the cursor on the index # and pressing <b>C</b> .	

	Instructions for Defining Data Connections (Continued)	
Step	Action	
6c	Paste this information onto a new connection line by positioning the cursor over the index numbers of the new connections, and pressing <b>P</b> .	
7	Modify these connection lines to complete the connections for data.	

	Instructions for Defining Voice Connections	
Step	Action	
1	Select the <b>FROM Slot</b> and <b>Port</b> for the first voice connection (i.e., Slot 0/Port 1 for T1-A Voice).	
2	Select the voice DS0s; i.e., 1 through 8 for Voice A.	
3	Select the <b>TO Slot</b> and <b>Port</b> (PBX Connection); i.e., Quad T1/PRI in Slot 1/Port 2.	
4	From <b>Configuration</b> , set the starting DS0 that these voice DS0s will appear in; i.e., 1 for Voice A; 9 for Voice B; 17 for Voice C. (This action sets the DACSing between the T1s.)	
5	Set RBS to On for the voice connections.	
6	(Optional) From <b>Configuration</b> , set the trunk conditioning (Signaling and Data code) for T1 failure.	
7	Repeat for the remaining voice connections.	



A connection is not actually "made" (connected) until the cursor leaves the connection. The cursor leaves the connection when you press ESC to move the cursor to the index # or when you move the cursor onto another connection line.

61200226L1-1 ATLAS 800<sup>PLUS</sup> User Manual 8-9

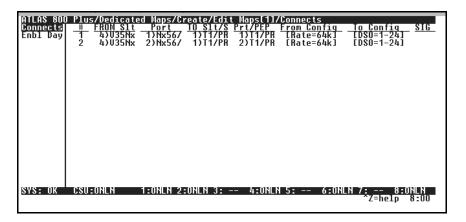


Figure 8-5. Completed Dedicated Map

### **OVERVIEW**

This chapter describes the configuration of dedicated circuits for backup and discusses the **Circuit Status** menu.

## **Dedicated Circuit Dial Backup Setup**

In Figure 9-1, the host ATLAS  $800^{PLUS}$  has a fractional T1 of 16 DS0s going to the T1 cloud, which is then DACSed out to two different remote sites, 8 DS0s each.

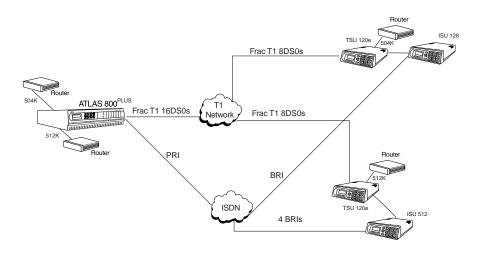


Figure 9-1. Dedicated Circuits Backup Configuration

Dedicated circuit backup allows the user to configure the ATLAS to dial up a backup link when the dedicated link goes into alarm. Additionally, the ATLAS Nx 56/64 V.35 and USSI modules can rob an inband 8kbps channel over which messages can be transferred. When the ATLAS loses communication with the remote site, backup will be initiated. This feature is compatible with the Inband Mode of the ADTRAN TSU series of products.

Currently, dedicated circuit backup is supported only for Nx interfaces (V.35 or USSI) nailed to T1s.

### Configuration

9-2

First, configure your dedicated maps normally. Refer to Chapter 8 for more information on configuring Dedicated Maps. One thing to remember is that the endpoint receiving the backup data (i.e., the Nx endpoint) needs to be in the **From** column.

All dedicated circuit dial backup configuration is the **Dial Plan/User Term** menu. For **Slot/Svc**, select **Circuit Backup**. When you select **Port/PEP**, you should get a list of all endpoints that are available for backup configuration. For information on configuring In#Accept and Out#Reject lists, see Chapter 10.

Under **Dial Plan/User Term/Interface Config** (see Figure 9-2), several options are applicable only for Originating endpoints, and will not display for Answer endpoints.

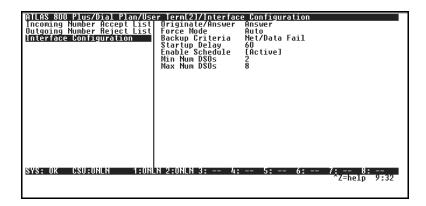


Figure 9-2. Interface Config Menu

To help you follow the terminal menu hierarchy, the following notations are used.

- > MENUS
- » Submenus
- »» Sub-submenus

### > INTERFACE CONFIGURATION

» **Originate/Answer** The following selections are available for the **Originate/Answer** menu item.

**Originate** The endpoint will originate the backup call.

**Answer** The endpoint will answer any incoming calls, but will

only go into backup if an error is detected.

**Answer Any** The endpoint will answer any incoming calls and go

immediately into backup.

» Outgoing Call Type This only applies to originating endpoints.

**Source ID** This only applies to originating endpoints. The **Source ID** field is used to simplify the creation of a Dial Plan in applications where the criterion for

switching calls to a certain endpoint is a function of which endpoint origi-

nated the call.

• Default value = 0. The default ID for all endpoints is 0 and all accept #s is 0. With default values, all calls are routed based only on dialed num-

ber.

Multiple endpoints can have the same Source ID.

• When creating the **Call Accept** list, specify source ID(s) as well as a di-

aled number or range of dialed numbers to accept.

**» Outdial Number** This only applies to originating endpoints. This is the number dialed when

the endpoint goes into backup.

**» Force Mode**This forces the backup state of this endpoint. This is a configuration setting,

so it will retain its value until it is changed. To temporarily force an endpoint

into backup, or to force a restore, try the Manual activator.

**» Backup Criteria** Criteria for automatic backup. Note that this setting affects the available op-

tions for Restore Criteria.

» **Restore Criteria** This only applies to originating endpoints. These are criteria for automati-

cally coming out of backup. Note that **Network Success** is only available

when a backup criterion is not Net/Data Fail.

**Net Success** When network is out of alarm

**Manual Only** Only by the Manual activator

**Startup Delay** The amount of time to wait after creating or changing the endpoint before

allowing backup.

» Backup Delay This only applies to originating endpoints. The amount of time to delay after

detecting an alarm before going into backup. If the circuit comes out of alarm

before this time has expired, the endpoint will not go into backup.

» **Restore Delay** This only applies to originating endpoints. The amount of time to delay after

clearing an alarm before coming out of backup. If the circuit goes into alarm

before this time has expired, the endpoint will remain in backup.

» Max Num Redials This only applies to originating endpoints. The backup endpoint will at-

tempt this many retries before giving up and declaring a backup failure.

» **Redial Timer** This only applies to originating endpoints. The amount of time delayed be-

tween a failed backup call and the redial.

» **Enable Schedule** Use this menu to schedule the times when backup is enabled. The following

selections are available for the **Enable Schedule** menu item.

**Enable Time** This is the time of day to enable dial backup.

**Disable Time** This is the time of day to disable dial backup. If the dis-

able time is earlier than the enable time, backup moni-

toring will be active across midnight.

Days Enabled Use this record to enable/disable backup monitoring

on particular days of the week.

» **Test Call** This only applies to originating endpoints. Use this menu to schedule regu-

larly occuring test calls. The following selections are available for the Test

Call menu item.

**Period** How often test calls are to be made.

**Next Test Time** The date of the next scheduled test call.

**» Min Num DS0s** This option will specify the number of DS0s to use for this switched call. If

this number is 1, all calls will be directly to the endpoint, and not use a BONDING resource. Any number other than 1 will use BONDING resourc-

es to inverse multiplex the multiple switched channels together.

**» Max Num DS0s** This option will specify the number of DS0s to use for this switched call. If

this number is 1, all calls will be directly to the endpoint, and not use a BONDING resource. Any number other than 1 will use BONDING resourc-

es to inverse multiplex the multiple switched channels together.

# **CIRCUIT STATUS MENU**

The Circuit Status menu allows the user to view at a glance the status of any circuits that are configured for dedicated circuit backup. Figure 9-3 shows the Circuit Status menu.

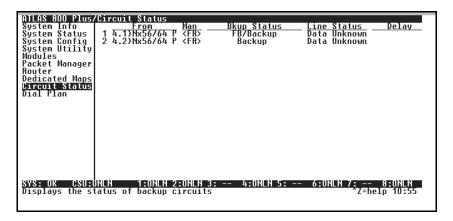


Figure 9-3. Circuit Status Menu

#### > FROM Write security:3; Read security:5

Indicates the slot, port, and name of the endpoint that is configured for backup.

# > MAN (MANUAL **BACKUP)**

Use this activator to force a link into/out of backup.

FB Force Backup FR Force Restoral

# > BKUPSTATUS (BACKUP STATUS)

String indicates the current status of the dedicated line. The following selections are available for the **Backup Status** menu item.

FΒ Backup is forced through the interface menu.

FR Restoral is forced through the interface menu.

**Primary** The link is active.

**Dialing** Attempting to dial the backup link.

**Backup Failed** Exceeded Max Num Redials.

**Retry Dial** 

Will retry backup dial in [num] seconds. [num]

**Primary Down** The link is in error and waiting on backup.

Answering The link is answering a backup endpoint.

**Backup** The link is in backup.

# > LINE STATUS

This gives you the overall status of the connection. The following selections are available for the Line Status menu item.

Unknown Endpoints do not support (or are not configured) for moni-

toring.

Active The connection is up and running.

Inactive The connection is down due to configuration (i.e., the DTR

is down).

**Data Alarm** The FROM endpoint is in data alarm.

Network

**Alarm** 

The TO endpoint is in network alarm.

Net/Data

Both the FROM endpoint and the TO endpoint are in alarm.

Alarm

The status of the FROM endpoint is unknown.

Data Unknown

# > DELAY

When present, this indicates that one ATLAS has detected a change in state and is counting down to delay/restoral.

> **TEST** This only displays if an endpoint is configured for Originate. This submenu

is used to monitor regular test call status for the backup endpoint. The record label displays the number of successful tests and the number of test

failures, respectively.

» **Last Run Time** Only displays if a test call has been attempted. This displays the date of the

last attempted test call.

**» Next Run Time** Only displays if a test call is scheduled. This displays the date of the next

test call attempt.

**» Last Test Status** Displays the status of the most recent test call.

Idle No test call has been attempted.

**Running** A test call is currently running.

**Failed** The most recent test call failed.

**Passed** The most recent test call passed.

» Pass: Fail Displays the number of successful tests and the number of test failures, re-

spectively.

**» Test Now** Use this activator to manually initiate a test call.

# Chapter 10 Dial Plan Terminal Menu

# **OVERVIEW**

The **Dial Plan** submenus (see Figure 10-1) set global ATLAS switch parameters as well as individual parameters for each ATLAS port handling a switched call. The individual ports are separated into two port types: network and user. Network ports terminate a connection from the Network. User ports terminate incoming calls and, in turn may be connected to user equipment. *Network Term* on page 10-3 and *User Term* on page 10-5 provide clarification for these two port types. (See also Figure 10-2 for the complete menu structure.)

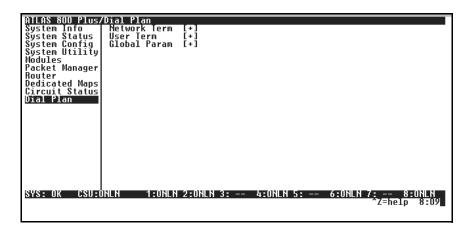


Figure 10-1. Dial Plan Menu



In the menus described in the following sections, Incoming Calls refer to calls coming to ATLAS from the Network (PSTN) and Outgoing Calls refer to calls directed toward the Network (PSTN).

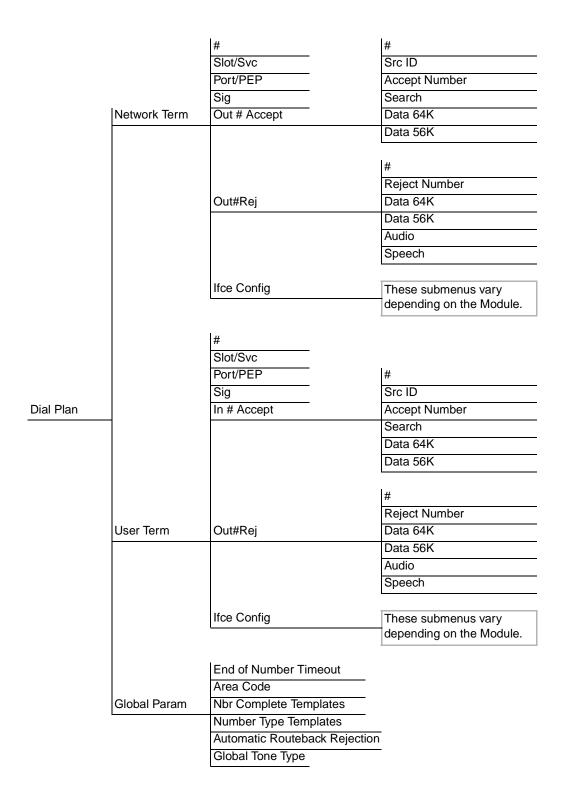


Figure 10-2. Dial Plan Menu Tree

# > NETWORK TERM

This menu allows the user to define option parameters for ports which terminate a connection from the Network (PSTN).



In applications where two ATLAS units are used in a point-topoint configuration, a port in the ATLAS at one end would act as the Network (User Termination), while the ATLAS at the opposite end would be terminating a "Network" connection.

» Slot/Svc

Write security: 3; Read security: 5

Select the ATLAS slot that terminates a Network connection.

» Port/PEP

Write security: 3; Read security: 5

Select the ATLAS port that terminates a Network connection.



There may be more than one "end point" associated with a particular port. If a T1 is connected to the PSTN, some DS0s may be used for long distance, while others are used for local calls. These would constitute two "end points" (trunks) over a single physical port.

» Siq

# Write security: 3; Read security: 5

Defines the type of signaling being used for this connection (end point). RBS would be for a T1 using Robbed Bit Signaling while PRI designates a Primary Rate ISDN interface. This selection is only necessary if a T1/PRI is selected as the Slot/Port type.

» Out#Accept

# Write security: 3; Read security: 5

Defines the parameters for the outgoing calls that ATLAS sends to the Network.

»» Src ID

# Write Security: 3 Read Security: 5

Identifies the call source ID from which this endpoint accepts calls This field simplifies the creation of a Dial Plan in applications where the criterion for switching calls to a certain endpoint is a function of which endpoint originated the call. Source ID may be entered with the usual wild card entries (except \$)

X = any digit 0-9

[1,3,5] = any of these digits

Default value = 0. The default ID for all Source endpoint is 0 and all accept #'s is 0. This results in all calls being routed based on the dialed number.

# »» Accept Numbers

This field designates which numbers this end point will pass on toward the Network (PSTN). The accept list may consist of multiple entries. The numbers are defined using "wild cards":

X = Any single digit

N = Any single digit 2-9

\$ = Any number of digits of any value

**9** = This specific number

[1,2,3...] = A single digit in this group

Example: 1-800-\$ would only permit toll free long distance calls to 1-800. If this were used, then a second accept # would need to be specified - NXX-XXXX. This would permit local numbers to be dialed.



Any specific entry will take precedence over a wild card. For example, if end point "A" was designated as \$ while end point "B" accepted 963-800X, then an incoming call to 963-800X would only be accepted by end point "B".

# »» Search

# Write Security: 3 Read Security: 5

The Search parameter instructs ATLAS which order to search for an accept number match. Normally all searches are set to Primary. The Secondary search selection would be used to force ATLAS to only accept a call at this end point if all Primary end points were unavailable.

# Primary Search

All long distance calls should go out a PRI directly to an IXC (MCI, ATT, etc.) and local calls should go out a T1 to the LEC. It may be desirable to place long distance calls on the local exchange if all of the IXC trunks are unavailable (busy or in alarm). In this case, the primary accept number for the local exchange would be N\$, and the secondary accept would be 1\$.

# Secondary Search

The same accept rules apply for all secondary number searches as for primary searches.

# »» Data 64K, Data 56K

These options reflect the bearer capability the Network has provisioned for this line. If the ISDN lines were purchased with different services provisioned, then ATLAS would send the call out of the port which supports the type of service the call requires.

For example, the Network Termination is on a pair of BRIs (with the same phone number) with one provisioned for data and the other for voice. By enabling data in one and not the other, ATLAS ensures that calls bearing data will be sent out the right BRI interface.

## » Out#Rej

# Write security: 3; Read security: 5

This submenu defines the parameters for the outgoing calls that ATLAS will not send to the Network.

# »» Reject Number

This field identifies which numbers this end point will not pass on toward the Network (PSTN). The reject list may consist of multiple entries. The reject list may be used to more easily specify the call filtering desired. The "wild cards" are identical as in Outgoing Call Accept.



The Reject list takes precedence over the Accept list.

For example, 1- 900-\$ would reject all 1-900 long distance calls, and 1-\$ would reject all long distance calls.

# »» Data 64K, Data 56K, Audio, and Speech

These items allow ATLAS to reject outgoing calls based on call type. For example, a "\$" for the Reject Number and Digital 56/64 enabled and Audio & Speech Disabled would reject all digital calls while not rejecting analog calls.



This list may remain blank if the Accept list meets desired filtering.

# » Ifce Config

Sets configuration parameters for the end point. These parameters vary by the type of port selected. For detailed information on the interface configuration, refer to *Quad T1/PRI Module Interface Configuration* on page 10-9.

# **JUSER TERM**

This menu allows you to define option parameters for ports which terminate a connection from user equipment. In this case, ATLAS  $800^{PLUS}$  is acting like the Network.



In applications where two ATLAS units are used in a point-topoint configuration, a port in the ATLAS at one end would act as the Network (set up as a User Termination), while the ATLAS at the opposite end would be terminating a Network connection.

### » Slot/Svc, Port/PEP

# Write security: 3; Read security: 5

Selects the ATLAS port that terminates a User connection. (The user selects from a list of option modules/ports.)



There may be more than one "end point" associated with a particular port. If a T1 port is connected to a channel bank with analog voice cards, each DS0 or a group of DS0s may have a different phone number. These would constitute multiple "end points" over a single physical port.

10-5

# » Sig Write security: 3; Read security: 5

(User Selection - RBS; PRI) Defines the type of signaling being used for this connection (end point). RBS would be for a T1 using Robbed Bit Signaling while PRI designates a Primary Rate ISDN interface. This selection is only necessary if a T1/PRI is selected as the Slot/Port type.

# » In#Accept

# Write security: 3; Read security: 5

This submenu defines the parameters for incoming calls that ATLAS 800<sup>PLUS</sup> will accept from the Network.

#### »» Source ID

# Write Security: 3 Read Security: 5

This field identifies the ID of the call sources that this endpoint will accept calls from. The Source ID field is used to simplify the creation of a Dial Plan in applications where the criteria for switching calls to a certain endpoint is a function of which endpoint originated the call.

Source ID may be entered with the usual wild card entries (except \$)

X = any digit 0-9

[1,3,5] = any of these digits

Default value = 0. The default ID for all Source endpoint is 0 and all accept #'s is 0. This results in all calls being routed based on the dialed number.

# »» Accept Numbers

# Write security: 3; Read security: 5

This field designates which numbers this end point will accept (terminate) from the Network (PSTN). The accept list may consist of multiple entries. The numbers are defined using "wild cards":

X = Any single digit

N = Any single digit 2-9

\$ = Any number of digits of any value

**9** = This specific number

[1,2,3...] = A single digit in this group

For example, 963-8000 would be a specific incoming number that would be accepted by this end point. If this end point consisted of a T1 with multiple DS0s, a "hunt" group for 963-8000 would be formed. The entry \$ would accept any call.



Any specific entry will take precedence over a wild card. For example, if end point "A" was designated as \$ while end point "B" accepted 963-800X, then an incoming call to 963-800X would only be accepted by end point "B."

# »» Search

# Write Security: 3 Read Security: 5

Defines to ATLAS the order in which to search for an Accept Number.

# Primary Search

The Search parameter instructs ATLAS which order to search for an accept number match. Normally all searches are set to Primary. The Secondary search selection would be used to force ATLAS to only accept a call at this end point if all Primary end points were unavailable.

For example, all long distance calls should go out a PRI directly to an IXC (MCI, ATT, etc.) and local calls should go out a T1 to the LEC. It may be desirable to place long distance calls on the local exchange if all of the IXC trunks are unavailable (busy or in alarm). In this case, the primary accept number for the local exchange would be N\$, and the secondary accept would be 1\$.

# Secondary Search

The same accept rules apply for all secondary number searches as for primary searches.

#### »» Data 64K, Data 56K

# Write security: 3; Read security: 5

This reflects the bearer capability that the attached user equipment (typically a TA) has. If the attached TA can only handle digital calls, then a voice call sent to this end point would be rejected.

# » Out#Rej

# Write security: 3; Read security: 5

Defines the parameters for outgoing calls that ATLAS  $800^{PLUS}$  will not send to the Network.

# »» Reject Number

This field designates which numbers this particular end point will NOT pass on toward the Network (PSTN). This is used when the outgoing call filter is different for different users. The "wild cards" are identical as in Outgoing Call Accept. For example, if desired, each user termination port can be set to reject different numbers.



[0,1]-\$ would reject all long distance calls, but only for this user termination. If permitted in the Network Termination end point, this user could not dial long distance numbers while other users could.

# »» Data 56K, Data 64K, Audio, Speech

These items allow ATLAS  $800^{PLUS}$  to reject outgoing calls based on call type. For example, a "\$" for the Reject Number, Digital 56/64 enabled, and Audio & Speech Disabled would reject all digital calls while not rejecting analog calls.



This list may remain blank if the Accept List meets desired filtering. The Call Reject list takes precedence over the Call Accept list.

# » Ifce Config

Sets configuration parameters for the end point. These parameters vary by the type of port selected. For detailed information on the interface configuration, see *Quad T1/PRI Module Interface Configuration* on page 10-9.

# > GLOBAL PARAM

Set ATLAS options which apply to all switched operations, both incoming and outgoing calls.

# » End of Number Timeout

# Write security: 3; Read security: 5

This parameter sets the length of time ATLAS will wait before assuming the outgoing dialed number is complete. The default value is six seconds. This timeout will only be invoked if the dialed number does not match one of the patterns set in the Number Complete Template menu.

#### » Area Code

# Write security: 3; Read security: 5

The local area code. This is used for sending caller ID to the Network.

# » Nbr Complete Templates

# Write security: 1; Read security: 5

For any outgoing call, ATLAS must be able to recognize when the phone number is complete. For example, a local number will be seven digits long while a long distance (1+ #) will be 11 digits long. The ATLAS defaults will cover almost any installation, and these templates should not require any additional user input except for unusual circumstances. The template allows the use of "wildcard" inputs to define numbers:

**X** = Any single digit

N = Any single digit 2-9

**911** = This specific number

[1,2,3...] = A single digit in this group

# » Number Type Templates

# Denotes an Entry Number (MAX 50). Press **INS/DEL** to in-

sert/delete any entry.

**Pattern** Modifies an entry when you press **Enter** (MAX 40).

For example, 1+(NXX) NXX - XXXX would be a pattern for a normal long distance call. Note that the symbols (), +, - and space are not required and are only used to improve read-

ability.

# Write security: 1; Read security: 5

ISDN interfaces require that a number type be sent over the D channel when a call is sent or received. A normal RBS trunk does not send a type designator, but uses prefixes instead. For example, "1 +" prefix is national long distance call type while a "011 +" prefix would be an international long distance call type. These templates form a table to permit ATLAS to translate the RBS prefix into a call type for ISDN and vice- versa.



The ATLAS default templates should cover all applications and should not need to be added to by the user except for very rare circumstances.

# » AutomaticRoutebackRejection

# Denotes an Entry Number (MAX 50). Press **INS/DEL** to in-

sert/delete any entry.

**Prefix** Sets the prefix for the number type. Only digits 0 and 1 are

allowed (MAX 6).

Pattern Modifies an entry when you press **Enter** (MAX 40).

**Number Typ** Lists valid selections when you press **Enter**.

# Write security: 1; Read security: 5

When enabled, **Automatic Routeback Rejection** prevents calls which enter through network termination interfaces from being forwarded out another network interface. Such an event could happen if an incoming call specifies a number that has no endpoint configured to accept it and another network interface has a call acceptance entry which could accept it (such as \$). Without automatic rejection, such a call would be forwarded back to the Network. The Network would in turn resend the call to the unit until all incoming resources are consumed.



Use extreme caution when disabling this option!



For information on Circuit Backup Configuration, refer to Dedicated Circuit Backup and Circuit Status on page 9-1.

# QUAD T1/PRI MODULE INTERFACE CONFIGURATION

This section describes the **Network Termination** and **User Termination** configuration settings for the Quad T1/PRI module when using the **Dial Plan** menus.

# Quad T1/PRI Module (Network Termination/PRI)

When you are working in the Network Termination section of the Dial Plan menu, the Slot is defined as a T1/PRI module, and Sig is set to PRI, the following configuration options are available:

»» Switch Type Write security: 2; Read security: 5

Defines the type of PRI switch that ATLAS is connected to. If connected to another ATLAS, both need to be set to the same type. The available options include Lucent 5E, Northern DMS 100, National ISDN, and AT&T 4ESS.

10-9

**»» First DS0** Write Security: 3 Read Security: 5

Defines the first active DS0 for a fractional PRI.

#### »» Number of DS0s

# Write Security: 3 Read Security: 5

Defines the number of DS0s used for calls on this PRI. DS0 24 is assumed to be used by the PRI for the D channel.

# »» Outgoing Number Conversion

# Write Security: 3 Read Security: 5

This item defines the rules for converting as-dialed numbers into ISDN number type and plan.

As dialed Send digits provided as unknown number type.

ISDN - Convert to ISDN type, using the 10-digit national

**National pref** form if possible.

**ISDN -** Convert to ISDN type, using the 7-digit subscrib-

**Subscriber pref** er form if possible.

**ISDN - National DMS** Send digits provided as National Number Type,

**Reserved pref** DMS Reserved Numbering Plan.



When a 4ESS is configured, many installations will require the national form where possible; this may also be the preferred form in 10-digit calling areas.

# »» Strip MSD

# Write Security: 3 Read Security: 5

Strips a selected quantity of the Most Significant Digits (MSD) of a dialed number prior to being forwarded out of the port. For example, a Network port set to accept all calls beginning with 9 (9\$), and with **Strip MSD** set to 1, would send all digits toward the Network except the leading 9.



**Strip MSD** does not affect the **Call Accept** criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criteria.

# »» Netwrk Spec. Fac. -Voice

#### Write Security: 3 Read Security: 5

(Network Specific Facility - Voice) Defines specific facility IEs to send to the Network. Use this option if the customer has subscribed to a network specific facility service such as AT&T Megacom service. The facility request sent can be different for voice calls versus data calls. A setting of **Normal** indicates no special facilities have been subscribed.

### »» Netwrk Spec. - Fac. Data

#### Write Security: 3 Read Security: 5

(Network Specific Facility - Data) Defines specific facility IEs to send to the Network. Use this option if the customer has subscribed to a network specific facility service such as AT&T Megacom service. The facility request sent can be different for voice calls versus data calls. A setting of **Normal** indicates no special facilities have been subscribed.

# »» Called Digits Transferred

# Write security: 2; Read security: 5

Some PRI switches may be provisioned to only send a portion of the called number (like DID). This menu item allows ATLAS to know how many digits to expect (choose from **None**, **Three**, **Four**, and **AII**). The default is All and

would almost always be correct. If less than All digits are sent, then the prefix is defined below.

# »» Outgoing Caller ID

# Write Security: 3 Read Security: 5

Inserts a called ID based on the following selections.

Send as provided

ATLAS forwards whatever ID it receives (including None).

rovided

Substitute if ATLAS inserts a User-defined ID value if no value is re-

not present ceived.

**ID Presentation** Sends to the Network control informa-

tion for the presentation of Caller ID (Presentation Allowed; Presentation Restricted; Number Not Available.)

**ID Number** 

Value for Caller ID to be sent to the Net-

work(i.e., 256 963 8020).

Substitute always

ATLAS always inserts the User-defined ID in place of the

value received.

**ID Presentation** Same as above.

**ID Number** Same as above.

#### »» Source ID

The **Source ID** field simplifies the creation of a Dial Plan in applications where the criteria for switching calls to a certain end point is a function of which end point originated the call.

- Default value = 0. The default ID for all end points is 0 and for all accept # s is 0. With default values, all calls are routed based only on dialed number.
- Multiple end points can have the same Source ID
- When creating the **Call Accept** list, specify a **Source ID**(s) as well as a dialed number or range of dialed numbers to accept.

Say, for example, an application requires that all calls originating from Port 1 of the Quad T1/PRI module in Slot 1 be switched to Port 4 of that same module. Assign a unique **Source ID** (e.g., 7) to Port 1 of the module, and then configure Port 4 to only accept calls from that unique **Source ID** (7).

# »» Swap ANI/DNIS

This option swaps the ANI and DNIS numbers received from the Network. ANI (Automatic Number Identification), is the billing number of the calling party, and DNIS (Dialed Number Identification Service), is the called party number.



This swap will cause the ATLAS switchboard to use ANI to route the call. The accept # in the dial plan must use the ANI number, not the DNIS number.

# QUAD T1/PRI MODULE (NETWORK TERMINATION/RBS)

When you are working in the Network Termination section of the Dial Plan menu, the Slot is defined as a T1/PRI module, and Sig is set to RBS, the following interface configuration options are available:

# »» First DS0 Write security: 2; Read security: 5

Defines to ATLAS the DS0s which will be used for this endpoint. These are the DS0s which ATLAS will use to send and receive calls to and from the Network (PSTN). Outgoing calls which will be allowed or restricted over these DS0s are set by the **Outgoing Call Accept** and **Reject Numbers** discussed earlier.

# »» Number of DS0s Write security: 3; Read security: 5

Specifies the number of DS0s already defined for this endpoint. This field is read-only.

# »» DS0s Available Read security: 5

Indicates which DS0s of the T1 have been defined in this switched end point (indicated by "! "), in another switched end point (indicated by "s"), or in a Dedicated Map (indicated by "n"). The following symbols may display in this field:

**digits** This DS0 is available. The digit that displays in this field represents the last digit of the DS0 number.

- \* This port is requesting this DS0 for this connection, but the DS0 is not yet activated.
- ! This DS0 is used by this port in this connection and is activated.
- **s** This DS0 is used in the switched Dial Plan.
- S This DS0 is used in the switched Dial Plan and conflicts with this connection.
- **n** This DS0 is already used in this dedicated map.
- **N** This DS0 is already used in this dedicated map and conflicts with this connection.

#### »» Signaling Method Write security: 3; Read security: 5

This defines to ATLAS the type of signaling to be used across this trunk. The signaling selected needs to match the signaling being provided by the Network (PSTN). The available options include E&M Immediate, E&M Wink, Loop Start, and Ground Start.

# »» Direct Inward Dialing

# Write security: 3; Read security: 5

This defines to ATLAS whether or not DID is being used by the Network. If DID is Enabled, then the following information must be defined:

# DID Digits Write security: 3; Read security: 5

Transferred Defines the number of digits sent to ATLAS from the Net-

work if DID is used.

# DID Prefix Write security: 3; Read security: 5

Defines to ATLAS the prefix digits which are not received as a part of the DID number. ATLAS uses the combination of prefix and DID number to determine the User end point that should receive the incoming call.

This option only displays if Direct Inward Dialing (DID) is set to Enabled. If DID is Disabled, then you must define the trunk number.

#### »» Trunk Number

# Write security: 3; Read security: 5

When the Network connection does not provide DID digits, then ATLAS must be given a number to use to determine which user end point should receive the incoming call. This field only displays when Direct Inward Dialing is set to Disabled. For example, if a certain incoming DS0 (trunk) is meant to connect to an end point with the accept number of 963-8615, the trunk number would be set to 963-8615.



The trunk number must be specific (i.e., no "wild cards").

# »» Strip MSD

# Write Security: 3 Read Security: 5

Strips a selected quantity of the Most Significant Digits (MSD) of a dialed number prior to being forwarded out of the port. For example, a Network port set to accept all calls beginning with 9 (9\$), and with **Strip MSD** set to 1, would send all digits toward the Network except the leading 9.



**Strip MSD** does not affect the **Call Accept** criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criteria.

# »» Source ID

The **Source ID** field is used to simplify the creation of a Dial Plan in applications where the criteria for switching calls to a certain end point is a function of which end point originated the call.

- Default value = 0. The default ID for all end points is 0 and all accept # s
  is 0. With default values, all calls are routed based only on dialed number.
- Multiple end points can have the same Source ID

• When creating the **Call Accept** list, specify a **Source ID(**s) as well as a dialed number or range of dialed numbers to accept.

For example, an application requires that all calls originating from Port 1 of the Quad T1/PRI module in Slot 1 be switched to Port 4 of that same module. Assign a unique **Source ID** (e.g., 7) to Port 1 of the module, and then configure Port 4 to only accept calls from that unique **Source ID** (7).

# QUAD T1/PRI MODULE (USER TERMINATION/PRI)

When you are working in the User Termination section of the Dial Plan menu, the Slot is defined as a T1/PRI module, and Sig is set to PRI, the following configuration options are available:

# »» Switch Type Write security: 3; Read security: 5

Defines the type of PRI switch that ATLAS is going to emulate. If connected to another ATLAS, both need to be set to the same type. Options include Lucent 5E and AT&T 4ESS.

# »» First DS0 Write Security: 3 Read Security: 5

Defines to ATLAS the first active DS0.

# **»» Number of DS0s** Write Security: 3 Read Security: 5

Defines the number of DS0s used for calls on this PRI. DS0 24 is assumed to be used by the PRI for the D channel.

# » Strip MSD Write Security: 3 Read Security: 5

This option allows a selected quantity of the Most Significant Digits (MSD) of a dialed number for ATLAS to be stripped prior to being forwarded out of the port.

For example, a Network port could be set to accept all calls beginning with 9 (9\$), and then with **Strip MSD** set to 1, all digits would be sent toward the Network except the leading 9.



The Strip MSD parameter does not affect the Call Accept criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criteria.

# » Network Specific Facility Voice

# Write Security: 3 Read Security: 5

Defines the specific facility IEs to send to the Network. Use this option if the customer has subscribed to a network specific facility service such as AT&T Megacom service. The facility request sent can be different for voice calls versus data calls. A setting of **Normal** indicates no special facilities have been subscribed.

# » Network Specific Facility Data

#### Write Security: 3 Read Security: 5

Defines the specific facility IEs to send to the Network. Use this option if the customer has subscribed to a network specific facility service such as AT&T Megacom service. The facility request sent can be different for voice calls

versus data calls. A setting of **Normal** indicates no special facilities have been subscribed.

# »» Called Digits Transferred

# Write security: 3; Read security: 5

Defines to ATLAS the number of called-number digits to forward. When attached to a PBX, the PBX may be provisioned to expect to receive fewer than all of the called digits of the incoming call. This would normally be set to All.

# »» Outgoing Caller ID

# Write Security: 3 Read Security: 5

This item allows the user to insert a called ID to be added to outgoing calls (coming in from attached User equipment). If set to **Send as Provided**, then ATLAS will forward whatever ID it receives (including none). If set to **Substitute if not present**, then ATLAS will insert a User defined ID value if no value is received. If set to **Substitute Always**, then ATLAS will always insert the User defined ID in place of the value received.

# » ID Presentation

Defines control information for the presentation of **Caller ID** to be inserted (**Presentation Allowed**; **Presentation Restricted**; **Number Not Available**).

#### » ID Number

Value for **Caller ID** to be sent to the Network (i.e., 256 963 8020).

# » Source ID

The **Source ID** field simplifies the creation of a Dial Plan in applications where the criterion for switching calls to a certain end point is a function of which end point originated the call.

- Default value = 0. The default ID for all end points is 0 and all accept # s
  is 0. With default values, all calls are routed based only on dialed number
- Multiple end points can have the same Source ID.
- When creating the Call Accept list, specify a Source ID(s) as well as a dialed number or range of dialed numbers to accept.

For example, an application requires that all calls originating from Port 1 of the Quad T1/PRI module in Slot 1 be switched to Port 4 of that same module. Assign a unique **Source ID** (e.g., 7) to Port 1 of the module, and then configure Port 4 to only accept calls from that unique **Source ID** (7).

#### »» Swap ANI/DNIS

This option swaps the ANI and DNIS numbers prior to being forwarded to the attached user equipment. ANI (Automatic Number Identification) is the billing number of the calling party, and DNIS (Dialed Number Identification Service) is the called party number.



This swap will occur after the ATLAS switchboard has routed the call. The accept # in the dial plan must use the number in the DNIS position prior to swapping.

# QUAD T1/PRI MODULE (USER TERMINATION/RBS)

When you are working in the User Termination section of the Dial Plan menu, the Slot is defined as a T1/PRI module, and Sig is set to RBS, the following configuration options are available:

# »» First DS0/Number of DS0s

# Write security: 3; Read security: 5

Defines to ATLAS the DS0s which will be used for this end point. These are the DS0s which will be used by ATLAS to send and receive calls to and from User equipment (PBX). The incoming calls which will be accepted and the outgoing calls which will be restricted over these DS0s are set by the Incoming Call Accept and Outgoing Call Reject Numbers discussed earlier.

#### »» DS0s Available

# Read security: 5

Indicates which DS0s of the T1 have been defined in this switched end point (indicated by "! "), in another switched end point (indicated by "s"), or in a Dedicated Map (indicated by "n").

# »» Signaling Method

# Write security: 3; Read security: 5

Defines to ATLAS the type of signaling to be used across this trunk. The signaling selected needs to match that being used by the user equipment (PBX). The available options include E&M Immediate, E&M Wink, Loop Start, and Ground Start.



ATLAS converts signaling types between Network and User Terminations.

# »» Direct Inward Dialing

# Write security: 3; Read security: 5

Defines to ATLAS whether DID is being used by the Network. This option only displays if Direct Inward Dialing (DID) is set to Enabled. If DID is Enabled, then the following information must be defined:

DID Digits Write security: 3; Read security: 5

**Transferred** Defines the number of digits sent to ATLAS from the Net-

work if DID is used.

#### DID Prefix Write security: 3; Read security: 5

Defines to ATLAS the prefix digits which are not received as a part of the DID number. ATLAS uses the combination of prefix and DID number to determine the User end point that should receive the incoming call.



If DID is Disabled, then you must define the trunk number.

#### » Caller ID Number

# Write security: 3; Read security: 5

Defines the number for ATLAS to use to provide Caller ID to the Network for outgoing calls sent through this end point. This option only displays if **Direct Inward Dialing** is set to **Disabled**. This item is optional.



The Caller ID number must be specific (i.e., no "wild cards").

#### »» Strip MSD

# Write Security: 3 Read Security: 5

This option allows a selected quantity of the Most Significant Digits (MSD) of a dialed number to be stripped prior to being forwarded out of the port. For example, a User port could be set to accept all calls beginning with 8 (8\$), and then with Strip MSD set to 1, all digits would be sent toward the network except the leading 8.



The Strip MSD parameter does not affect the Call Accept criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criteria.

#### »» Source ID

# Write security: 3; Read security: 5

The **Source ID** field simplifies the creation of a Dial Plan in applications where the criteria for switching calls to a certain end point is a function of which endpoint originated the call.

- Default value = 0. The default ID for all end points is 0 and all accept # s
  is 0. With default values, all calls are routed based only on dialed number.
- Multiple end points can have the same Source ID.
- When creating the **Call Accept** list, specify a **Source ID**(s) as well as a dialed number or range of dialed numbers to accept.

For example, an application requires that all calls that originate from Port 1 of the Quad T1/PRI module in Slot 1 be switched to Port 4 of that same module. Assign a unique Source ID (e.g. 7) to Port 1 of the module, and then configure Port 4 to only accept calls from that unique Source ID (7).

# **QUAD NX56/64 MODULE (USER TERMINATION)**



The Quad Nx56/64 can only serve as a user termination end point.

When you are working in the **User Termination** section of the **Dial Plan** menu, and the **Slot** is defined as a QuadNx56/64 module, the following interface configuration options are available:

**»» Ports Available** Indicates which of the four ports of the Quad Nx56/64 module have

already been defined either in another switched end point (indicated by "s") or in a Dedicated Map (indicated by "n"). This field is read-only.

»» **Number of Ports** Defines to ATLAS how many of the ports could be used to answer calls to

the number(s) defined in the Accept Call list. You can enter numbers 1 through 4. The ports are contiguous beginning with the Port number select

and the number of ports.

For example, if the port selected (as a part of Slot/Port selection) is 2, and the number of ports selected here was 2, then ports 2 and 3 would be enabled to receive calls to the numbers listed under the Incoming Call

Accept list.

**»» Number to dial** When originating a call, this is the number to dial.

**Specifies** whether originated calls 56K or 64K.

»» Dial Call As Specifies whether originated calls are dialed as Digital, Voice, or Audio.

**»» Source ID** Source ID for the outgoing call.

**»» Min DS0s** Minimum number of DS0s to connect with using BONDING. Note that this

requires the IMUX-56/64 module.

»» Max DS0s Maximum number of DS0s to connect with using BONDING. Note that this

requires the IMUX-56/64 module.

# **OCTAL BRI MODULE (NETWORK TERMINATION)**

The Octal BRI with a "U" interface can interface directly to the Network (PSTN). When you are working in the **Network Termination** section of the **Dial Plan** menu and the **Slot** is defined as a UBRI-8 option module, the following interface configuration options are available:

»» Switch Type Write security: 2; Read security: 5

Defines the type of ISDN switch that ATLAS is connected to. If connected to another ATLAS, both need to be set to the same type. The available options

are Lucent 5E, Northern DMS 100, and National ISDN.

»» SPID List Write security: 2; Read security: 5

In order to properly operate with a network (PSTN) ISDN switch, the BRI interface must have SPID (Service Profile Identifier) and phone number(s) that match the SPID(s) and Phone number(s) which have been programmed into the ISDN switch for this line. Each BRI may have one or more phone numbers and SPIDs. The **SPID Number** list submenu defines to ATLAS these parameters.

This option allows a selected quantity of the Most Significant Digits (MSD)

**Phone Number** The phone number(s) assigned to this BRI phone

line.

**SPID Number** This entry must match the SPID number(s) which

have been set in the Network's ISDN switch (or in the PBX) for this BRI line. A SPID must be entered for

each phone number.

**Calls** The number of calls (1 or 2) which can be received or

sent on this number/SPID.

D64, D56, Audio,

Speech

These options reflect what the Network has provisioned for this SPID. If the BRI was purchased with different services provisioned for the SPIDs, then the

call must match the services supported.

»» Strip MSD

This option allows a selected quantity of the Most Significant digits of a dialed number for ATLAS to be stripped prior to being forwarded out of the port. Note that the Strip MSD parameter does not affect the Call Accept criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criteria.

»» Source ID

Source ID for the incoming calls.

# **OCTAL BRI MODULE (USER TERMINATION)**

The Octal BRI with a "U" interface acts as the Network while interfacing to user equipment (terminal adapters). When you are working in the **Network Termination** section of the **Dial Plan** menu and the **Slot** is defined as a UBRI-8 module, the following interface configuration options are available:

»» Switch Type

# Write security: 2; Read security: 5

Defines the type of ISDN switch that ATLAS will simulate. If connected to another ATLAS, both need to be set to the same type. The available options include Lucent 5E, Northern DMS 100, and National ISDN.

»» SPID List

## Write security: 2; Read security: 5

ATLAS, acting as the Network, must use a SPID and a phone number in order to satisfy the ISDN connection protocol expected by the User's Terminal Adapter (TA).

**Phone Number** The phone number(s) assigned to this BRI phone line.

**SPID Number** This entry will define the SPID number(s) which will be

used for this BRI line. Although the value of the SPID is not significant, a SPID must be entered for each phone number. For convenience, the SPID can be set to be the

same as the phone number.

NOTE

ATLAS 800<sup>PLUS</sup> does not support autoSPID detection software

which some terminal adapters offer.

**Calls** For User terminations, the number of calls is fixed at 2.

D64, D56, Audio, Speech These options reflect what the Network has provisioned for this SPID. If the BRI was purchased with different services provisioned for the SPIDs, then the call must match

the services supported.

»» Strip MSD

This option allows a selected quantity of the Most Significant digits of a dialed number for ATLAS to be stripped prior to being forwarded out of the port. Note that the Strip MSD parameter does not affect the Call Accept criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criteria.

»» Source ID

Source ID for the incoming calls.

»» Outgoing Caller ID

Specifies how caller ID information is sent to the user BRI device.

**Send as** Send caller ID information as provided by the user BRI device.

**Substitute if** If no caller ID information is provided by the user BRI device, substitute with **ID Presentation** and **ID Number**.

Substitute Ignore caller ID information is provided by the user BRI device, and substitute with ID Presentation and ID Num-

ber.



The following options are only available if Outgoing Caller ID is not set to Send as Provided.

**»» ID Presentation** Specifies the presentation of the caller ID information.

**»» ID Number** This is the substitute number for the caller ID information.

# CREATING DIAL PLANS—EXAMPLES

The ATLAS **Dial Plan** acts as the numbering plan for switched connections. This menu defines to ATLAS the phone numbers and features associated with dual-tone-multifrequency (DTMF) dialing, Primary Rate ISDN (PRI), and Basic Rate ISDN (BRI). To operate as a switch, ATLAS must be able to terminate network connections (*network terminations*) and emulate the network onto other termination equipment (*user terminations*).

# **Understanding Dial Plan Configurations**

Understanding Dial Plan configurations results in the successful creation of a switched connection. This understanding includes determining which of the connections are acting as network terminations and which are acting as user terminations. Use Examples 1 and 2 to help clarify the definitions for these two types of terminations.

# **Example 1** PSTN Connection Dial Plan Configuration

In this example, access to the PSTN is provided by a single PRI line. Therefore, this line is configured as a network termination. The remaining circuits, which feed various types of switched equipment, are configured as user termination because ATLAS is emulating the network on those connections (see Figure 10-3).

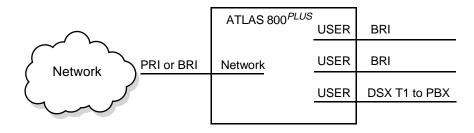


Figure 10-3. PSTN Connection

# **Example 2** Point-to-Point Connection Dial Plan Configuration

In this example, ATLAS A operates as the network while ATLAS B *terminates* the network. That is, ATLAS A emulates the network and its PRI interface acts as the user termination. The PRI interface of ATLAS B acts as the network termination (see Figure 10-4).

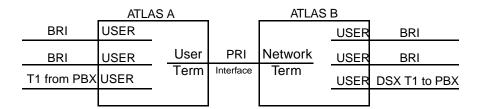


Figure 10-4. Point-to-Point

# **Example 3** Remote Access and Video Conferencing Dial Plan

A corporate office has T1 RBS service for voice but wants to add a PRI for video conferencing and remote access. The office would like to use the PRI for all functions, but it still wants to use the incoming BRI to supply added bandwidth. The office wants to provide BRI lines to the video equipment, provide a PRI to the remote access server (RAS), and send a T1 RBS to the PBX (see Figure 10-5).

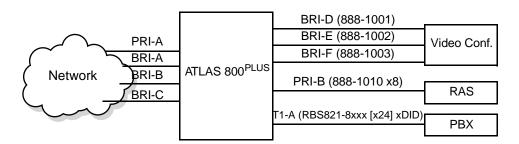


Figure 10-5. Remote Access and Video Conferencing Setup

For this example, the user termination BRI lines (D, E, F) each have a specific phone number. The PRI serving the RAS has an 8-number hunt group, and the T1 to the PBX uses DID. Assume that all calls originating from the PBX to 1-900 numbers are restricted. Also, assume that the network termination BRI lines (A, B, C) only allow outgoing calls to other local corporate offices for video conferencing. The numbers fall in the range of 888-0100 to 888-0120. The following Step/Action Tables and numbered tables provide information on setting up this example.

Instructions for Configuring the Ports for Example 3			
Step Action			
1	Prior to setting up the Dial Plan, you must configure the Controller T1/PRI interfaces.		
2	This configuration action only brings up the T1 transport; set the BRI configuration (SPID and phone number) as part of the Dial Plan.		

	Instructions for Setting Up Dial Plan for Example 3			
Step	Action			
1	Determine the network and the attached equipment (video equipment and PBX) provisioning (see Table 10-1).			
2	From <b>Dial Plan</b> , select <b>Global Parameter</b> , and enter the local area code (needed for Caller ID operation).			
3	Determine which ports are network terminations and which are user terminations.			
4	Define the phone number acceptance and rejection criteria for each termination.			
NOTE	This example includes one PRI port terminating the network (PRI-A) and three BRIs (BRI A, B, and C)—see Table 10-2.  User terminations include one PRI, one RBS T1, and three BRIs			
	(see Table 10-3).			

61200226L1-1 ATLAS 800<sup>PLUS</sup> User Manual 10-23

Table 10-1. Network and Attached Equipment Provisioning

Network PRI	Type of provided PRI switch National ISDN DMS 100 custom 4ESS custom 5ESS custom DID- number of digits
	Type of provided BRI switch National ISDN DMS 100 custom 5ESS custom SPID(s) and phone number(s) provisioned for the BRI line
User Equipment	PRI Switch type the user equipment expects to interface to (ATLAS supports 4ESS custom and 5ESS custom).
	DID Number of digits.
	BRI Switch type the user equipment expects to interface to (ATLAS supports National ISDN, 5ESS custom, and DMS 100 custom). SPID and phone numbers provisioned in equipment.
	T1 RBS DID enabled on PBX/number of digits; Signaling (E&M/Loop Start/Ground Start).

**Table 10-2. Network Terminations** 

NAME	PORT	OUTGOING ACCEPT#	OUTGOING REJECT#	OTHER
PRI-A	Controller T1 Slot 0, Port 1	•	Blank - No called number will be rejected.	PRI Type: National ISDN
BRI-A BRI-B BRI-C	Octal BRI Slot 1, Port 1,2,3	1)888-01[0,1]X  Allows calls to 888-0100 to 888-0119 2)888-0120	Blank - No called number will be rejected.	BRI Type: National ISDN SPID #s PHONE #s: 888-1001, 1002,1003, & 888-1010 (All)

Table 10-3. User Terminations

NAME	PORT	INCOMING ACCEPT #	OUTGOING REJECT#	OTHER
BRI-D BRI-E BRI-F	Octal BRI Slot 1, Ports 4-5,6	888-1001 (D); 888-1002 (E); 888-1003 (F)	Blank - No called number will be rejected.	BRI type: 5ESS SPID # to match Video Equipment provisioning.  Phone #s: 888-1001 (D); 888-1002 (E); 888-1003 (F)  Phone numbers must match phone numbers provisioned in video equipment.
PRI-B	Controller T1 Slot 0, Port 2	888-1010 This forms a hunt group.	Blank - No called number will be rejected.	PRI type: 5ESS Must match RAS equipment. DID=none
T1-A	Slot 2, Port 1	821-8XXX This accepts all calls beginning with 821-8.	1-900-\$ This rejects all calls beginning with 1-900.	RBS 1st DS0=1; #DS0 = 24 Signalling = E&M wink DID = Enable/# of digits = 4

To implement the Dial Plan for Example 3, navigate to **Dial Plan/Global Param** and set the global parameters for PRI A, B, and C. Then, navigate to **User Term** and set the connections for PRI D, E, and F. The following Step/Action tables provide step-by-step instructions for completing these procedures.

	Setting PRI A Global Param		
Step	Action		
1	Navigate to <b>Dial Plan</b> (in the terminal menu).		
2	Enter the area code by selecting <b>Global Param/Area Code</b> and pressing <b>Enter</b> . Input the area code, and press <b>Enter</b> again.		
3	Define the interface type as PRI by selecting <b>Network Term</b> and entering the following settings: <b>Slot = 0, Port = 1, Sig = PRI</b> .		
4	Tell ATLAS to forward any call to the network by selecting  Out#Accept and entering \$ in the number field. Leave all other selections set to default (Enabled).		
5	Ensure Out#Reject contains no entry.		
6	Set the PRI switch type to <b>National ISDN</b> (from <b>Ifce Config</b> ).		

Setting PRI A Global Param			
Step	Action		
7	Back out of the connection to the index number column by pressing <b>ESC</b> on the keyboard.		
8	Insert three more connections into the list for the BRI lines by typing the letter I three times.		
9	Enter Out#Accept and Out#Reject numbers for Slot 1/ Port 1. The Out#Accept numbers have two entries:  Entry 1) 888-01[0,1]X Entry 2) 888-0120  Allows all numbers 888-0100 to 888-0120		
10	Set the BRI switch type (from <b>Ifce Config</b> ) used by the network to <b>National ISDN</b> . From <b>SPID</b> , enter the SPID numbers and phone numbers which match the network provisioning for this BRI line.		
11	Press <b>ESC</b> to return to the index column, #.		

Setting PRI B Global Param			
Step	Action		
1	While on the entry for BRI A, type C to copy the entire BRI A entry.		
2	Move to the next connection list entry and type <b>P</b> to paste all of the BRI data.		
3	Move to each field and modify as appropriate for BRI B.		

Setting PRI C Global Param			
Step	Action		
1	While on the entry for BRI B, type C to copy the entire BRI B entry.		
2	Move to the next connection list entry and type <b>P</b> to paste all of the BRI data.		
3	Move to each field and modify as appropriate for BRI C.		

After completing the network entries, the network connection map appears as shown in Figure 10-6.

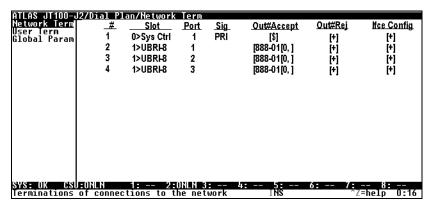


Figure 10-6. Completed Network Map

	Setting User Term Connections		
Step	Action		
1	Navigate to <b>User Term.</b>		
2	Enter connections for BRI D,E, and F in the same manner as BRI A, B, and C: use the copy ( <b>C</b> ) and paste ( <b>P</b> ) commands to enter the appropriate <b>Out#Accept</b> and <b>Out#Reject</b> numbers.		
3	Ensure that the <b>SPID</b> and <b>Phone</b> entries under <b>Ifce Config</b> match the SPID and phone numbers of the attached equipment.		
4	Enter the connection for T1-A: select <b>RBS</b> under <b>Sig</b> , and enter 1-900-\$ under <b>Out#Reject</b> .		
5	Set Trunk Type (under Ifce Config) to Analog.		
6	Set Signaling Method to E&M Wink.		
7	Set <b>DID</b> (under <b>Ifce Config</b> ) to enabled.		
8	Set the DID Digits Transferred to 4.		

When you complete the **User Term** Dial Plan, it appears as shown in Figure 10-7.

61200226L1-1 ATLAS 800<sup>PLUS</sup> User Manual 10-27

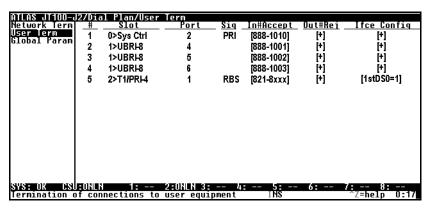


Figure 10-7. Completed User Map

A connection is not actually made (available) until you press **Esc** to move the cursor to the index number or move the cursor onto another connection line.

# Chapter 11 Updating Firmware

# **OVERVIEW**

To provide feature enhancements in the future, ATLAS 800<sup>PLUS</sup> supports firmware updating by field personnel. Two transfer methods are available for use in updating any modules that contain Flash memory, including the ATLAS 800<sup>PLUS</sup> system controller. The first transfer method is via the ATLAS 800<sup>PLUS</sup> Chain-In port using XMODEM protocol. The second transfer method is via the ATLAS built-in Ethernet port using TFTP (Trivial File Transfer Protocol). To simplify the update procedure, a common menu interface is available for updating any upgradable module within ATLAS 800<sup>PLUS</sup> (see also *Update Firmware* on page 6-13). The following sections describe the procedure for updating using either transfer method.



Please consult the appropriate ATLAS 800<sup>PLUS</sup> module manual to determine if the module supports flash upgrading.



Users must use the supplied connector when using VT-100 or when doing any asynchronous Flash activity.

# **XMODEM FIRMWARE UPDATES**

The ATLAS 800<sup>PLUS</sup> supports firmware updating to any upgradable module using XMODEM transfer protocol via the base unit's Chain-In port. XMODEM is found in most PC communications software packages. To configure the Chain-In port's data rate and other communication parameters, consult *Control/Chain In Port* on page 2-4 and *Control/Chain Out Port* on page 2-5.



Ensure the communications software package being used has flow control turned off.

# **Updating Firmware using XMODEM**

Before beginning this procedure,

- you must have a level 2 password for updating any module within ATLAS  $800^{PLUS}$ . Please consult the ATLAS  $800^{PLUS}$  administrator if you do not know the password.
- you must obtain the appropriate update file for the particular module from ADTRAN Technical Support at (888) 4ADTRAN (423-8726).
- you may want to review *Update Firmware* on page 6-13.

	Instructions for Updating Firmware Using XMODEM			
Step	Action			
1	Using a VT-100 terminal emulation communication software package which contains XMODEM protocol support, <b>log in</b> to ATLAS 800 PLUS.			
2	Select System Utility / Update Firmware (see Figure 11-1).			
	Move the cursor to <b>Module Slot</b> , and press <b>Enter</b> . Select the appropriate module slot to update.			
3	To update multiple modules of the same type, select All Modules of a Type from Module Slot. (Only upgradable modules are displayed as choices for Module Type when updating All Modules of a Type in the ATLAS.)			
4	Select XMODEM for Transfer Method.			
5	From <b>Restart Schedule</b> , select the time for the module to perform a restart after completing the update process (see <i>Restart Schedule</i> on page 6-14).			
6	View <b>Current Update Status</b> to verify the progress of the current firmware update or any errors encountered during the download process (see <i>Current Update Status</i> on page 6-15).			
	Select <b>Begin Firmware Update</b> to start the update process. Enter <b>Y</b> to confirm the transfer and to set up the module to receive the XMODEM upload.			
7	When ATLAS is ready to receive the XMODEM upload, the menu screen will clear and display Awaiting XMODEM Upload <ctrl-x> to Cancel. If this does not appear, please review the steps above for possible configuration errors.</ctrl-x>			

Inst	Instructions for Updating Firmware Using XMODEM (Continued)			
Step	Action			
8	From the terminal emulation software, begin the XMODEM upload by using the appropriate command sequence. (If necessary, refer to terminal emulation software documentation for help. Also, when specifying the filename, ensure that the file transferred is the one provided by ADTRAN. Otherwise, the update will not complete successfully.)			
8	Because XMODEM data is being transferred in-band through the menu interface, the VT-100 menus of ATLAS will be inoperable from the Chain-In port. You can cancel the update at any point in time within the terminal emulation software. (Please consult the documentation provided by the terminal emulation software to determine how to do this.)			
9	To update additional modules, begin at step 3 and repeat this process.			

When the update process has successfully completed, Idle displays in the Current Update Status field and Module Update Complete displays in the Previous Update Status field. Either the module restarts immediately and resumes operation, or it restarts at the specified time and day of the week—depending on your selection.

If an error occurred during the update process, **Previous Update Status** displays an appropriate error message.



Figure 11-1. Update Firmware Menu Interface

# **TFTP FIRMWARE UPDATES**

ATLAS  $800^{PLUS}$  supports firmware updates to any module via the 10BaseT Ethernet port using TFTP from a network server. The network server must be capable of supporting TFTP server requests from the TFTP client within ATLAS  $800^{PLUS}$ .

# **Updating Firmware using TFTP**

Before beginning this procedure,

- you must have a level 2 password to perform updates of any modules within ATLAS. Please consult the ATLAS administrator if this password is not known.
- you must obtain the appropriate update file for the particular module from ADTRAN Technical Support at (888) 4ADTRAN (423-8726).
- you must copy the update file provided by ADTRAN to a network server that supports TFTP server requests. Record both the IP address of the server and the full path location of the update file to be downloaded.

Instructions for Updating Firmware Using TFTP	
Step	Action
1	Using a Telnet program, log in to ATLAS.
2	Select System Utility / Update Firmware (see Figure 11-2).
	Move the cursor to <b>Module Slot</b> , and press <b>Enter</b> . Select the appropriate module slot to update.
3	To update multiple modules of the same type, select All Modules of a Type from Module Slot. (Only upgradable modules are displayed as choices for Module Type when updating All Modules of a Type in the ATLAS.)
4	Select TFTP for the Transfer Method.
5	Enter into <b>TFTP Server IP Address</b> , the IP address of the network server that was recorded earlier.
6	Enter into <b>TFTP Server Filename</b> , the full path name and filename of the update file that was recorded earlier.
7	From <b>Restart Schedule</b> , select the time for the module to perform a restart after completing the update process (see <i>Restart Schedule</i> on page 6-14).

In	Instructions for Updating Firmware Using TFTP (Continued)					
Step	Action					
8	View <b>Current Update Status</b> to verify the progress of the current firmware update or any errors encountered during the download process (see <i>Current Update Status</i> on page 6-15).					
9	Select <b>Begin Firmware Update</b> to start the update process. Enter <b>Y</b> to confirm the transfer and to set up the module to receive the TFTP upload.					
9	During the TFTP upload process, various status messages display in Current Update Status to indicate progress.  Table 11-1 describes these messages.					
10	To update additional modules, begin at step 3 and repeat this process.					

When the update process has successfully completed, **Idle** displays in **Current Update Status**, and **Module Update Complete** displays in **Previous Update Status**. Either the module restarts immediately and resumes operation, or it restarts at the specified time and day of the week—depending on your selection.

If an error occurred during the update process, **Previous Update Status** displays the appropriate error message. In this case, return to step 3 and attempt the update process again. If the same error occurs, contact ADTRAN Technical Support.

Table 11-1. TFTP Upload Messages

Message	Meaning
Contacting Server	Indicates communication with the TFTP network server is trying to be established with the specified server address in the TFTP Server IP Address field.
Beginning TFTP Transfer	Indicates communication with the TFTP network server has been established and the update file is being transferred between ATLAS and the TFTP network server.
Completed	Indicates the ATLAS product successfully received the update file.
Error: File Not Found	Indicates the TFTP network server was unable to locate the specified file name or path in the TFTP Server Filename field.
Error: Access Violation	Indicates the TFTP network server denied ATLAS access to the given update file name and path. Please verify appropriate user rights are selected for the specified path.

**Table 11-1. TFTP Upload Messages (Continued)** 

Message	Meaning	
Error: Illegal Operation	An unknown operation was detected by ATLAS when transferring the update file from the TFTP network server.	
Error: User Aborted	Indicates the user selected Cancel Update to abort reception of the update file from the TFTP network server.	

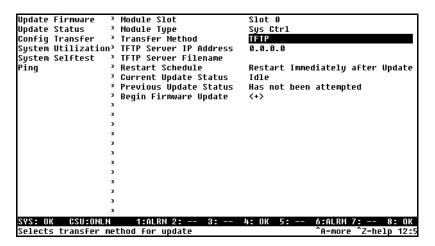


Figure 11-2. Update Firmware Menu Interface

## Chapter 12 SNMP Management

#### **SNMP**

As local area network (LAN) environments became standardized over the past ten years, multivendor equipment grew with competition. It became necessary to manage various vendor equipment from a single control console. Thus, Simple Network Management Protocol (SNMP) emerged as the standard for managing commercial TCP/IP networks. The term SNMP broadly refers to the message protocols used to exchange information between the network management station and the managed devices, as well as to the structure of network management databases.

## **Basic Components**

SNMP has three basic components: network manager, agent, and management information base (MIB).

#### **Network Manager**

The network manager is a control program that collects, controls, and presents data pertinent to the operation of the network devices. It resides on a network management station.

#### Agent

The agent is a control program that responds to queries and commands from the network manager and returns requested information or invokes configuration changes initiated by the manager. It resides in **each** network device.

#### **MIB**

The MIB is an index to the organized data stored within a network device. The MIB defines the operating parameters that can be controlled or monitored. When the MIB requests the network manager to retrieve or modify a particular piece of information about a network device, the network manager transmits that request to the network device. The **agent** in that device interprets the incoming request, performs the requested task, and sends its response to the network manager. The network manager collects all of the data from the various network devices and presents it in a consistent form.

#### **SNMP TRAPS**

An SNMP trap is a message sent by a network device, such as the ATLAS  $800^{PLUS}$ , to report an operational anomaly or alarm condition.

### **Trap Destination List**

A trap destination list contains information about sites designated to receive SNMP traps. You can configure this list via a Telnet session or the VT-100 terminal menu. The ATLAS  $800^{PLUS}$  supports up to four trap destination lists. By default, the destination list is empty.

### **Configuring a Trap Destination List via Terminal Menu**

To configure the trap destination list, from the terminal menu select **System Config / SNMP / Traps Destination**. Then enter your information, similar to that shown in Table 12-1. (See also, *Traps Destination* on page 6-10.)

**IP Address Trap Filtering** Community 0 0.0.0.0 public [+] 1 0.0.0.0 public [+] 2 0.0.0.0 public [+] 3 0.0.0.0 public [+]

Table 12-1. Trap Destination List

*IP Address* is the address of the network management station to which ATLAS 800<sup>PLUS</sup> sends the trap. *Community* is the trap community-name used for the selected network device. *Trap Filtering* is a record allowing you to assign thresholds to each category of the ATLAS 800<sup>PLUS</sup> events.

## Filtering (Disabling) Traps

You can disable trap generating events in three ways:

- 1. Disable Trap Transmission.
  - From the terminal menu, select **SNMP** and set **Trap Transmission** to **DISABLED**.
- 2. Define trap thresholds to disable specific trap events. Refer to the ATLAS MIB in *System Event Logging* on page A-1 for a description of each trap event supported by the ATLAS.
  - For example, consider the **coldStart** trap, a system controller event. If you defined for destination 0 a trap filtering threshold of **Warning** for

the system controller, the **coldStart** trap would not generate to that destination because the **coldStart** trap severity level is defined as **Normal**. (Recall that each trap event has a severity level: **Disabled**, **Informational**, **Normal**, **Warning**, **Minor**, **Major**, and **Critical**.)

3. Control certain traps through SNMP of specific MIB variables. These variables are outlined in the remainder of this chapter.

#### **Standard Traps**

Table 12-2 describes the standard traps supported by ATLAS.

Table 12-2. Standard Traps

Index	Trap Name	Severity	Description
0	coldStart	Normal	ATLAS is such that its configuration may be altered; this trap is generated on power up.
1	warmStart	Normal	ATLAS is reinitializing without altering its configuration.
2	linkDown	Warning	One of the ATLAS communication links has failed.
3	linkUp	Normal	One of the ATLAS communication links has come up.
4	authenticationFailure	Informational	ATLAS has received a protocol message that has failed authentication.

RFC1213, or MIB II, defines the object type <code>snmpEnabledAuthenTraps</code>. If you set this value to 2, the generation of the <code>authenticationFailure</code> trap is disabled. This trap is enabled by setting <code>snmpEnableAuthenTraps</code> to 1. One possible reason for an authentication failure would be an invalid community name in the received protocol message.

#### **DS1 Traps**

ATLAS supports RFC1406, the DS1 standard MIB, as well as the ADTRAN DS1 MIB, an extension to RFC1406. The ADTRAN DS1 group lets you send traps for DS1 Alarm Failures and Performance Threshold Crossing Alerts. The DS1 Alarm Table, defined in the ADTRAN DS1 extension MIB, contains entries that enable the status bits to send an Alarm Trap message. Each Alarm Table row entry corresponds to a DS1 interface managed by the device. The DS1 Alert Table, also defined in the ADTRAN DS1 MIB, contains similar entries for controlling the Alert Traps.

#### **DS1 Alarm Traps**

DS1 line status is reported in the bit-encoded dsx1LineStatus object variable. Each trap represents a bit value = 1 change in dsx1LineStatus. Table 12-3 describes the DS1 alarm traps supported by ATLAS  $800^{PLUS}$ .

Table 12-3. DS1 SNMP Traps

Alarm	Severity	Description
adATLAS800NoAlarm	Warning	No alarms are present.
adATLAS800RxYellow	Minor	The Far end is experiencing Red Alarm (a.k.a. Yellow Alarm).
adATLAS800TxYellow	Warning	The Near end is sending Loss Frame Indication (a.k.a. Yellow Alarm).
adATLAS800RxAIS	Minor	The Far end is sending Alarm Indication Signal (a.k.a. Blue Alarm).
adATLAS800TxAIS	Warning	The Near end is sending Alarm Indication Signal (a.k.a. Blue Alarm).
adATLAS800RedAlarm	Major	The Near end is experiencing Loss of Frame (a.k.a. Red Alarm).
adATLAS800LOS	Major	The Near end is experiencing Loss of Signal.

When enabled, ATLAS  $800^{PLUS}$  sends alarm traps to the each member of the trap destination list upon detecting status bit changes in dsx1LineStatus. Each status change sets an event bit = 1 in the adDS1LineEvent variable in the DS1 alarm table. If you have previously set the corresponding enable bit = 1 in the adDS1LineArm variable and adDS1AlarmEnable = On, then

ATLAS  $800^{PLUS}$  sends an alarm trap message. A single alarm trap message may report multiple event changes. ATLAS  $800^{PLUS}$  clears the event bits after sending the trap message or sending the response to a *Get* request for the *adDS1LineEvent* variable.

#### **DS1 Alert Traps**

RFC1406 also defines a series of *Current* and *Total Alert* threshold values. You can enable ATLAS  $800^{PLUS}$  to send an alert trap message to each member of the trap destination list when accumulated error statistics exceed these threshold values. Table 12-4 describes the alert traps supported by ATLAS  $800^{PLUS}$  for events that have occurred in the last 15-minute interval.

Table 12-4. DS1 Current Alert SNMP Traps

Current Alert	Severity	Description
adATLAS800CurrentES	Warning	The current interval errored second threshold has been exceeded.
adATLAS800CurrentSES	Warning	The current interval severely errored second threshold has been exceeding.
adATLAS800CurrentSEFS	Warning	The current interval severely errored framing second threshold has been exceeded.

Table 12-4. DS1 Current Alert SNMP Traps (Continued)

Current Alert	Severity	Description
adATLAS800CurrentUAS	Major	The current interval is unavailable.
adATLAS800CurrentCSS	Warning	The current interval path code violations have been exceeded.
adATLAS800CurrentLES	Warning	The current interval line errored second threshold has been exceeded.
adATLAS800CurrentCV	Warning	The current interval line code violation threshold has been exceeded.

When one of the *Current Alert* thresholds is exceeded, the corresponding event bit is set to 1 in the adDS1CurrentAlert variable in the DS1 alert table. When enabled, ATLAS  $800^{PLUS}$  sends alert traps to each member of the trap destination list upon detecting status bit changes in adDS1CurrentAlert. If you have previously set the corresponding enable bit = 1 in the adDS1CurrentArm variable and adDS1AlertEnable = On, then ATLAS  $800^{PLUS}$  sends an alert trap message. A single alert trap message may report multiple event changes. ATLAS  $800^{PLUS}$  clears the event bits after sending the trap message or sending the response to a Get request for the adDS1CurrentAlert variable. ATLAS  $800^{PLUS}$  clears the Current Cur

Table 12-5 shows the *Total Alert Traps*, which describe events that have occurred in the last 24-hour interval.

**Table 12-5. Total Alert Traps** 

Total Alert	Severity	Description
adATLAS800TotalES	Warning	The total interval errored second threshold has been exceeded.
adATLAS800TotalSES	Warning	The total interval severely errored second threshold has been exceeded.
adATLAS800TotalSEFS	Warning	The total interval severely errored framing second threshold has been exceeded.
adATLAS800TotalUAS	Major	The total interval unavailable second threshold has been exceeded.
adATLAS800TotalCSS	Warning	The total interval controlled slip second threshold has been exceeded.
adATLAS800TotalPCV	Warning	The total interval path code violations has bee exceeded.

Table 12-5. Total Alert Traps

Total Alert	Severity	Description
adATLAS800TotalLES	Warning	The total interval line errored second threshold has been exceeded.
adATLAS800TotalLCV	Warning	The total interval line code violation threshold has been exceeded.

When one of the *Total Alert* thresholds is exceeded, the corresponding event bit is set to 1 in the *adDS1TotalAlert* variable in the DS1 alert table. When enabled, ATLAS  $800^{PLUS}$  sends alert traps to each member of the trap destination list upon detecting status bit changes in *adDS1TotalAlert*. If you have previously set the corresponding enable bit = 1 in the *adDS1TotalArm* variable and *adDS1AlertEnable* = On, then ATLAS  $800^{PLUS}$  sends an alarm trap message. A single alert trap message may report multiple event changes. ATLAS  $800^{PLUS}$  clears the event bits after sending the trap message or sending the response to a Get request for the adDS1TotalAlert variable.

Current Alert and Total Alert described above are *Near End* events. ATLAS 800<sup>PLUS</sup> also supports Current Alert and Total Alert for the *Far End*. Far End alert traps are generated upon status bit changes in *adDS1FarCurrentAlert* for Current Alerts and *adDS1FarTotalAlert* for Total Alerts. Current and Total Far End Alerts can be disabled by setting the corresponding enable bit = 0 in the *adDS1FarCurrentArm* and *adDS1FarTotalArm* variables, respectively. Far End alert traps can also be disabled by setting *adDS1AlertEnable* = *Off*.

## Chapter 13 ADTRAN Utilities

#### **OVERVIEW**

ADTRAN delivers several PC software utilities along with the ATLAS  $800^{PLUS}$ . These utilities are located on the three diskettes that came with your shipment. They also include MIB files (located in the MIB directory).



Review the readme file (Readme.txt) for the latest information about the utilities.

The utilities make interfacing with the terminal menu and transferring configuration files to and from TFTP servers easier. The utilities all run on Microsoft Windows 3.1 or higher. The following sections describe the Syslog, Telnet, VT-100, and TFTP Server utilities.

#### SYSLOG HOST DAEMON

The SysLog Host Daemon allows remote monitoring, collecting, and logging of ATLAS  $800^{PLUS}$  events in realtime. This information can be useful during installation setups and/or troubleshooting.

To use this utility, you must configure the remote ATLAS  $800^{PLUS}$  (using a Telnet or VT-100 connection) with destination IP address of the PC to which you want to transmit SysLog messages; i.e., the IP address of the PC running the SysLog host utility.

### SysLog GUI

Figure 13-1 on page 13-2 shows the SysLog Host GUI. The conventional Menu Bar is described below beginning on page 13-3 (see also Figure 13-2). Other features are described here.

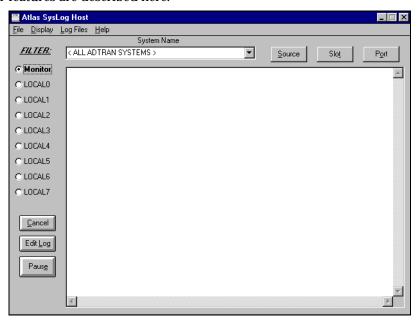
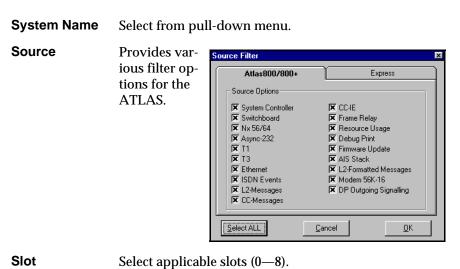


Figure 13-1. ATLAS SysLog Host GUI

#### **Monitor**

The **Monitor** feature allows all SysLog messages to be pre-filtered by **System Name**, **Source**, **Slot** and **Port** before displaying these messages to the user and logging the message to the pre-designated monitor log file.



Select applicable port range.

**Port** 

#### Menu Bar

The SysLog Menu Bar provides common functions. The Menu Tree shown in Figure 13-2 shows the structure.

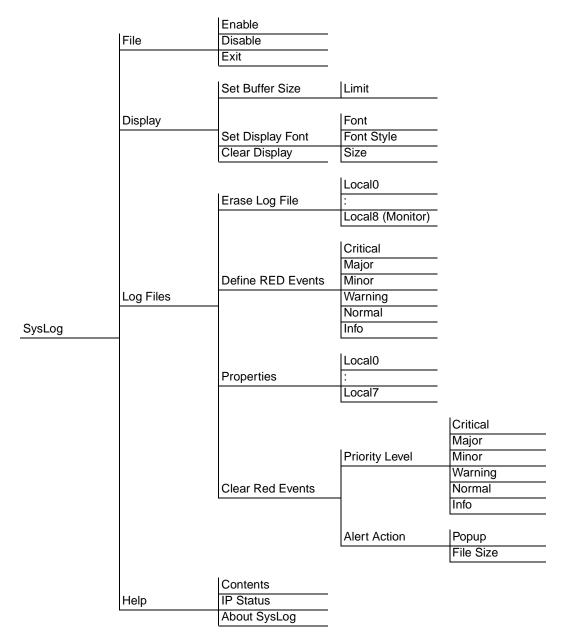


Figure 13-2. SysLog Menu Tree for the Menu Bar

> **FILE** Enables, disables, and exits the SysLog Host program.

> **DISPLAY** Sets the buffer size and display font. Also, clears the display.

#### > LOG FILES

Erases log files, defines Red events, sets priorities and action to be taken when an event occurs, and clears Red events. (See *Define RED Events* on page 13-4.)

#### » Erase Log Files

The SysLog utility, by default, stores all messages of a certain priority in a specified local log file or facility. These files are named LOCAL0.txt, LOCAL1.txt, LOCAL2.TXT, and so on To erase the file, click on this menu.

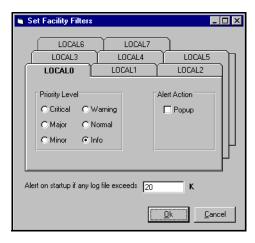
#### » Define RED Events

The red events feature allows the user to predefine a message priority condition so that if the condition occurs, the file is highlighted in red. In the figure shown here, any LOCAL0 through LOCAL7 facility becomes highlighted in red if a Critical, Major or Minor message is received. This feature allows a user to quickly locate problem units during troubleshooting.



#### » Properties

When you click on **Properties**, the **Set Facility Filters** dialog box opens allowing you to specify what types of messages will be logged to an ASCII text file. In the example shown in here, all Sys-Log event messages of **NORMAL** and above (i.e., **CRITICAL**, **MAJOR**, **MINOR** and **WARNING**) will be logged. **Info** (debug) messages will be blocked. In this example, if the log file exceeds 20K, SysLog alerts the user on startup to this fact. Also, from this box, you can set the alert action.



#### » Clear Red Events

Click this item to clear all predefined red events.

#### > HELP

Opens the help files, reports on the IP status, and provides information on SysLog version number.

#### TELNET UTILITY

The Telnet utility delivered with the ATLAS 800 provides enhancements to standard Telnet programs that make it easier to work with ATLAS 800 options.

Access the Telnet program remotely through the 10BaseT Ethernet port. For a detailed description of how to work with the Telnet program, refer to *Navigating the Terminal Menu* on page 5-1, and for a detailed description of the Telnet interface, see Figure 5-1 on page 5-1. If you need help setting up the ATLAS 800 for a Telnet session, refer to *Using The Terminal Menu* on page 3-2.

The Telnet menus include **Session**, **Edit**, **Options**, **Capture**, and **Help** (see the menu tree in Figure 13-3 on page 13-5).

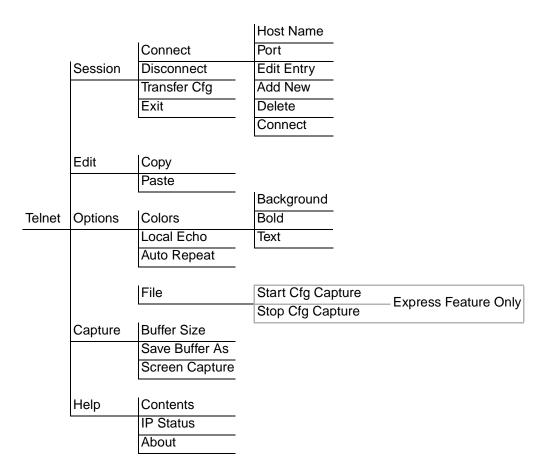


Figure 13-3. Telnet Menu Tree

#### > SESSION MENU

Click on **Session** to open the Telnet session.

» Connect

Opens dialog box for setting **Host Name** and **Port** parameters for a Telnet session. Also lets you **Edit Entry**, **Add New** entry, and **Delete** 



stored entries. When the parameters are set, click **Connect** to make the connection. Click **Cancel** to end the session.

»» Host Name

Accepts and stores host names. You may either enter a name, an IP address, or a domain name directly from this field. Click on the drop-down arrow to display a complete list of previously stored host names.

»» Port

Provides several port options. You may enter port numbers directly into this field to connect to non-standard ports or select the drop-down combo-box to display the following options:

**Telnet** establishes a Telnet session

**Echo** provides a loopback for troubleshooting

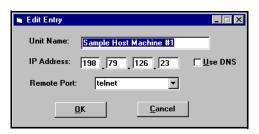
**Discard** bit bucket; discards data

**Daytime** returns the time

**Chargen** displays as a unique character stream; used for self-tests

»» Edit Entry

Changes either the unit name or the IP address of each host. Press either **Tab**, **Return**, or a **period** (.) after each number in the IP address to move to the next field. If you press **Return** or (.) while the cursor is located in each IP field, that field entry is deleted.



»» Add New

Prompts you for the same information as the **Edit Entry** dialog box for new host. When enabled, the **Use DNS** (Domain Name Server) feature allows users to request **Domain Look Up** via a DNS server on the network, rather than specifying an IP address. The name then appears in the **Host Name** field.

»» Delete

Removes a host name from the list; simply, select the host name you want to remove, and, at the prompt, click **Delete**.

»» Connect

Establishes the Telnet session.

» Disconnect

Terminates the Telnet session.

To re-establish the session, select **Connect** from **Session Menu** or press **Enter** three times. This action restores the previous connection.

**» Transfer Cfg**This feature is used with Express products primarily for sending configura-

tion files to the unit.

**» Exit** Ends the Telnet session and closes the Telnet screen.

> **EDIT MENU** Provides **Copy** and **Paste** commands.

> OPTIONS MENU

Provides viewing alternatives for the terminal screen.

**» Colors** Three options change the color of the background window (**BackGround**),

bold highlights (Bold), and text (Text).

**» Local Echo** Echoes each character that you enter.

**» AutoRepeat** Repeats characters you select from the keyboard, if you hold down the key.

> CAPTURE MENU

Provides options for capturing screen images.

**» File** Sends screen options data to a file in the format options listed below:

»» Start Cfg Capture Used with the Express product line to start sending the scrolling screen cap-

ture to a file storage location.

**»» Stop Cfg Capture** Used with the Express product line to stop sending the scrolling screen cap-

ture to a file storage location.

» **Buffer Size** Disables terminal window scroll bars when set to zero. (This is the normal

setting for ATLAS.) This number represents the number of lines to capture

in the memory buffer.

**» Save Buffer As** Save screen capture to a file.

**Screen Capture** Copies the text on the current Telnet screen to the clipboard. You can open

any word processor and paste the clipboard contents into the program. This

option is helpful when debugging.

> **HELP MENU** Provides on-line help for using the ADTRAN Utilities.

**» Contents** Opens the on-line help.

» **IP Status** Displays the local port address and the status of the connection.

» About Displays version and owner information.

#### **VT-100 UTILITY**

Use the VT-100 to configure an ATLAS 800 which is directly connected to a PC. The VT-100 display is almost identical to the Telnet display.

For a detailed description of how to work with the Telnet program, refer to *Navigating the Terminal Menu* on page 5-1, and for a detailed description of the VT-100 interface, see *VT-100 Utility* on page 13-8. If you need help setting up the ATLAS 800 for a VT-100 session, refer to *Using VT-100 Terminal Emulation* on page 3-4.

VT-100 menus include **Session**, **Edit**, **Port**, **Options**, **Capture**, and **Help** (see the menu tree in Figure 13-4).

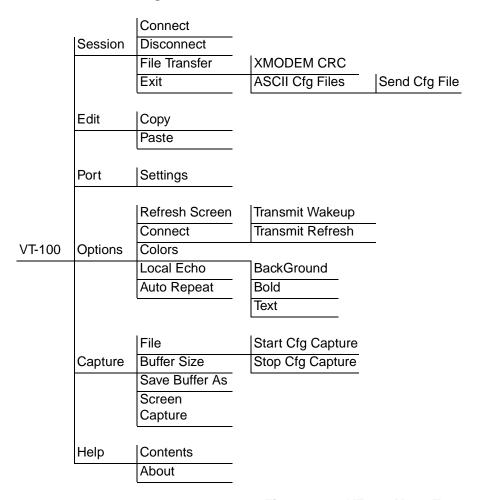


Figure 13-4. VT-100 Menu Tree

# > SESSION MENU

Opens VT-100 terminal emulation session.

**» Connect** Opens a specified serial port for a VT-100 session.

**» Disconnect** Closes a specified serial port at the end of a VT-100 session.

**» File Transfer** Uploads and downloads files to and from an ATLAS.

**»» XMODEM CRC** Selects the XMODEM file transfer protocol.

»» **ASCII Cfg Files** Selects ASCII transfer mode. Primarily useful for configuration transfers for

the Express products.

> **EDIT MENU** Identical to the Telnet **Edit Menu** (see *Edit Menu* on page 13-7).

> **PORT MENU** Changes serial COM port **Settings**. Provides data

rate settings from 300—57600 bps.



#### > OPTIONS MENU

Provides terminal screen commands.

» Refresh Screen Redraws the screen.

» Connect Provides the options Transmit Wakeup and Transmit Refresh.

»» Transmit Wakeup Provides a control sequence that puts the ATLAS Control Port online in ter-

minal mode.

»» Transmit Refresh Provides a control sequence to automatically refresh the screen when con-

necting. (This is the default setting for the ATLAS.)

» **Colors** Identical to Telnet **Colors Menu** (see *Colors* on page 13-7).

**» Local Echo** Echoes each character that you enter.

**» AutoRepeat** Repeats characters you select from the keyboard if you hold down the key.

# > CAPTURE MENU

Identical to the Telnet Capture Menu (see Capture Menu on page 13-7).

> **HELP MENU** Provides on-line help and information about the version number.

**» Contents** Opens on-line help.

**» About** Displays version and owner information.

#### **TFTP SERVER**

The TFTP Server utility transfers ATLAS 800 configuration files to and from a TFTP server. You can install this program on a PC running any version of Microsoft Windows. The configuration of an ATLAS 800 can be saved offline as a backup file. The saved file may also be used to send the same configuration to multiple ATLAS 800 units. Transfer configuration files using the TFTP protocol (a TCP/IP user protocol) via the 10BaseT Ethernet port. The ATLAS 800 must have a valid IP address, subnet mask, and default gateway (if required), and be connected to an Ethernet network before proceeding. Figure 13-6 shows the TFTP server interface.



Files must be placed in the Application directory where you installed the product. Received files are also placed here.

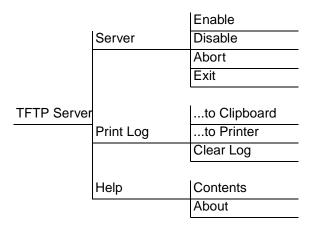


Figure 13-5. TFTP Server Interface Menu Tree

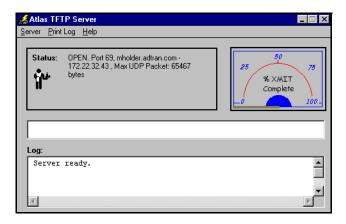


Figure 13-6. TFTP Server Interface

Only one configuration transfer session (upload or download) may be active at a time. The TCP/IP parameters are not saved or overwritten as part of an ATLAS 800 unit's transferred configuration to allow sending identical configurations to multiple units. When you start this program, a port is automatically opened.

>	<b>SERVER</b>
	MENU

Provides enable, disable, abort, and exit options.

**» Enable** Enables the TFTP server. The IP address displays in the Status field and

Server Ready displays in the Log field.

**» Disable** Disables the TFTP server. When you select this option, the message PORT

CLOSED displays in the Status field and Port Closed displays in the Log

field.

**» Abort** Terminates a transfer that is in progress.

**» Exit** Terminates active transfers and closes the TFTP window.

> **PRINT LOG** Provides print options.

**» ...to Clipboard** Copies the information in the Log field to the clipboard. You can then open

any word processor and paste the information into the program for review.

**» ...to Printer** Sends the information in the Log field to the default printer.

» Clear Log
Deletes the information stored in the Log field.

> **HELP** Provides on-line help and version information.

**» Contents** Opens on-line help.

**» About** Displays version and owner information.

#### STATUS FIELD

This field displays general information about port and transfer status. This field is read-only. The unlabeled field in the center of the screen displays prompts about the status of active transfers, such as bytes transferred and received.

#### **METER FIELD**

The **XMIT** meter provides a visual record of the transfer process.

#### **LOG FIELD**

This field displays a record of all of the events that occur during the time the TFTP Server is enabled. Use the scroll bar to move up and down the list. To clear the information in this field, from the **Print Log** menu, select **Clear Log**. Save this information to a file before deleting it with the ...to **Clipboard** command.

## Saving the Current Configuration to a TFTP Server

Before trying to save a configuration, ensure that the TFTP server is running. If you are using the ADTRAN TFTP Server program, the server automatically enables when you start the program. Also, please note the following:

- A level 3 or better password is required for a configuration download the same level required to modify most configuration parameters.
   Please consult the ATLAS administrator if level 3 access is not available.
- Some TFTP servers constrain filename formats. For example, a TFTP server running on a PC under any platform may only permit 8.3 format filenames (8 characters, period, and three extender characters).

To save the current configuration, follow these steps:

Step	Action
1	Use Telnet and <b>log in</b> to the ATLAS 800 for which you want to save the configuration file.
2	Select the <b>System Utility</b> menu, then the <b>Config Transfer</b> menu.
3	Set the TFTP Server IP Address to the IP address of the machine running the TFTP server program. (If you are using the ADTRAN TFTP server, the IP address displays in the Status field.)
4	Change the TFTP Server filename to a unique filename for saving the configuration file to the remote server. (Enter the complete directory path to the file.)
5	Move to the <b>Save Config Remotely</b> button and press <b>Enter</b> . Press <b>Y</b> to confirm the transfer request.

#### Successful Transfer

The **Previous Transfer Status** field indicates success or failure of the transfer. If successful, the field reads **TFTP Download Complete**, and the **Current Transfer Status** field displays **Idle**. The file is now present on the TFTP server. (For the ADTRAN TFTP Server, it is stored in the installation directory or the directory you specified.)



TFTP is **not** secure. No passwords are required for client access. Anyone can access files through the IP port on the server machine if they know the target file's name. For security purposes, close this utility as soon as you have finished using it.

#### **Unsuccessful Transfer**

There are various reasons why a configuration download may fail. For example, the server may not allow the specific filename to be created or overwritten, the specified directory path may not be valid, or there may not be sufficient disk space on the remote server for the new file (although configuration files are not normally large). A specific error message displays when the transfer is unsuccessful.

Also, a TFTP server may not be available at the configured IP address. If the TFTP server cannot be contacted, the download attempt will timeout in approximately 20 seconds. Remember to direct transferred files to the Application directory.

## **Retrieving the Configuration from a TFTP Server**

Before trying to retrieve the configuration, ensure that a TFTP server is running on a remote machine. If you are running the ADTRAN TFTP Server program, the server is automatically enabled when you start the program.

Also, a level 3 or better password is required for performing a configuration upload. Please consult the ATLAS administrator if level 3 access is not available.

Ins	Instructions for Retrieving a Configuration from TFTP Server					
Step		Action				
1		Use Telnet to <b>log in</b> to the ATLAS 800 <sup>PLUS</sup> to which you want to upload a configuration file.				
2	Select th	e System Utility menu, then the Config Transfer menu.				
3	running t	Set the TFTP Server IP Address to the IP address of the machine running the TFTP server program. (If you are using the ADTRAN TFTP server, the IP address displays in the Status field.)				
4	saved co	Change the TFTP Server filename to the filename of a previously saved configuration you wish to load. (Enter the complete directory path to the file.)				
		Move to the <b>Load And Use Config</b> button and press <b>Enter</b> to proceed with the transfer. Respond with <b>Y</b> to confirm the transfer request.				
5	WARNING	The ATLAS 800 <sup>PLUS</sup> reboots immediately after a configuration successfully loads. No additional confirmation is requested, and any online sessions are terminated.				

The **Current Transfer Status** field indicates the transfer progress. If the upload succeeds, the unit automatically reboots and runs using the new configuration. If the upload fails, an error message displays in the **Previous Transfer Status** field. If the TFTP server cannot be contacted, the transfer attempt times out in approximately 20 seconds.

## Appendix A System Event Logging

This section describes the entries that may be logged by the system event log. Of particular importance is the log event's Category – this is the minimum severity level that must be set in order that the event be logged.



Use caution when changing Categories from their default levels. If too many sources have their Category values set too low, the number of messages being logged in a given period can be very large. If too many messages are being logged too rapidly, system performance can be adversely affected.

Most of the events shown in Table A-1 through Table A-11 are used primarily during troubleshooting and should be turned off in normal operation.

Table	Title	Page #
A-1	Source: System	A-2
A-2	Source: Switchboard	A-3
A-3	Source: Nx 56/64	A-4
A-4	Source Time	A-5
A-5	Source: Ethernet	A-6
A-6	Source: ISDN	A-7
A-7	ISDN Cause Codes	A-10
A-8	Cause Code Log Entries	A-12
A-9	Source: ISDN L2 Messages	A-12
A-10	Source: ISDN Call Control Messages	A-12
A-11	Source: ISDN Information Elements	A-13

Table A-1. Source: System

Event	Category	Console Log String	Front Panel Display String
System Cold Start Generated 5 seconds after the completion of system initialization.	Normal	Cold Start	COLD START
SNMP Authentication Failure Generated if the ATLAS receives an SNMP request from an SNMP manager defined in the ATLAS SNMP Communities list but with a community name that does not match the community name defined in the SNMP Communities list.	Info	SNMP Authentication Failure	AUTHEN FAIL
Module removed or not responding	Warning	Module Not Responding	MODULE OUT -A
Module found	Information	Module Found	MODULE FOUND
Console login failure Three consecutive login attempts were attempted and failed	Minor	Login Failure	LOGIN FAILURE
ATLAS 800 configuration file loaded into the system and activated	Critical	System Configuration Uploaded	CONFIG UPLOADED
The internal system temperature is too high	Critical	Internal Temperature Warning	TEMP WARN -A
The internal system temperature has returned to norma	Critical	Internal Temperature Warning Cleared	TEMP WARN -I
The primary power supply is present but is not operating properly	Critical	Main Power Supply Failure	PS1 WARNING -A
The primary power supply is operating properly or has been removed	Critical	Main Power Supply Failure Cleared	PS1 WARNING -I
The backup power supply is present but is not operating properly	Critical	Backup Power Supply Failure	PS2 WARNING -A
The backup power supply is operating properly or has been removed	Critical	Backup Power Supply Failure Cleared	PS2 WARNING -I

Table A-2. Source: Switchboard

Event	Category	Console Log String	Front Panel Display
Call rejected No such number in dial plan	Warning	<number> rejected: No such number</number>	n/a
Call rejected Number is on outgoing reject list	Normal	<number> rejected: Outgoing reject list</number>	n/a
Call successfully routed	Normal	<number> accepted: <slot> <port></port></slot></number>	n/a
Call rejected All endpoints busy	Normal	<number> rejected: Busy</number>	n/a

Table A-3. Source: Nx 56/64

Clock Slip Alarm Active Major Nx 56/64 Clock Slip Alarm Nx CLK SL Active  Clock Slip Alarm Cleared Major Nx 56/64 Clock Slip Alarm Nx CLK SL Cleared Nx 56/64 Clock Slip Alarm Nx CLK SL Cleared Nx 56/64 PLL Alarm Active Nx PLL AL Pll Alarm Cleared Major Nx 56/64 PLL Alarm Cleared Nx PLL AL External Clock Alarm Major Nx 56/64 External Clock Alarm Nx EXT CL External Clock Alarm Major Nx 56/64 External Clock Alarm Nx EXT CL Cleared Nx PLL AL Excessive Zeros from Nx EXT CL Cleared Nx PLL AL Excessive Zeros from Nx EXT CL Cleared Nx External Clock Alarm Nx EXT CL Cleared Nx PLL AL Excessive Zeros from Nx EXT CL Cleared Nx Excessive Zeros Alarm Nx XS0 AL Excessive Zeros condition Cleared Nx Excessive Zeros Alarm Nx XS0 AL Cleared Nx Excessive Zeros Alar	LIP -I  M -A  M -I  K ALM-A
PII Alarm Active Major Nx 56/64 PLL Alarm Active Nx PLL AL PII Alarm Cleared Major Nx 56/64 PLL Alarm Cleared Nx PLL AL External Clock Alarm Major Nx 56/64 External Clock Alarm Nx EXT CL External Clock Alarm Major Nx 56/64 External Clock Alarm Nx EXT CL Cleared Cleared Nx PLL AL  External Clock Alarm Nx EXT CL  External Clock Alarm Nx EXT CL  Excessive Zeros from Nx 56/64 Excessive Zeros Alarm Nx XS0 AL  Excessive Zeros condition Cleared Nx 56/64 Excessive Zeros Alarm Nx XS0 AL  Excessive Zeros condition Cleared Nx 56/64 Bilateral Loopback Nx BI-LAT  Activated Nx BI-LAT  Bilateral Loopback Nx BI-LAT  Cleared Nx 56/64 Bilateral Loopback Nx BI-LAT  Cleared Nx BI-LAT  Cleared Nx BI-LAT  Cleared Nx S6/64 511 Test Pattern Active Nx TEST F  511 Test Pattern Deactivated Warning Nx 56/64 511 Test Pattern  Cleared Nx TEST F	M -A M -I K ALM-A
PII Alarm Cleared Major Nx 56/64 PLL Alarm Cleared Nx PLL AL  External Clock Alarm Major Nx 56/64 External Clock Alarm Nx EXT CL  External Clock Alarm Major Nx 56/64 External Clock Alarm Nx EXT CL  External Clock Alarm Cleared Nx EXT CL  Excessive Zeros from Nx 56/64 Excessive Zeros Alarm Nx XS0 AL  Excessive Zeros condition Cleared Nx 56/64 Excessive Zeros Alarm Nx XS0 AL  Excessive Zeros condition Cleared Nx 56/64 Bilateral Loopback Nx BI-LAT  Activated Nx F6/64 Bilateral Loopback Nx BI-LAT  Bilateral Loopback Nx F6/64 Bilateral Loopback Nx BI-LAT  Cleared Nx F6/64 Bilateral Loopback Nx BI-LAT  Cleared Nx F6/64 S11 Test Pattern Active Nx TEST F  511 Test Pattern Mx Nx F6/64 S11 Test Pattern Active Nx TEST F  Cleared Nx F1 Alarm Cleared Nx F1 Alarm Cleared Nx F1 Alarm Nx EXT F  Nx F6/64 S11 Test Pattern Active Nx TEST F  Cleared Nx F1 Alarm Cleared Nx F1 Alarm Cleared Nx F1 Alarm Nx EXT F  Nx F6/64 S11 Test Pattern Active Nx TEST F  Cleared Nx F1 Alarm Cleared Nx F1 Alarm Cleared Nx F1 Alarm Nx EXT F  Nx F1 Alarm Cleared Nx F1 Alarm Cleared Nx F1 Alarm Nx EXT F  Nx F1 Alarm Cleared Nx F1 Alarm Cleared Nx F1 Alarm Nx EXT F  Nx F1 Alarm Cleared Nx F1 Alarm Nx EXT CLEARED Nx F1 Alarm Cleared Nx F1 Alarm Nx EXT F  Nx F1 Alarm Cleared Nx F1 Alarm Nx EXT CLEARED Nx F1 Alarm Nx EXT F  Nx F1 Alarm Cleared Nx F1 Alarm Nx EXT F1 Alarm Cleared Nx F1 Alarm Nx EXT	M -I K ALM-A LK ALM-I
External Clock Alarm Major Nx 56/64 External Clock Alarm Nx EXT CL  External Clock Alarm Major Nx 56/64 External Clock Alarm Nx EXT CL  Excessive Zeros from DTE Nx 56/64 Excessive Zeros Alarm Nx XS0 AL  Excessive Zeros condition Cleared Nx 56/64 Excessive Zeros Alarm Nx XS0 AL  Excessive Zeros condition Cleared Nx 56/64 Excessive Zeros Alarm Nx XS0 AL  Excessive Zeros condition Warning Nx 56/64 Excessive Zeros Alarm Nx XS0 AL  Cleared Nx BI-LAT  Active Nx BI-LAT  Bilateral Loopback Nx BI-LAT  Cleared Nx 56/64 Bilateral Loopback Nx BI-LAT  Cleared Nx 56/64 511 Test Pattern Active Nx TEST F  511 Test Pattern Marning Nx 56/64 511 Test Pattern Active Nx TEST F  Cleared Nx TEST F	K ALM-A _K ALM-I
External Clock Alarm Cleared  Major Nx 56/64 External Clock Alarm Nx EXT CL Cleared  Excessive Zeros from DTE  Warning Nx 56/64 Excessive Zeros Alarm Nx XS0 AL Excessive Zeros condition cleared  Warning Nx 56/64 Excessive Zeros Alarm Nx XS0 AL Cleared  Nx XS0 AL Excessive Zeros condition Cleared  Nx XS0 AL Cleared  Nx S6/64 Bilateral Loopback Activated  Nx BI-LAT Cleared  Nx BI-LAT Cleared  Nx BI-LAT Cleared  Nx S6/64 S11 Test Pattern Active Nx TEST F Cleared  Nx TEST F Cleared  Nx TEST F	_K ALM-I
Cleared  Excessive Zeros from DTE  Warning Nx 56/64 Excessive Zeros Alarm Nx XS0 AL  Excessive Zeros condition cleared  Bilateral Loopback Activated  Bilateral Loopback Deactivated  Warning Nx 56/64 Bilateral Loopback Nx BI-LAT Cleared  Warning Nx 56/64 Bilateral Loopback Nx BI-LAT Cleared	
Excessive Zeros condition cleared Warning Nx 56/64 Excessive Zeros Alarm Cleared Nx XS0 AL Cleared Nx S0/64 Excessive Zeros Alarm Nx XS0 AL Cleared Nx S0/64 Bilateral Loopback Nx BI-LAT Activated Warning Nx 56/64 Bilateral Loopback Nx BI-LAT Cleared Nx BI-LAT Cleared Nx BI-LAT Cleared Nx EI-LAT Cleared Nx S0/64 S11 Test Pattern Active Nx TEST F S11 Test Pattern Deactivated Warning Nx 56/64 S11 Test Pattern Nx TEST F Cleared Nx EI-LAT Cleared Nx EI-LAT Cleared Nx EI-LAT Nx TEST F Cleared Nx EI-LAT Cleared Nx EI-LAT Nx TEST F Cleared Nx EI-LAT Nx TEST F Cleared Nx EI-LAT Nx TEST F Cleared Nx EI-LAT Nx	.M-A
Cleared  Bilateral Loopback Activated  Warning Nx 56/64 Bilateral Loopback Active  Nx BI-LAT  Warning Nx 56/64 Bilateral Loopback Deactivated  Warning Nx 56/64 Bilateral Loopback Cleared  Nx BI-LAT  Nx BI-LAT  Nx BI-LAT  Nx BI-LAT  Nx BI-LAT  Nx BI-LAT  Cleared  Nx 56/64 511 Test Pattern Active Nx TEST F  S11 Test Pattern Deactivated  Warning Nx 56/64 511 Test Pattern Cleared  Nx TEST F	
Active  Bilateral Loopback Deactivated  Warning Nx 56/64 Bilateral Loopback Cleared  Nx BI-LAT  S11 Test Pattern Activated  Warning Nx 56/64 511 Test Pattern Active Nx TEST F  S11 Test Pattern Deactivated  Warning Nx 56/64 511 Test Pattern Cleared  Nx TEST F	.M-I
Deactivated Cleared  511 Test Pattern Activated Warning Nx 56/64 511 Test Pattern Active Nx TEST F  511 Test Pattern Warning Nx 56/64 511 Test Pattern Nx TEST F  Deactivated Cleared Cleared	LBK -A
511 Test Pattern Warning Nx 56/64 511 Test Pattern Nx TEST F Deactivated Cleared	LBK -I
Deactivated Cleared	PTRN -A
	PTRN -I
DTR Asserted Information Nx 56/64 DTR Asserted n/a	
DTR Dropped Information Nx 56/64 DTR Dropped n/a	
RTS Asserted Information Nx 56/64 RTS Asserted n/a	
RTS Dropped Information Nx 56/64 RTS Dropped n/a	
DCD Asserted Information Nx 56/64 DCD Asserted n/a	
DCD Dropped Information Nx 56/64 DCD Dropped n/a	
CTS Asserted Information Nx 56/64 CTS Asserted n/a	
CTS Dropped Information Nx 56/64 CTS Dropped n/a	

Table A-4. Source Time

Event	Category	Console Log String	Front Panel Display String
Red Alarm Set	Major	T1 Red Alarm Active	T1 RED ALRM -A
Red Alarm Cleared	Major	T1 Red Alarm Cleared	T1 RED ALRM -I
Yellow Alarm Set	Major	T1 Yellow Alarm Active	T1 YELW ALRM -A
Yellow Alarm Cleared	Major	T1 Yellow Alarm Cleared	T1 YELW ALRM -I
Blue Alarm Set	Major	T1 Blue Alarm Active	T1 BLUE ALRM -A
Blue Alarm Cleared	Major	T1 Blue Alarm Cleared	T1 BLUE ALRM -I
LOS Alarm Set	Major	T1 LOS Active	T1 LOS -A
LOS Alarm Cleared	Major	T1 LOS Cleared	T1 LOS -I
Tx Blue Alarm Set	Major	T1 Tx Blue Alarm Active	T1 TX BLUE -A
Tx Blue Alarm Cleared	Major	T1 Tx Blue Alarm Cleared	T1 TX BLUE -I
Tx Yellow Alarm Set	Major	T1 Tx Yellow Alarm Active	T1 TX YELW -A
Tx Yellow Alarm Cleared	Major	T1 Tx Yellow Alarm Cleared	T1 TX YELW -I
D Channel Alarm Set	Major	T1 D Channel Alarm Active	T1 D CH ALRM -A
D Channel Alarm Cleared	Major	T1 D Channel Alarm Cleared	T1 D CH ALRM -I
Line Loopback Active	Warning	T1 Line Loopback Active	T1 LINE LB -A
Payload Loopback Active	Warning	T1 Payload Loopback Active	T1 PYLD LB -A
Loopback Cleared	Warning	T1 Loopback Cleared	T1 LBK -I
Current T1 Errored Seconds Threshold Exceeded	Warning	T1 Curr ES Thrs Exceeded	T1 CUR ES THRS
Current T1 Severely Errored Seconds Threshold Exceeded	Warning	T1 Curr SES Thrs Exceeded	T1 CUR SES THRS
Current T1 Severely Errored Framing Seconds Threshold Exceeded	Warning	T1 Curr SEFS Thrs Exceeded	T1 CUR SEFS THRS
Current T1 Unavailable Seconds Threshold Exceeded	Warning	T1 Curr UAS Thrs Exceeded	T1 CUR UAS THRS

Table A-4. Source Time (Continued)

Event	Category	Console Log String	Front Panel Display String
Current T1 Controlled Slip Seconds Threshold Exceeded	Warning	T1 Curr CSS Thrs Exceeded	T1 CUR CSS THRS
Current T1 Path Code Violations Threshold Exceeded	Warning	T1 Curr PCV Thrs Exceeded	T1 CUR PCV THRS
Current T1 Line Errored Seconds Threshold Exceeded	Warning	T1 Curr LES Thrs Exceeded	T1 CUR LES THRS
Current T1 Line Code Violations Threshold Exceeded	Warning	T1 Curr LCV Thrs Exceeded	T1 CUR LCV THRS
Total T1 Errored Seconds Threshold Exceeded	Warning	T1 Tot ES Thrs Exceeded	T1 TOT ES THRS
Total T1 Severely Errored Seconds Threshold Exceeded	Warning	T1 Total SES Thrs Exceeded	T1 TOT SES THRS
Total T1 Severely Errored Framing Seconds Threshold Exceeded	Warning	T1 Total SEFS Thrs Exceeded	T1 TOT SEFS THRS
Total T1 Unavailable Seconds Threshold Exceeded	Warning	T1 Total UAS Thrs Exceeded	T1 TOT UAS THRS
Total T1 Controlled Slip Seconds Threshold Exceeded	Warning	T1 Total CSS Thrs Exceeded	T1 TOT CSS THRS
Total T1 Path Code Violations Threshold Exceeded	Warning	T1 Total PCV Thrs Exceeded	T1 TOT PCV THRS
Total T1 Line Errored Seconds Threshold Exceeded	Warning	T1 Total LES Thrs Exceeded	T1 TOT LES THRS
Total T1 Line Code Violations Threshold Exceeded	Warning	T1 Total LCV Thrs Exceeded	T1 TOT LCV THRS

**Table A-5. Source: Ethernet** 

Event	Category	Console Log String	Front Panel Display String
Not enough memory for Ethernet driver	Critical	No memory for driver structure	n/a

Table A-6. Source: ISDN

Event	Category	Console Log String	Front Panel Display String
No BRI resources available	Critical	BRI configuration failed: No ISDN resources are available	NO MORE ISDN AVL
No PRI resources available	Critical	PRI configuration failed: No ISDN resources are available	NO MORE ISDN AVL
Unknown SPID received	Major	BRI LT: SPID <spid> received - NOT IN LIST</spid>	SPID FAILED
SPID Negotiation failed	Major	BRI NT: SPID Negotiations failed - resetting the link	SPIDS FAILED
SPID Failed	Major	BRI NT: Spid <spid> was rejected</spid>	SPID FAILED
D Channel Down	Major	D channel is DOWN	D CHAN DOWN
Incorrectly formatted IE	Major	<message>: Incorrectly formatted cause IE</message>	n/a
SPID Retry in progress	Minor	BRI NT: SPID Negotiations failed - Retrying	SPID RETRY
SPID Unregistration attempted	Warning	LT: Tried to call unregistered SPID <spid></spid>	n/a
No Matching SPID found	Warning	No SPID matches the call profile: <called number=""> <call type=""></call></called>	n/a
No Matching SPID found	Warning	No SPID with free B channels matches call type: <call type=""></call>	n/a
ISDN line released	Normal	Released: No longer an ISDN line	RELEASED
BRI LT configuration successful	Normal	Configured BRI as LT	CONFIG BRI LT
BRI NT configuration successful	Normal	Configured BRI as NT	CONFIG BRI NT
PRI CO configuration successful	Normal	Configured PRI as central office emulator	CONFIG PRI CO

Table A-6. Source: ISDN (Continued)

Table A-0. Source. IoDiv (Continued			
Event	Category	Console Log String	Front Panel Display String
PRI CPE configuration successful	Normal	Configured PRI as CPE	CONFIG PRI CPE
No B channels for call	Normal	No outgoing B channel available for call to <number></number>	n/a
SPID Registration in progress	Normal	BRI LT: Registering SPID <spid></spid>	REGISTER SPID
SPID Registration complete	Normal	BRI LT: All SPIDs registered	SPIDS COMPLETE
SPID registered	Normal	BRI NT: Spid <spid> registered</spid>	SPID REGISTERED
SPID Registration complete	Normal	BRI NT: All SPIDs registered	SPIDS COMPLETE
SPID Registration in progress	Normal	BRI NT Registering SPID <spid></spid>	REGISTER SPID
Call Rejected	Normal	Rejected an incoming call for an unregistered SPID	n/a
D Channel Up	Normal	D channel is UP	D CHAN UP
Dialing number	Information	Dialing <called number=""></called>	n/a
Call not accepted	Information	Call not accepted to <called number="">: No channel available</called>	n/a
Call cleared	Information	Call to <called number=""> cleared from ATLAS end</called>	n/a
Call busy	Information	Call to <called number=""> declared busy after leaving ATLAS</called>	n/a
Call connected	Information	Call to <called number=""> connected</called>	n/a
Call ringing	Information	Call to <called number=""> ringing</called>	n/a
Call busy	Information	Call to <called number=""> refused: Busy</called>	n/a
Call disconnected	Information	Call to <called number=""> disconnected by far end</called>	n/a

Table A-6. Source: ISDN (Continued)

Event	Category	Console Log String	Front Panel Display String
Call received	Information	Call to ATLAS: <called number=""> received</called>	n/a
Incoming call refused	Information	Incoming call to <called number=""> refused</called>	n/a
Incoming call accepted	Information	Incoming call to <called number=""> accepted</called>	n/a

In addition to the above, certain recognized ISDN cause codes are sent to the event log from the ISDN Message facility. The codes applicable to the AT-LAS 800 are shown below along with the minimum category required for logging the cause code event.

**Table A-7. ISDN Cause Codes** 

Cause Code Message	Code	Category
UNASSIGNED_NUMBER	1	Information
NO_ROUTE	2	Information
CHANNEL_UNACCEPTABLE	6	Information
NORMAL_CLEARING	16	Information
USER_BUSY	17	Information
NO_USER_RESPONDING	18	Information
CALL_REJECTED	21	Information
NUMBER_CHANGED	22	Information
DEST_OUT_OF_ORDER	27	Information
INVALID_NUMBER_FORMAT	28	Information
FACILITY_REJECTED	29	Information
RESP_TO_STAT_ENQ	30	Information
UNSPECIFIED_CAUSE	31	Information
NO_CIRCUIT_AVAILABLE	34	Warning
NETWORK_OUT_OF_ORDER	38	Warning
TEMPORARY_FAILURE	41	Warning
NETWORK_CONGESTION	42	Warning
ACCESS_INFO_DISCARDED	43	Warning
REQ_CHANNEL_NOT_AVAIL	44	Warning
PRE_EMPTED	45	Warning
FACILITY_NOT_SUBSCRIBED	50	Minor
OUTGOING_CALL_BARRED	52	Minor
INCOMING_CALL_BARRED	54	Minor
BEAR_CAP_NOT_AVAIL	58	Minor
SERVICE_NOT_AVAIL	63	Minor
CAP_NOT_IMPLEMENTED	65	Major
CHAN_NOT_IMPLEMENTED	66	Major
FACILITY_NOT_IMPLEMENTED	69	Major
INVALID_CALL_REF	81	Major
CHAN_DOES_NOT_EXIST	82	Major

Table A-7. ISDN Cause Codes (Continued)

Cause Code Message	Code	Category
INCOMPATIBLE_DEST	88	Major
INVALID_MSG_UNSPEC	95	Major
MANDATORY_IE_MISSING	96	Major
NONEXISTENT_MSG	97	Major
WRONG_MESSAGE	98	Major
BAD_INFO_ELEM	99	Major
INVALID_ELEM_CONTENTS	100	Major
WRONG_MSG_FOR_STATE	101	Major
TIMER_EXPIRY	102	Major
MANDATORY_IE_LEN_ERR	103	Major
PROTOCOL_ERROR	111	Major
INTERWORKING_UNSPEC	127	Major

Cause Code IEs that are non-Q.931 (Coding Standard field is not 0) are logged with the following format:

<message> : <coding standard> code <cause code>

The coding standard field is one of:

- Reserved
- National
- Local

Each Cause Code IE log entry will end with a location designation. These designations are shown below:

Table A-8. Cause Code Log Entries

Code	Location
U	User
LPN	Private network serving the local user
LN	Public network serving the local user
TN	Transit network
RLN	Public network serving the remote user
RPN	Private network serving the remote user
INTL	International network
INWK	Network beyond internetworking point

Table A-9. Source: ISDN L2 Messages

Event	Category	Console Log String	Front Panel Display String
ISDN Layer 2 (LAPD) Message. Provides a hex dump of the entire LAPD frame	Information	<message contents=""></message>	n/a

Table A-10. Source: ISDN Call Control Messages

Event	Category	Console Log String	Front Panel Display String
ISDN Call Control Messages	Information	Host>>CC <tag> <call id=""> <message></message></call></tag>	n/a
ISDN Call Control Messages	Information	CC>>Host <tag> <call id=""> <message></message></call></tag>	n/a

**Table A-11. Source: ISDN Information Elements** 

Event	Category	Console Log String	Front Panel Display String
ISDN Information Elements. Provides a hex dump of the ISDN IE sent with a call control message	Information	<message contents&gt;</message 	n/a

# Appendix B Troubleshooting



# **Power-up Self Test Fails**

# Modules seated improperly, module failure

Remove all modules and cycle power to the unit. If self test still fails, call Technical Support and report the results. If the self test now passes, re-insert modules one at a time, running the self test after installing each module. When an installed module causes the self test to fail, note it and report results to tech support.



# **System Timing Source Unlocked**

(Displayed on Terminal Interface, "System Status")

# Selected Timing Source is not present or clock is out of tolerance

- Verify that system timing is correctly configured for the desired clock.
- Verify that the interface cable to clock source is present.
- Temporarily configure the system to operate off of internal timing. Verify that the system can lock to this clock.



# Cannot pass data from T1 interface to V.35 port

## Misconfiguration, improper cabling

- Verify that the T1 signal is being received. If not, check that the cabling is correct.
- Verify that the T1 is being received without errors. If not, double-check that framing and coding are set properly.
- Verify that desired dedicated map is active.
- Verify that bandwidth is mapped to the correct V.35 port.
- Verify that the V.35 port is set to the correct data rate (terminal interface).
- Check T1 performance using the terminal interface; if excessive errors, report fault to the Telco.
- Verify proper state of DTE signals via the terminal interface or the LCD front panel.



# Switched calls are not working

# Misconfiguration

Verify that the end point has proper call accept/reject criteria. For RBS
applications, check signaling bit status on the terminal interface for
proper operation.

Verify that the end point is set up for correct signaling.



# Cannot communicate with ATLAS USING VT-100 connected to the Control/Chain In Port

#### Misconfiguration, improper cabling

- Verify that ATLAS is receiving commands (press keys on terminal and verify that the received byte count in the front panel increments).
- Check cabling, verify that the chain port rate matches that of the attached terminal; check chain port status leads on the front panel.



# **Cannot establish Telnet session with ATLAS**

# Max Telnet sessions set to 0, IP address of ATLAS does not match remote host IP address

- Verify that the ethernet connection is in place, check IP addresses programmed in ATLAS and in the Telnet client, verify that session timeout value is not set too low.
- Check for ethernet port activity on the front panel. Make sure the link is up, and data is being transmitted and received.

# Appendix C Warranty and Technical Support Information

# WARRANTY AND CUSTOMER SERVICE

ADTRAN will replace or repair this product within five years from the date of shipment if the product does not meet its published specifications or if it fails while in service. For detailed warranty, repair, and return information refer to the ADTRAN Equipment Warranty and Repair and Return Policy Procedure.

Return Material Authorization (RMA) is required prior to returning equipment to ADTRAN.

For Service, RMA requests, or more information, see the following sections for the correct toll-free contact number.

# PRODUCT SUPPORT INFORMATION

# **Pre-sales Inquiries and Applications Support**

Please contact your local distributor, ADTRAN Applications Engineering, or ADTRAN Sales:

Applications Engineering (800) 615-1176 Sales (800) 827-0807

# Post-Sale Support

Please contact your local distributor first. If your local distributor cannot help, please contact ADTRAN Technical Support and have the unit serial number available.

Technical Support (888) 4ADTRAN

# **Repair and Return**

If ADTRAN Technical Support determines that a repair is needed, Technical Support will coordinate with the Customer and Product Service (CAPS) department to issue an RMA number. For information regarding equipment currently in house or possible fees associated with repair, contact CAPS directly at the following number:

CAPS Department (256) 963-8722

Identify the RMA number clearly on the package (below address), and return to the following address:

ADTRAN, Inc. 6767 Old Madison Pike Progress Center Building #6 Suite 690 Huntsville, Alabama 35807

RMA # \_\_\_\_\_

# Appendix D Acronyms and Abbreviations

**AMI** alternate mark inversion

ANI automatic number identification

B8ZS bipolar eight zero substitution

BRI Basic Rate ISDNbps bits per second

**CPE** customer premise equipment

**CSU** channel service unit

CTS Clear to send

DACS Digital Access Cross-Connect System
 DCE data communications equipment
 DNIS dialed number identification service
 DS0 digital service, level 0 (64 kbps)

**DSU** data service unit

DTEdata terminal equipmentDTMFdual tone multifrequencyESFextended superframeFTPFile Transfer Protocol

**ISDN** Integrated Services Digital Network.

kbpskilobits per secondLANlocal area networkLCDliquid crystal displayLEDlight emitting diodeMbpsMega bits per second.

**MIB** management information base

NT1 network termination 1PBX private branch exchange

**PRI** Primary Rate ISDN

**PSTN** public switched telephone network

**SNMP** simple network management protocol

**RBS** robbed bit signaling

TCP/IP Transmission Control Protocol/Internet Protocol

TDM time division multiplexing
TFTP Trivial File Transfer Protocol

TSU terminal service unit
WAN wide area network

# Appendix E Glossary

#### 10BaseT Ethernet connection

The ATLAS 800 RJ-48C port that provides Ethernet LAN connection for TFTP, SNMP, and Telnet.

#### **AMI**

alternate mark inversion. A Layer 1 line code used in a T1 carrier. Zeros are transmitted as zero volts, and ones are transmitted as pulses that alternate polarity. Although B8ZS is an enhancement to AMI, B8ZS and AMI are normally referred to as mutually-exclusive options for a T1. (See also *B8ZS*.)

#### **ANI**

Automatic Number Identification. Service provided by a local phone company that provides incoming Caller ID information.

#### Async-232 Module

One of the ATLAS 800 option modules. The Aysnc-232 provides sixteen asynchronous EIA-232 DTE ports and serves as an interface between terminal servers and other DTE equipment.

#### **ATLAS 800**

A bandwidth management system which functions as a central site multiplexer. (See also *Integrated Access System.*)

#### **B87.**S

bipolar eight zero substitution. In a T1 carrier system, a specific eight bit pattern containing two deliberate bipolar violations which replaces eight consecutive customer zero bits. (See also 10BaseT Ethernet connection.)

#### **B** channel

bearer channel. Bearer channels of an ISDN service carry provide data transmission. Compare with D channel.

#### bandwidth

The transmission capacity of a communications channel, stated in megabits per second (Mbps).

#### **Basic Rate ISDN**

See BRI.

#### bit

Bit is a contraction of the term binary digit. It is the smallest unit of information a computer can process representing either high or low, yes or no, or 1 or 0. It is the basic unit in data communications. A bit can have a value of zero (a mark) or one (a space).

#### bps

Bits per second. A measure of the speed of data communications.

#### **b**yte

Eight bits of information composed of zeros or ones, one of which may include a parity bit.

#### BRI

Basic Rate ISDN. An ISDN service that offers two bearer (B) channels. One channel (64 kbps) is used for data transfer and as a data-link. The second channel (16 kbps) is used for signaling and control information.

#### clocking

An oscillator-generated signal that provides a timing reference for a transmission link. A clock provides signals used in a transmission system to control the timing of certain functions. The clock has two functions, (1) to generate periodic signals for synchronization and (2) to provide a time base.

#### **CPE**

Customer premise equipment. All telecommunications terminal equipment located on the customer premises, including telephone sets, private branch exchanges (PBXs), data terminals, and customerowned coin-operated telephones.

#### **CSU**

channel service unit. A device that functions similarly to a modem except that the CSU works with digital signals rather than analog signaling.

#### CS

See CTS.

#### CTS

Clear to send. A signal on the DTE interface indicating that the DCE is clear to send data.

#### **DACS**

Digital Access Cross-Connect System. A system, such as the ATLAS 800, that assigns and redistributes (grooms) any DS0 on any T1 circuit to any other DS0 on any other T1 circuit in the system.

#### DCE

Data communications equipment. The part of a computer or data terminal that connects to a communications channel or network.

#### D channel

delta channel. Controls the operation of the ISDN connection.

#### dedicated bandwidth

Bandwidth which has been set aside (dedicated) for a specific number.

#### Dial plan

The numbering plan for ATLAS ports (user and network) handling switched connections. Individual dial plans contain phone number and features associated with DTMF dialing, PRI and BRI.

#### **Digital Access Cross-Connect System**

See DACS.

#### DNIS

Dialed Number Identification Service. Service provided by a telephone company that allows the caller to see what number has been dialed.

#### DS0

Digital signal (or service) having a transmission rate of 64 kbps intended to carry one voice channel (a phone call). Also called a fractional T1 because it bridges the gap between 56-kbps direct dial service (DDS) and a full T1 implementation (24 channels).

#### **DSU**

data service unit. A device used with a CSU to support digital communications by converting signals. (See also CSU.)

#### DTE

Data terminal equipment. The portion of a data terminal that interfaces to the end-user's equipment. The main difference between DCE and DTE is that pins 2 and 3 are reversed on the EIA-232.

#### DTMF dialing

dual tone multifrequency dialing. The tones used by customer equipment to signal the network.

#### E1 circuit

European equivalent to the T-1.

#### **ESF**

extended superframe. A method of grouping T1 carrier frames into larger superframes, each containing 24 consecutive T1 frames.

#### flash memory

A kind of non-volatile storage device, similar to EEPROM, where erasing can only be done in blocks or the entire chip.

#### flash upgrades

Upgrades that can be downloaded into the flash memory.

#### FTP

File Transfer Protocol. The TCP/IP protocol used to log in to a network, list files and directories, and transfer files.

#### hot swappable

A device is hot swappable if it can be installed without powering down the main unit.

#### **Integrated Access System**

A chassis-based product that supports a number of end-user applications on the subscriber side and a number of carrier interfaces on the trunk side. The ATLAS 800 is an Integrated Access System designed to provide significant wide-area cost savings through the consolidation of voice, data, fax, and video.

#### **ISDN**

Integrated Services Digital Network. A network architecture that enables end-to-end digital connections. The network supports diverse services through integrated access arrangements and defines a limited set of standard, multipurpose interfaces for equipment vendors, network providers, and customers. Interworking with a public switched telephone network is retained.

#### **kbps**

Kilobits per second. 1,000 bits per second.

#### I.AN

local area network. Group of computers and peripheral devices connected by a communications channel, limited by distance.

#### LCD

liquid crystal display. Alphanumeric characters that appear in a display area as a result of light reflecting off a special crystalline substance.

#### leased line

A telecommunication facility or link reserved for the exclusive use of one customer. Also called a dedicated line.

## local loop

In telephony the wire pair that connects a subscriber to a phone company end office, typically containing two wires. Four-wire local loops are common, however, especially with leased voice grade circuits.

## loopback

A diagnostic procedure where data is sent to the device being tested, and the output of the device is fed directly back to its input, looped around, and the returning data is checked against that which was sent.

#### LED

light emitting diode. Alphanumeric characters that glow when supplied with a specified voltage.

## **Mbps**

Mega bits per second. A measure of the amount of information travelling across a network or communications link.

#### **MIB**

management information base. The MIB is an index to the organized data stored within a network device.

#### **Modem 16 Module**

One of the ATLAS 800 option modules. The Modem 16 Module supports sixteen 56Kflex modem (analog) calls or sixteen ISDN connections.

#### multiplexer

(mux) A device that takes several low-speed channels and merges them into one high-speed channel at one end of a link. Another multiplexer at the other end of the link reverses this process.

#### NT1

Network termination 1. A unit that provides physical and electromagnetic termination of the U-interface, 2-wire transmission line; converts between Layer 1 formats used at the U- and T- reference points; and performs some maintenance functions.

#### nonvolatile memory

Any form of memory that retains its contents when power is removed (for example, ROM, EPROM, etc.)

#### Octal BRI/U Module

One of the ATLAS 800 option modules. The Octal BRI/U Module provides eight basic rate ISDN U interfaces, each capable of operating in NT or LT mode.

#### option modules

Any optional, hot-swappable module that can be added to the ATLAS 800 system for a variety of applications. See also

#### **overbooking**

ATLAS 800 feature that reduces telecommunications expenses by allowing you to over-subscribe switched bandwidth for situations where simultaneous access to the network by every subscriber is not required.

#### **PBX**

private branch exchange. A telephone system usually owned by the customer that serves a particular location. It provides connections from one phone extension to another and connects to the external telephone network.

#### PRI

Primary Rate ISDN. An ISDN service that provides 23 B (bearer) channels (64 kbps each) and 1 D (data) channel (64 kpbs). The combined capacities are equivalent to one T1 channel.

#### Quad Nx56/64 Module

(Nx is pronounced "en-by.") One of the ATLAS 800 option modules. The Quad Nx56/64 Module provides four synchronous V.35 DTE ports, each of which can operate at any rate that is a multiple of 56 or 64 kbps, up to 1.536 Mbps.

#### Quad T1/PRI Module

One of the ATLAS 800 option modules. The Quad T1/PRI Module provides four channelized T1 or Primary Rate ISDN (PRI) interfaces. Each interface can operate independently in DS-1 or DSX-1 mode, and any port can serve as the primary or backup timing source for the entire system.

#### Remote Access

The ability to connect to non-local communications equipment.

## robbed bit signaling

A type of in-band signaling used with voice transmissions for multiplexing multiple voice circuits onto a T1.

## **SNMP**

Simple Network Management Protocol. A control and reporting scheme widely used to manage devices from different vendors. SNMP operates on top of the Internet protocol.

#### synchronous

1. The condition occurring when two events happen in a specific time relationship with each other, both under control of a master clock.

2 A method of data transmission requiring the transmission of timing pulses to keep the sender and receiver synchronized in their communication used to send blocks of information. Synchronous data transmission is used in high speed data circuits because there is less overhead than asynchronous transmission of characters which contain two extra bits per character to affect timing.

#### T1 circuit

Also T-1. A digital transmission link with a capacity of 1.544 Mbps. T1 uses two pairs of normal twisted wires. T1 normally can handle 24 voice conversations with each conversation being digitized at 64 kbps. With more advanced digital voice encoding techniques, it can handle more voice channels. T1 is a standard for digital transmission in North America.

#### T3 Module

One of the ATLAS 800 option modules. The T3 Module provides one or two channelized T3 interfaces.

#### TCP/IP

Transmission Control Protocol/Internet Protocol. A set of communications protocols that encompasses media access, packet transport, session communications, file transfer, electronic mail, and terminal emulation.

#### **TDM**

Time Division Multiplexing. A method for sending two or more signals over a common transmission path by assignment the path sequentially to each signal, each assignment being for a discrete time interval.

#### Telco

Telephone company.

#### Telnet

A terminal emulation protocol, part of the TCP/IP suite of protocols, that provides remote terminal-connection services. (See also *VT-100*.)

#### TFTP

Trivial File Transfer Protocol. A simplified version of the TCP/IP file transfer protocol that does not include password protection or user-directory capability.

#### trunk

A direct line between two telephone switching centers.

#### TSU

terminal service unit.

#### T-Watch PRO

The ADTRAN Microsoft Widows-based management software program designed to control TSU units from a remote PC. It also provides limited control over the configuration of the ATLAS 800 using a graphical user interface.

#### VT-100

A non-intelligent terminal or terminal emulation mode used for a synchronous communications. Used to configure the ADTRAN ATLAS  $800^{PLUS}$ .

#### WAN

wide area network. A network that connects users across large distances.

#### **XMODEM**

An error-correcting file transfer, data transmission protocol used to transmit files between PCs. The XMODEM protocol sends information in 128 byte blocks of data. Some sums (check sums) are done on each block and the result is sent along with the block. If the result does not check out at the other end, the computer at the other end sends a request (a NAK - negative acknowledgment) to retransmit that block again). If the block checks out, the computer sends ACK (an acknowledgment). In this way, relatively error-free transmissions can be accomplished.

# Index

Symbols	alarm menus 4-2
#8-3	alarms
	active 4-11
Numerics	DS0 7-4
10-BaseT	module 7-2
connection 2-7	view log 6-4
pinout 2-7	all
port 2-3	ones 7-7
status 6-5	zeros 7-7
15 minutes	alrm menu 4-11
performance 7-5	AMI 2-6
24 hour	analog
performance 7-5	accept 10-4, 10-7
1	reject 10-5
A	applications engineering C-1
abort 13-11	area code 10-8
accept numbers 10-4, 10-6	arrow keys 4-2
access	arrows 4-1, 4-4
passwords 6-11	assign dedicated connections 6-1
access rights 6-11	AT&T 4ESS 10-9
activate	ATLAS 800 PLUS
dedicated map 8-2	configuring 6-1
front panel 4-2	general system information 6-1
time 8-5	grounding instructions 2-2
activating operation keys 4-2	installing 2-1
active alarm 4-11	operating 3-1
add password 6-11	shipping contents 2-1
address	system status 6-1
ADLP 6-7	audio
ADLP address 6-7	reject 10-7
ADTRAN	authenticate trap transmission 6-9
utilities 13-1	auto daylight savings 6-10
ADTRAN data link layer protocol address 6-7	auto repeat 13-7, 13-9
alarm	auto TX yellow alarm 7-6
blue 7-4	automatic
red 7-4	routeback rejection 10-9
status 7-3	available DS0s 10-12, 10-16
system 6-5	_
yellow 7-4, 7-6	В
yellow auto TX 7-6	B8ZS 2-6
alarm key 4-1, 4-4	Backup Criteria 9-3
alarm log	Backup Delay 9-3
view 4-12	backup status 9-6
alarm menu 4-11	FB 9-5, 9-6

FR 9-5, 9-6	clear
primary 9-6	performance data 7-5
backup timing source 6-7	selftest log 6-18
bantam test jack 2-3	system event log 6-4
baud rt 4-8	system LED 6-5
begin firmware update 6-15	test pattern 7-7
BES 7-5	clear history 4-12
blinking green module status LED 4-3	clear key 4-1, 4-4
blinking green system LED 4-3	clear log 13-11
blinking red module status LED 4-3	clearing fields 4-2
blinking red system LED 4-3	clock 6-10
blue alarm 7-4	CLR 7-5
BONDING Config 6-12	code 7-6
bonding configuration 6-12	colors 13-7, 13-9
boot ROM rev 6-3	community
bootROM 6-18	trap destination 6-10
bursty errored seconds 7-5	completed network map 10-27
builty offorea becomes ? o	completed user map 10-28
С	config 4-7
Call Stagger 6-13	config menu
call stagger values 6-13	ethernet configuration 4-8
call type 10-18	S0 system 4-7
called digits transferred 10-10, 10-15	S1-S8 4-9
caller ID number 10-17	config transfer 6-16
cancel 4-1, 4-4	configuration
menu 4-5	from port 8-3
capture 13-7, 13-9	get from TFTP server 13-13
category 6-4	interface 10-7
logging A-1	load 6-17
chain in 2-4	module 7-5
pinout 2-5	Quad T1/PRI interface 10-9
chain out 2-3, 2-5	save to server 6-17
pinout 2-5	save to Server 0-17 save to TFTP server 13-12
chain port	use 6-17
-	configuration file
configure 6-8	9
framing errs 6-7 overrun errs 6-7	get from server 6-16 send to server 6-16
Rx bytes 6-7 signal leads 6-6	configuration menu 4-7
status menu 4-7	configure 6-8
Tx bytes 6-7	chain port 6-8 configure
chain port configuration 4-8	<u>e</u>
chain-in port 2-3	port type 6-9 default gateway 6-8
•	ethernet port 6-8
chain-out port 2-3 challenge # 4-11	ethernet port name 6-8
circuit status 6-1	event logging 6-10
	flow control 6-9
backup status 9-6	IP address 6-8
delay 9-6	module slots 7-2
from 9-5 line status 9-6	subnet mask 6-8
	configuring ATLAS 800 PLUS 6-1
man 9-5	configuring Syslog 6-10
test 9-7	connect
Circuit Status Menu 9-5	Telnet menu 13-6
COLOUR STATUS TURBUT 9-1	

connection	accept 10-4, 10-7
activate 8-2	reject 10-5, 10-7
control in / chain in 2-4	data field, described 4-5
create/edit 8-2	data tables 6-5, 6-6
current 8-2	configuring 6-6
dedicated 7-6	date 4-9
ethernet 10BaseT 2-7	current 6-10
from 8-3	restart schedule 6-15
LAN 2-7	restart system 6-14
name 8-2	set 6-3
network 2-6	daylight savings 6-10
power 2-1	DCD
connections 2-3	chain port status 4-7
connects 8-2	data carrier detect 6-6
contents of shipment 2-1	D-chan 7-4
control in 2-4	dedicate map
pinout 2-5	create/edit 8-2
control out 2-5	DS0 available 8-3
controlled slip seconds 7-5	Dedicated 1-3
controller	dedicated and switched connection maps
revision 6-3	description 1-3
controller board slots 7-1	Dedicated Circuit Dial Backup Setup 9-1
controller info 7-3	dedicated map 7-6
control-Z 5-3	activate 8-2
create	activate time 8-5
dedicate map 8-2	creating 8-6
creating	current 8-2
dedicated map 8-6	DS0 selection 8-3
dial plan 10-21	enter connections 8-2
CSS 7-5	from connection 8-3
CSU status LED 4-1, 4-3	insert connection 8-3
CTS	map name 8-2
chain port status 4-7	module configuration 8-8
clear to send 6-6	number of connections 8-3
current	overview example 8-6
dedicate map 8-2	dedicated maps menu 8-1
performance 7-5	def gateway 4-8
current date/time 6-10	default
current time/data 6-3	password 6-11
current transfer status 6-16	default gateway
current update status 6-15	configure 6-8
customer service C-1	define
customer service e-1	passwords 6-11
D	define IP address 3-3
D channel sync 7-4	delete
D4 2-6	alarm history 4-12
DACS	event log 6-4
	password 6-11
description 1-4 data	selftest log 6-18
	delete password 6-11
56 kbps	description of event 6-4
accept 10-7 56 kpbs	dial backup 9-1
reject 10-7	dial call as 10-18
64 kbps	dial plan 7-6, 8-5

complete 10-27	wink 10-12, 10-16
creating 10-21	edit
implementing 10-25	dedicated map 8-2
network terminations 10-3	entry (Telnet utility) 13-6
plan 10-23	editing front panel data fields 4-5
provision network 10-23	empty module slot 7-3
remote access setup 10-22	enable
sample network terminations 10-24	TFTP 13-11
sample user termination 10-25	enable day 8-5
signaling 10-3	Enable Schedule 9-4
slot/port 10-3	enbl day 8-5
video conferencing setup 10-22	end of number timeout 10-8
dial plan menus 10-1	enter
DID 10-13, 10-16	dedicated map connections 8-2
digits transferred 10-13, 10-16	enter key 4-1
prefix 10-13, 10-16	entry
digital access cross-connect system (DACS) 1-4	edit (Telnet utility) 13-6
direct inward dialing 10-13, 10-16	erase
disable 13-11	alarm history 4-12
disconnect 13-6	event log 6-Å
display	selftest log 6-18
event log 6-10	errored seconds 7-5
download	ES 7-5
configuration file 6-16	ESF 2-6
firmware 6-13	ethernet
DRAM 4-11, 6-18	10BaseT connection 2-7
installed 6-3	configuration
DS0	config menu 4-8
alarms 7-4	connection 2-7
available 8-3, 10-12, 10-16	pinout 2-7
first 10-12, 10-16	port 6-5, 6-8
number of 10-12, 10-16	configure 6-8
selection 8-3	status
status 7-4	status menu 4-7
usage 7-4	
DS0 signaling 7-4	event
DS0 status	description 6-4
* 7-4	log A-1
A 7-4	logging 6-10
D 7-4	severity 6-4 slot of event 6-4
M 7-4	types 6-10
N 7-4	J 1
O 7-4	event log 6-4 clear 6-4
R 7-4	
DS0s, number of 10-10	view 4-12
DSP RAM 4-11, 6-18	event logging 4-11
DTE cable 2-1	configure 6-10
DTR	exit
chain port signal leads 6-6	menu 4-5
chain port status 4-7	exiting front panel menu fields 4-5
-	F
E	<del>-</del>
E&M	failure messages 13-1 filename
immediate 10-12, 10-16	menanie

TFTP server 6-14, 6-16	module status LEDs 4-2
firmware	navigating 4-5
begin update 6-15	navigation example 3-2
revision 6-3	numeric keypad 4-2
update 6-13	online status 4-2
begin 6-15	operation 4-1
module slot 6-14	operation keys 4-4
restart schedule 6-14	return to main menu 4-4
TFTP 6-14, 11-1, 11-4 XMODEM 6-14, 11-1	selecting menus 4-5
updating 11-1	shift 4-2
first DS0 10-9, 10-12, 10-14	shift key 4-4
flash 6-18	structure 4-1
flash memory installed 6-3	system LED 4-2
flashing red CSU LED 4-3	system LED light
flow control 4-8	green (fast blink) 4-3
configure 6-9	green (solid) 4-3
Force Mode 9-3	red (fast blink) 4-3
forget password 4-11	red (solid) 4-3
frame 7-5	yellow 4-3 test status 4-2
frame relay	using 4-1
description 1-2	doing 11
framing errors 6-7	G
from	general system information 6-1
configuration 8-3	get
from slot 8-3	configuration file 6-16
front panel	configuration from TFTP server 13-13
access active alarm display menus 4-4	global parameters 10-8
activating 4-2	global switch parameters 10-1
alarm 4-2	green CSU LED 4-3
arrow keys 4-2	green module status LED 4-3
cancel 4-2	ground start 10-16
clear 4-2	grounding 2-2
clear data 4-4	grounding instructions 2-2
CSU LED light	8 8
flashing red 4-3	Н
green 4-3	hardware revision 7-3
red 4-3	help 5-5, C-1
yellow 4-3	history
CSU status LEDs 4-2	clear 4-12
editing data fields 4-5 enter 4-2	view 4-12
	home 4-1
exiting fields 4-5 home 4-2	home key 4-4
	<i>y</i>
layout 3-1, 4-1 LCD window 4-2	1
	I/F status 6-5
main menu 4-5 main menu tree 4-6	ID number 10-11, 10-15, 10-21
menu structure 4-4	ID presentation 10-11, 10-15, 10-21
menu structure 4-4 module slot numbers 4-2	in#accept 10-6
module status 4-2	incrementing fields 5-5
	information
module status LED light	controller 7-3
blinking green 4-3 blinking red 4-3	initialization 2-8
green 4-3	initialize
red 4-3	modem 6-9

insert	LES 7-5
dedicated map connection 8-3	levels
insert password 6-11	password 6-11
Installation 2-1	line build out 7-6
installed memory 6-3	line code 7-6
installing	line code violaions 7-5
ATLAS 800 PLUS 2-1	line errored seconds 7-5
modules 2-8	line status 9-6
interface	active 9-6
configuration	inactive 9-6
Quad T1/PRI 10-9	unknown 9-6
Interface Configuration 9-3	LNK
interface configuration 10-7	ethernet status 4-7
Introduction 1-1	load configuration 6-17
IP	Loc LB 7-6
status (Telnet utility) 13-7	local echo 13-7, 13-9
IP address	local loopback 7-6
configure 6-8	modules 7-6
TFTP server 6-14, 6-16	LOFC 7-5
IP adress	log
SNMP 6-9	clear events 6-4
ISDN access switch	clear selftest 6-18
description 1-5	failure messages 6-4
	field (Telnet utility) 13-12
K	system events 6-10
keyboard keys 5-3	view selftest 6-17
keypad 4-4	warnings 6-4
	log out of a session 5-4
L	loop start 10-16
label	loopback
password 6-11	local 7-6
LAN	modules 7-6
connection 2-7	remote 7-7
Last Run Time 9-7	loopback accept 7-6
Last Test Status 9-7	LOS 7-4
layout	loss of frame count 7-5
front panel 3-1, 4-1	loss of signal 7-4
LB accept 7-6	Lucent 5E 10-9
LBO	Octal BRI 10-18, 10-20
line build out 7-6	Quad T1/PRI 10-14
LCD 4-1	
LCD window 4-2	M
LCV 7-5	management via PC 3-5
LED	map
clear system LED 6-5	user map complete 10-28
CSU status 4-1	map name 8-2
module status 4-1	maps
system 4-1	dedicated 7-6
LEDs 4-2	nailed 7-6
CSU status 4-3	max DS0s 10-18
module online 4-3	Max Num DS0s 9-4
module status 4-3	Max Num Redials 9-4
module test 4-3	max telnet session 6-8
system 4-3	memory

installed 6-3	online 7-3
menu	status 7-3
alarm 4-11	test 7-2
configuration 4-7	test pattern 7-7
module 7-2	modules menu 7-1
modules 6-20	MON 2-3, 2-7
path 5-1	MON test jack 2-7
session 13-6	Monitor 2-3
status 4-7	monitor 2-7
submenu 7-3	most significant digits (MSD) 10-10, 10-13, 10-14,
system status 6-3	10-17
system utility 6-13	MSD 10-10, 10-13, 10-14, 10-17
util 4-9	1010, 10 10, 10 11, 10 17
menu structure, front panel 4-4	N
menu tree	nailed
front panel main menu 4-6	maps 7-6
menus	nailed map
circuit status 9-5	activate 8-2
dedicated maps 8-1	create/edit 8-2
dial plan 10-1	current 8-2
modules 7-1	name 8-2
system config 6-7	name
system info 6-2	TFTP server 6-14
system utility 6-13	National ISDN 10-9
method	Octal BRI 10-18, 10-20
signaling 10-12	navigating front panel 4-5
min DS0s 10-18	network
Min Num DS0s 9-4	connection 2-6
modem	management methods 1-3
initialize 6-9	pinouts 2-6
modem initialization string 6-9	specific facility data 10-10, 10-14
module	specific facility voice 10-10, 10-14
configuration 7-5	termination
menu 7-2	
slot 7-1	configuration settings 10-9 Octal BRI 10-18
slot number 4-1	Quad T1/PRI 10-12
state 7-2	Quad T1/PRI configuration 10-9
status LED 4-1	terminations 10-3
type 7-2	network map
update firmware 6-14	complete 10-27
module online LED 4-3	new password 6-11
module settings 6-1	Next Run Time 9-7
module slot	no response 7-3
update firmware 6-14	Northern DMS 100 10-9
module slots	Octal BRI 10-18, 10-20
preconfigure 7-2	Quad T1/PRI 10-14
module status 4-2	NTWK1 2-3, 2-6
module status 4-2 module status LED 4-3	NTWK2 2-3, 2-6
	number
module submenu 7-3	complete template 10-8
module test LED 4-3	of DS0s 10-16
modules	of ports 10-18
alarms 7-2	number of DS0s 10-10, 10-12, 10-14
installing 2-8	number of users currently logged into system 6-
menu options 6-20	

4.0	D
12	Pass
number to dial 10-18	Fail 9-7
number type template 10-8	passcode
numberic keypad 4-2	set 4-11
numbers	password
accept 10-4, 10-6	access 6-11
reject 10-5, 10-7	add new 6-11
numeric keypad 4-4	change 6-11
NVRAM 4-11	default 6-11
Nx 56/64	define 6-11
user termination 10-17	delete 6-11
	front panel 4-11
0	label 6-11
Octal BRI	levels 6-11
network termination 10-18	new 6-11
switch type 10-20	reset 4-11
user termination 10-20	passwords
offline 7-3	adding 6-11
offline/no response 7-3	deleting 6-11
online 7-2, 7-3	path code 7-5
online help 5-5	pattern
online status 4-2	clear 7-7
operating	module test
front panel 4-1	test
terminal menu 5-1, 10-1	pattern (modules) 7-7
VT 100 3-4	pattern clear 7-7
operating ATLAS 800 PLUS 3-1	PC management 3-5
operation 3-1	performance
operation keys 4-4	15 minutes 7-5
operation keys, described 4-4	24 hour 7-5
option slot	current 7-5
arrangement 2-7	performance data
•	clear 7-5
numbering 2-7	performance monitoring 2-6
option slots	pinout
arrangement 2-7	10-BaseT 2-7
Originate/Answer 9-3	
out#rej 10-4, 10-7	chain in 2-5
Outdial Number 9-3	chain out 2-5
Outgoing Call Type 9-3	control in 2-5
Outgoing caller ID 10-20	control in / chain in 2-5
outgoing caller ID 10-11, 10-15	control out / chain out 2-5
outgoing number conversion 10-10	ethernet 2-7
outgoing#accept 10-3	Ethernet 10BaseT 2-7
overrun errors 6-7	network 2-6
overview	PLL status 7-3
	polls
product 1-1	no response 7-3
<b>D</b>	
P	port 6-4
packing list 2-1	10-Base-T 2-3
panel	10-BaseT 2-7
rear 2-3	chain in 2-3, 2-4
parameters	chain out 2-5
global 10-8	control in 2-4
part num 7-3	control out 2-5

dial plan 10-3	RCV 7-5
ethernet 2-7	real time clock 6-10
ethernet status 6-5	rear panel 2-3
name 7-5	reboot system 6-20
configure ethernet port 6-8	receive level 7-4
speed 6-9	red alarm 7-4
port name 7-5	red CSU LED 4-3
port type	red module status LED 4-3
configure chain port 6-9	Redial Timer 9-4
ports	refresh screen 13-9
available	reject numbers 10-5, 10-7
Nx 56/64 10-18	remote access
number of 10-18	setup with dial plan 10-22
power connection 2-1	remote LB 7-7
power up testing 2-8	remote loopback 7-7
preconfigure	repair C-2
module slots 7-2	reset password 4-11
pre-sales support C-1	response # 4-11
previous transfer status 6-16	restart
previous update status 6-15	date and time 6-15
PRI	schedule 6-14
Quad T1/PRI 10-14	schedule after update 6-14
Quad T1/PRI configuration 10-9	system 6-20
PRI switch 10-9	Restore Criteria 9-3
primary search 10-4, 10-7	Restore Dela 9-4
primary timing sources 6-7	restore factory default settings 5-4
print log 13-11	results
privileges	clear 7-7
SNMP 6-9	module test 7-7
PRMs	retrieve
transmit 7-6	configuration from TFTP server 13-13
product	return C-2
overview 1-1	return material authorization C-2
provision network 10-23	returning to main menu 4-2
Prt 7-5	returning to previous menu 4-2
prt 7-4	rev 7-3
PS1 fail 6-5	revision
PS2 fail 6-5	boot ROM 6-3
pulse density enforcer 7-6	controller 6-3
	firmware 6-3
Q	hardware 7-3
QRSS 7-7	software 4-9
QRSS generation 2-6	RMA C-2
QRSS/RLB results 7-7	RMA requests C-1
Quad T1/PRI	robbed bit signaling 8-5
interface configuration 10-9	routeback rejection 10-9
network termination/PRI 10-9	RTC RAM 4-11, 6-18
network termination/RBS 10-12	RTS
user termination/PRI 10-14	chain port signal leads 6-6
user termination/RBS 10-16	chain port status 4-7
	RX
R	ethernet status 4-7
RBS 8-5	Rx
Quad T1/PRI 10-12, 10-16	level 7-4

Rx frames 6-5	signaling dial plan 10-3
<b>S</b>	status 7-4
S0 system	signaling conversion
config menu 4-7	description 1-3
status menu 4-7	signaling method 10-12, 10-16
S1-S8	slot 6-4
config menu 4-9	dial plan 10-3
status menu 4-7	update firmware 6-14
save	slot/port
configuration file 6-17	user termination 10-5
saving	slt 7-1
configuration to TFTP server 13-12	SNMP 6-9
schedule	access 6-9
restart system 6-14	communities 6-9
secondary search 10-4, 10-7	IP address 6-9
security	privileges 6-9
TFTP server 13-13	software rev 4-9
security levels 6-11	solid green system LED 4-3
SEFS 7-5	solid red system LED 4-3
selecting active menu 4-2	sort to/from 8-2
selecting front panel menu items 4-5	Source ID 9-3, 10-19, 10-20
self test	source ID 10-3, 10-6, 10-11, 10-13, 10-15, 10-17
failure messages 13-1	speech
selftest 2-8, 4-10	accept 10-4, 10-7
clear log 6-18	reject 10-5, 10-7
run 4-10, 6-17	SPID list 10-18
system 6-17	Octal BRI 10-20
view log 6-17	start
send	ground 10-16
configuration file 6-16	loop 10-16
serial number 6-3	start telnet session 3-4
service C-1	Start terriet session 3-4 Startup Delay 9-3
SES 7-5	
session	startup mode mode
menu 13-6	
	startup 6-3 state
session timeout 6-8	module 7-2
deta 4.0.6.2.6.10	status
date 4-9, 6-3, 6-10	10-BaseT 6-5
time 4-9, 6-3, 6-10	alarm 7-3
set passcode 4-11	current configuration transfer 6-16
set up passwords 6-11	current firmware update 6-16
setup	current update 6-15
remote access 10-22	DS0 7-4
video conferencing 10-22	ethernet port 6-5
severely errored frame seconds 7-5	field (Telnet utility) 13-12
severely errored seconds 7-5	I/F 6-5
severity level threshold 6-10	menu 4-7
severity of event 6-4	
shift 4-1	modules 7-3 PLL 7-3
shift key 4-4	
sig	previous update 6-15
dial plan 10-3	previous updates 6-16
sig status 7-4	status field, described 4-5

status menu	utility menu 6-13
chain port status 4-7	system LED 4-3
ethernet status 4-7	·
S1-S8 4-7	T
stopping current activity 4-2	T1 bandwidth management
storing	description 1-4
configuration on TFTP server 13-12	T1/PRI interface ports 7-1
Strip MSD 10-19, 10-20	TANULL Timer 6-12
strip MSD 10-10, 10-13, 10-14, 10-17	TCID Timer 6-13
structure	TDM MAP 4-11
front panel 4-1	TDM RAM 6-18
terminal menu 5-1, 10-1	technical support C-1
submenu	telnet 3-3
menu 7-3	define IP address 3-3
modules 7-3	maximum sessions 6-8
subnet mask	start session 3-4
config menu 4-8	temp fail 6-5
configure 6-8	template
support C-1	number complete 10-8
post-sales C-1	number type 10-8
pre-sales C-1	terminal emulation 3-4
swap ANI/DNIS 10-11, 10-15	terminal menu 5-5
switch parameters 10-1	copy items to clipboard 5-4
switch type 10-9	decrementing fields 5-5
Octal BRI 10-18, 10-20	delete list item 5-5
Quad T1/PRI 10-14	extended help 5-3
switched call parameters 6-1	help 5-5
Syslog	insert new list item 5-5
host facility 6-10	invalidate the password entry 5-4
IP address 6-10	log out of a session 5-4
setup 6-10	menu path 5-1
transmission 6-10	moving around in 5-2
system	navigating with the keyboard keys 5-3
alarm 6-5	navigation help 5-3
config 6-7	operation 5-1, 10-1
configuration menu 6-7	paste items from clipboard 5-4, 5-5
contact 6-3	port status 5-3
event log	refresh the screen 5-4
clear 6-4	restore factory default settings 5-4
event logging 6-10, A-1	right pane notation 5-2
info menu 6-2	structure 5-1, 10-1
information 6-2	Sys 5-3
LED 4-1	system time 5-3
clear 6-5	tool tip 5-3
location 6-3	termination
name 6-3	network
resource usage 6-5	Octal BRI 10-18
restart 6-20	user
selftest 6-17	Octal BRI 10-20
status 6-1, 6-3	terminations
status menu 6-3	user 10-5
timing sources 6-5	test 7-7
uptime 6-3	modules 7-2
utility 6-13	self 2-8

Test Call 9-4	number 10-13
test jack 2-7	trunk conditioning 8-4
MON 2-7	trunk usage 6-6
Test Now 9-7	T-Watch PRO 3-5
test pattern 7-7	TX
error inject 7-7	ethernet status 4-7
test status 4-2	Tx frames 6-5
testing	Tx PRMs 7-6
power up 2-8	Tx yellow alarm
TFTP	enable/disable 7-6
delivered utility 13-10	TXADD01 Timer 6-12
save configuration file 6-17	TXDEQ Timer 6-12
security 13-13	TXFA Timer 6-12
server filename 6-14, 6-16	TXINIT Timer 6-12
server IP address 6-14, 6-16	type
update firmware 6-13, 6-14, 11-1, 11-4	module 7-2
time	
current 6-10	U
restart schedule 6-15	UAS 7-5
restart system 6-14	unavailable seconds 7-5
set 6-3	up and down arrows 4-1, 4-4
time event log/time 6-4	update
time/date 4-9	current status 6-15
timeout	firmware 6-13
end of number 10-8	module slot 6-14
terminal session 6-8	restart schedule 6-14
timing source	TFTP 11-1, 11-4
backup 6-7	XMODEM 11-1
primary 6-7	previous status 6-15
timing sources 6-5	update status 6-16
tips for troubleshooting B-1	updating
to clipboard 13-11	firmware 11-1
To Config 8-5	upload
to printer 13-11	configuration file 6-16
TO slot 8-3	uptime
transfer	system 6-3
	usage
configuration file 6-16 current status 6-16	DS0 7-4
method 6-16	use configuration 6-17
	user
previous status 6-16 transfer method	map completed 10-28
update firmware 6-14	termination
transmit PRMs 7-6	configuration settings 10-9
	Nx 56/64 10-17 Octal BRI 10-20
trap destination 6-10	Quad T1/PRI 10-14, 10-16
	terminations 10-5
community 6-10 filtering 6-10	users logged into system, number of 6-12
trap transmission 6-9	using operation keys 4-4
authenticate 6-9	using the front panel 4-1
treat call as	util menu 4-9
accept 10-4	utilities 13-1
reject 10-5	utility
troubleshooting B-1	TFTP server 13-10
trunk	VT 100 13-8
uuuu	

view log 6-4
warranty C-1
window
LCD 4-1
writing
configuration to TFTP server 13-12
X
XMODEM
update firmware 6-13, 6-14, 11-1
-
Υ
yellow alarm 7-4
auto TX 7-6
enable/disable 7-6
yellow CSU LED 4-3
yellow system LED 4-3

# **Product Support Information**

## **Presales Inquiries and Applications Support**

Please contact your local distributor, ADTRAN Applications Engineering, or ADTRAN Sales:

Applications Engineering (800) 615-1176 Sales (800) 827-0807

## **Post-Sale Support**

Please contact your local distributor first. If your local distributor cannot help, please contact ADTRAN Technical Support and have the unit serial number available.

Technical Support (888) 4ADTRAN

#### **Repair and Return**

If ADTRAN Technical Support determines that a repair is needed, Technical Support will coordinate with the Custom and Product Service (CAPS) department to issue an RMA number. For information regarding equipment currently in house or possible fees associated with repair, contact CAPS directly at the following number:

CAPS Department (256) 963-8722

Identify the RMA number clearly on the package (below address), and return to the following address:

ADTRAN Customer and Product Service 6767 Old Madison Pike Building #6 Suite 690 Huntsville, Alabama 35807

RMA #
-------