You'll be entered into a quarterly drawing for **free** Cisco Press books by returning this survey! Cisco is dedicated to customer satisfaction and would like to hear your thoughts on these printed manuals. Please visit the Cisco Product Comments on-line survey at **www.cisco.com/go/crc** to submit your comments about accessing Cisco technical manuals. Thank you for your time.

General Information

1 Years of networking experience: ________ Years of experience with Cisco products: ________

2 I have these network types: ___ LAN ___ Backbone ___ WAN
___ Other: ________

3 I have these Cisco products: ___ Switches ___ Routers
___ Other (specify models): ________

4 I perform these types of tasks: ___ H/W installation and/or maintenance ___ S/W configuration
___ Network management ___Other: ________

5 I use these types of documentation: ___ H/W installation ___ H/W configuration ___ S/W configuration
___ Command reference ___ Quick reference ___ Release notes ___ Online help
___ Other: ________

6 I access this information through: ___ % Cisco.com ___ % CD-ROM ___ % Printed manuals
___ % Other: ________

7 I prefer this access method: ___ Cisco.com ___ CD-ROM ___ Printed manuals
___ Other: ________

8 I use the following three product features the most: ________

Document Information

Document Title: Catalyst 6500 Series Switch Command Reference

Part Number: OL-8977-01 S/W Release (if applicable): 8.6

On a scale of 1–5 (5 being the best), please let us know how we rate in the following areas:

___ The document is complete. ___ The information is accurate.

___ The information is well organized. ___ The information I wanted was easy to find.

___ The document is written at my technical level of understanding. ___ The information I found was useful to my job.

Please comment on our lowest scores: ________

Mailing Information

Organization Date

Contact Name

Mailing Address

City State/Province Zip/Postal Code

Country Phone ( ) Extension

E-mail Fax ( )

May we contact you further concerning our documentation? ___Yes ___No

You can also send us your comments by e-mail to **bug-doc@cisco.com**, or by fax to **408-527-8089**.

When mailing this card from outside of the United States, please enclose in an envelope addressed to the location on the back of this card with the required postage or fax to 1-408-527-8089.

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

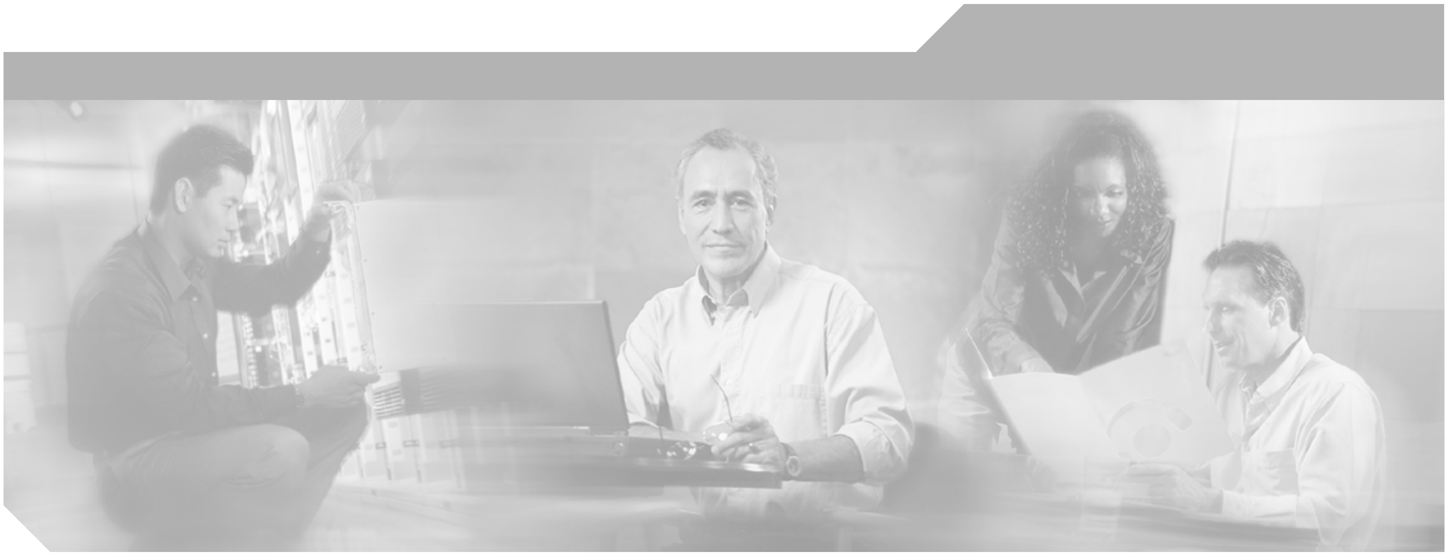
BUSINESS REPLY MAIL

FIRST-CLASS MAIL   PERMIT NO. 4631   SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

DOCUMENT RESOURCE CONNECTION
CISCO SYSTEMS INC
170 WEST TASMAN DR
SAN JOSE CA 95134-9916

8.6 EFT Copy



Catalyst 6500 Series Switch Command Reference

Release 8.6

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-8977-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Catalyst 6500 Series Switch Command Reference

CONTENTS

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy

Preface

This preface describes the audience, organization, and conventions of this publication and provides information on how to obtain related documentation.

Audience

This publication is for experienced network administrators who are responsible for configuring and maintaining Catalyst 6500 series switches.

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	Command-Line Interfaces	Describes the two types of CLIs found on Catalyst 6500 series switches.
Chapter 2	Catalyst 6500 Series Switch and ROM Monitor Commands	Lists alphabetically and provides detailed information for all Catalyst 6500 series switch and ROM-monitor commands.
Appendix A	Acronyms	Defines the acronyms used in this publication.

Related Documentation

Other documents in the Catalyst 6500 series switch documentation set include the following:

- *Catalyst 6500 Series Installation Guide*
- *Catalyst 6000 Series Installation Guide*
- *Catalyst 6500 Series Module Installation Guide*
- *Catalyst 6500 Series Software Configuration Guide*
- *Catalyst 6500 Series System Message Guide*
- *Catalyst 6500 Series Quick Software Configuration Guide*

- *ATM Software Configuration Guide and Command Reference for the Catalyst 5000 Family and 6500 Series Switches*
- *Release Notes for Catalyst 6500 Series*

For information about MIBs, refer to this URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Conventions

This publication uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Command-Line Interfaces

This chapter describes the command-line interfaces (CLI) available on the Catalyst 6500 series switches and contains these sections:

- Switch CLI, page 1-1
- ROM Monitor CLI, page 1-17

For information regarding the ATM CLI and commands, refer to the *ATM Software Configuration Guide and Command Reference—Catalyst 5000 Family and 6500 Series Switches* publication.

For information regarding the IDSM CLI and commands, refer to the *Catalyst 6500 Series Intrusion Detection System Module Installation and Configuration Note* publication.

For definitions of terms and acronyms listed in this publication, see Appendix A, "Acronyms."

Switch CLI

Catalyst 6500 series switches are multimodule systems. Commands you enter from the CLI can apply to the entire system or to a specific module, port, or VLAN.

You can configure and maintain the Catalyst 6500 series switches by entering commands from the switch CLI. The CLI is a basic command-line interpreter similar to the UNIX C shell. Using the CLI **session** command, you can access the router configuration software and perform tasks such as history substitution and alias creation.

Accessing the Switch CLI

You can access the switch CLI from a console terminal connected to an EIA/TIA-232 port or through a Telnet session. The CLI allows fixed baud rates. Telnet sessions disconnect automatically after remaining idle for a user-defined time period.

Note EIA/TIA-232 was known as RS-232 before its acceptance as a standard by the Electronic Industries Alliance and Telecommunications Industry Association.

Accessing the Switch CLI via the Console Port (EIA/TIA-232)

To access the switch through the console (EIA/TIA-232) port, perform these steps:

Step 1 From the Cisco Systems Console prompt, press **Return**.

Step 2 At the prompt, enter the system password. The Console> prompt appears, indicating that you have accessed the CLI in normal mode.

Step 3 Enter the necessary commands to complete your desired tasks.

Step 4 When finished, exit the session by entering the **quit** command.

After connecting through the console port, you see this display:

```
Cisco Systems Console
Enter password:
Console> <password>
Console>
```

Accessing the Switch CLI via Telnet

To access the switch through a Telnet session, you must first set the IP address for the switch. You can open multiple sessions to the switch via Telnet.

To access the switch from a remote host with Telnet, perform these steps:

Step 1 From the remote host, enter the **telnet** command and the host name or IP address of the switch that you want to access.

Step 2 At the prompt, enter the password for the CLI. If no password has been configured, press **Return**.

Step 3 Enter the necessary commands to complete your desired tasks.

Step 4 When finished, exit the Telnet session by entering the **quit** command.

After connecting through a Telnet session, you see this display:

```
host% telnet cat6000-1.cisco.com
Trying 172.16.44.30 ...
Connected to cat6000-1.
```

Operating the Switch CLI

This section describes command modes and functions that allow you to operate the switch CLI.

Accessing the Command Modes

The CLI has two modes of operation: normal and privileged. Both are password-protected. Use normal-mode commands for everyday system monitoring. Use privileged commands for system configuration and basic troubleshooting.

After you log in, the system enters normal mode, which gives you access to normal-mode commands only. You can enter privileged mode by entering the **enable** command followed by the enable password. Privileged mode is indicated by the word "enable" in the system prompt. To return to normal mode, enter the **disable** command at the prompt.

The following example shows how to enter privileged mode:

```
Console> enable
Enter password: <password>
Console> (enable)
```

Using Command-Line Processing

Switch commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to be different from any other currently available commands or parameters. You can scroll through the last 20 commands stored in the history buffer and enter or edit the command at the prompt. (See Table 1-1.)

Table 1-1 Command-Line Processing Keystroke

Keystroke	Function
Ctrl-A	Jumps to the first character of the command line.
Ctrl-B or the left arrow key	Moves the cursor back one character.
Ctrl-C	Escapes and terminates prompts and tasks.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Jumps to the end of the current command line.
Ctrl-F or the right arrow key[1]	Moves the cursor forward one character.
Ctrl-K	Deletes from the cursor to the end of the command line.
Ctrl-L; Ctrl-R	Repeats current command line on a new line.
Ctrl-N or the down arrow key[1]	Enters next command line in the history buffer.
Ctrl-P or the up arrow key[1]	Enters previous command line in the history buffer.
Ctrl-U; Ctrl-X	Deletes from the cursor to the beginning of the command line.
Ctrl-W	Deletes last word typed.

Table 1-1 Command-Line Processing Keystroke (continued)

Keystroke	Function
Esc B	Moves the cursor back one word.
Esc D	Deletes from the cursor to the end of the word.
Esc F	Moves the cursor forward one word.
Delete key or Backspace key	Erases a mistake when entering a command; reenter the command after using this key.

[1] The arrow keys function only on ANSI-compatible terminals such as VT100s.

Using the Command-Line Editing Features

Catalyst 6500 series switch software includes an enhanced editing mode that provides a set of editing key functions similar to those of the Emacs editor. You can enter commands in uppercase, lowercase, or a mix of both. Only passwords are case sensitive. You can abbreviate commands and keywords to the number of characters that allow a unique abbreviation.

For example, you can abbreviate the **show** command to **sh**. After entering the command at the system prompt, press **Return** to execute the command.

Moving Around on the Command Line

Perform one of these tasks to move the cursor around on the command line for corrections or changes:

Task	Keystrokes
Move the cursor back one character.	Press **Ctrl-B** or press the left arrow key[1].
Move the cursor forward one character.	Press **Ctrl-F** or press the right arrow key[1].
Move the cursor to the beginning of the command line.	Press **Ctrl-A**.
Move the cursor to the end of the command line.	Press **Ctrl-E**.
Move the cursor back one word.	Press **Esc B**.
Move the cursor forward one word.	Press **Esc F**.

[1] The arrow keys function only on ANSI-compatible terminals such as VT100s.

Completing a Partial Command Name

If you cannot remember a complete command name, press the **Tab** key to allow the system to complete a partial entry. To do so, perform this task:

Task	Keystrokes
Complete a command name.	Enter the first few letters and press the **Tab** key.

If your keyboard does not have a Tab key, press **Ctrl-I** instead.

8.6 EFT Copy

In the following example, when you enter the letters **conf** and press the **Tab** key, the system provides the complete command:

```
Console> (enable) conf<Tab>

Console> (enable) configure
```

If you enter a set of characters that could indicate more than one command, the system beeps to indicate an error. Enter a question mark (?) to obtain a list of commands that begin with that set of characters. Do not leave a space between the last letter and the question mark (?). For example, three commands in privileged mode start with co. To see what they are, enter **co?** at the privileged prompt. The system displays all commands that begin with co, as follows:

```
Console> (enable) co?
configure  connect  copy
```

Pasting in Buffer Entries

The system provides a buffer that contains the last ten items you deleted. You can recall these items and paste them in the command line by performing this task:

Task	Keystrokes
Recall the most recent entry in the buffer.	Press **Ctrl-Y**.
Recall the next buffer entry.	Press **Esc Y**.

The buffer contains only the last ten items you have deleted or cut. If you press **Esc Y** more than ten times, you cycle back to the first buffer entry.

Editing Command Lines That Wrap

The new editing command set provides a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. To scroll back, perform this task:

Task	Keystrokes
Return to the beginning of a command line to verify that you have entered a lengthy command correctly.	Press **Ctrl-B** or the left arrow key repeatedly until you scroll back to the beginning of the command entry, or press **Ctrl-A** to return directly to the beginning of the line[1].

[1] The arrow keys function only on ANSI-compatible terminals such as VT100s.

Use line wrapping with the command history feature to recall and modify previous complex command entries. See the "Using History Substitution" section on page 1-8 for information about recalling previous command entries.

The system assumes your terminal screen is 80 columns wide. If your screen has a different width, enter the **terminal width** command to tell the router the correct width of your screen.

Deleting Entries

Perform one of these tasks to delete command entries if you make a mistake or change your mind:

Task	Keystrokes
Erase the character to the left of the cursor.	Press the **Delete** or **Backspace** key.
Delete the character at the cursor.	Press **Ctrl-D**.
Delete from the cursor to the end of the command line.	Press **Ctrl-K**.
Delete from the cursor to the beginning of the command line.	Press **Ctrl-U** or **Ctrl-X**.
Delete the word to the left of the cursor.	Press **Ctrl-W**.
Delete from the cursor to the end of the word.	Press **Esc D**.

Scrolling Down a Line or a Screen

When you use the help facility to list the commands in a particular mode, the list is often longer than the terminal screen can display. In such cases, a ---More--- prompt is displayed at the bottom of the screen. To view the next line or screen, perform these tasks:

Task	Keystrokes
Scroll down one line.	Press the **Return** key.
Scroll down one screen.	Press the **Spacebar**.

Note The ---More--- prompt is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output.

Scrolling to Specified Text

If you enter /*text* and press the **Return** key at the --More-- prompt, the display starts two lines above the line containing the *text* string. If the text string is not found, “Pattern Not Found” is displayed. You can also enter “**n**” at the --More-- prompt to search for the last entered *text* string. You can use this search method on all **show** commands that use the more buffer to display screen by screen ouput. The following is a list of **show** commands that do not use the more buffer and do not support this feature:

- **show cam**
- **show mls**
- **show tech-support**

Redisplaying the Current Command Line

If you enter a command and the system suddenly sends a message to your screen, you can recall your current command line entry. To do so, perform this task:

Task	Keystrokes
Redisplay the current command line.	Press **Ctrl-L** or **Ctrl-R**.

Transposing Mistyped Characters

If you mistype a command entry, you can transpose the mistyped characters by performing this task:

Task	Keystrokes
Transpose the character to the left of the cursor with the character located at the cursor.	Press **Ctrl-T**.

Controlling Capitalization

You can change words to uppercase or lowercase, or capitalize a set of letters, with simple keystroke sequences:

Task	Keystrokes
Capitalize at the cursor.	Press **Esc C**.
Change the word at the cursor to lowercase.	Press **Esc L**.
Capitalize letters from the cursor to the end of the word.	Press **Esc U**.

Designating a Keystroke as a Command Entry

You can use a particular keystroke as an executable command. Perform this task:

Task	Keystrokes
Insert a code to indicate to the system that the keystroke immediately following should be treated as a command entry, *not* an editing key.	Press **Ctrl-V** or **Esc Q**.

8.6 EFT Copy

Using Command Aliases

Like regular commands, aliases are not case sensitive. However, unlike regular commands, some aliases cannot be abbreviated. See Table 1-2 for a list of switch CLI aliases that cannot be abbreviated.

Table 1-2 Switch CLI Command Aliases

Alias	Command
batch	**configure**
di	**show**
earl	**cam**
exit	**quit**
logout	**quit**

Using History Substitution

Commands that you enter during each terminal session are stored in a history buffer, which stores the last 20 commands you entered during a terminal session. History substitution allows you to access these commands without retyping them by using special abbreviated commands. (See Table 1-3.)

Table 1-3 History Substitution Commands

Command	Function
To repeat recent commands:	
!!	Repeat the most recent command.
!-nn	Repeat the nnth most recent command.
!n	Repeat command n.
!aaa	Repeat the command beginning with string aaa.
!?aaa	Repeat the command containing the string aaa.
To modify and repeat the most recent command:	
^aaa^bbb	Replace string aaa with string bbb in the most recent command.
To add a string to the end of a previous command and repeat it:	
!!aaa	Add string aaa to the end of the most recent command.
!n aaa	Add string aaa to the end of command n.
!aaa bbb	Add string bbb to the end of the command beginning with string aaa.
!?aaa bbb	Add string bbb to the end of the command containing string aaa.

Accessing Command Help

To see a list of top-level commands and command categories, type **help** in normal or privileged mode. Context-sensitive help (usage and syntax information) for individual commands can be seen by appending **help** to any specific command. If you enter a command using the wrong number of arguments or inappropriate arguments, usage and syntax information for that command is displayed. Additionally, appending **help** to a command category displays a list of commands in that category.

Top-Level Commands and Command Categories

In normal mode, use the **help** command to display a list of top-level commands and command categories, as follows:

```
Console> help
Commands:
----------------------------------------------------------------------
cd                             Set default flash device
dir                            Show list of files on flash device
enable                         Enable privileged mode
help                           Show this help screen
history                        Show contents of history substitution buffer
l2trace                        Layer2 trace between hosts
ping                           Send echo packets to hosts
pwd                            Show default flash device
quit                           Exit from the Admin session
session                        Tunnel to ATM or Router module
set                            Set commands, use 'set help' for more info
show                           Show commands, use 'show help' for more info
traceroute                     Trace the route to a host
verify                         Verify checksum of file on flash device
wait                           Wait for x seconds
whichboot                      Which file booted
Console>
```

In privileged mode, enter the **help** command to display a list of top-level commands and command categories, as follows:

```
Console> (enable) help
Commands:
----------------------------------------------------------------------
cd                          Set default flash device
clear                       Clear, use 'clear help' for more info
commit                      Commit ACL to hardware and NVRAM
configure                   Configure system from network
copy                        Copy files between TFTP/RCP/module/flash devices
delete                      Delete a file on flash device
dir                         Show list of files on flash device
disable                     Disable privileged mode
disconnect                  Disconnect user session
download                    Download code to a processor
enable                      Enable privileged mode
format                      Format a flash device
help                        Show this help screen
history                     Show contents of history substitution buffer
l2trace                     Layer2 trace between hosts
ping                        Send echo packets to hosts
pwd                         Show default flash device
quit                        Exit from the Admin session
reconfirm                   Reconfirm VMPS
reload                      Force software reload to linecard
reset                       Reset system or module
rollback                    Rollback changes made to ACL in editbuffer
```

```
session                   Tunnel to ATM or Router module
set                       Set commands, use 'set help' for more info
show                      Show commands, use 'show help' for more info
slip                      Attach/detach Serial Line IP interface
squeeze                   Reclaim space used by deleted files
switch                    Switch to standby <clock|supervisor>
telnet                    Telnet to a remote host
test                      Test command, use 'test help' for more info
undelete                  Undelete a file on flash device
upload                    Upload code from a processor
verify                    Verify checksum of file on flash device
wait                      Wait for x seconds
whichboot                 Which file booted
write                     Write system configuration to terminal/network
Console> (enable)
```

Command Categories

On some commands (such as **clear**, **set**, and **show**), typing **help** after the command provides a list of commands in that category. For example, this display shows a partial list of commands for the **clear** category:

```
Console> (enable) clear help

Clear commands:
----------------------------------------------------------------------------
clear alias                  Clear aliases of commands
clear arp                    Clear ARP table entries
clear banner                 Clear Message Of The Day banner
clear boot                   Clear booting environment variable
clear cam                    Clear CAM table entries
clear channel                Clear PAgP statistical information
.
.
.
```

Context-Sensitive Help

Usage and syntax information for individual commands can be seen by appending **help** to any specific command. For example, the following display shows usage and syntax information for the **set length** command:

```
Console> set length help
Usage: set length <screenlength> [default]
       (screenlength = 5..512, 0 to disable 'more' feature)
Console>
```

Designating Modules, Ports, and VLANs

The Catalyst 6500 series modules (module slots), ports, and VLANs are numbered starting with 1. The supervisor engine module is module 1, residing in the top slot. On each module, port 1 is the leftmost port. To reference a specific port on a specific module, the command syntax is *mod/port*. For example, **3/1** denotes module 3, port 1. In some commands, such as **set trunk**, **set cam**, and **set vlan**, you can enter lists of ports and VLANs.

You can designate ports by entering the module and port number pairs, separated by commas. To specify a range of ports, use a dash (-) between the module number and port number pairs. Dashes take precedence over commas. The following examples show several ways of designating ports:

Example 1: **2/1,2/3** denotes module 2, port 1 and module 2, port 3.

Example 2: **2/1-12** denotes module 2, ports 1 through 12.

Example 3: **2/1-2/12** also denotes module 2, ports 1 through 12.

Each VLAN is designated by a single number. You can specify lists of VLANs the same way you do for ports. Individual VLANs are separated by commas (,); ranges are separated by dashes (-). In the following example, VLANs 1 through 10 and VLAN 1000 are specified:

```
1-10,1000
```

Designating MAC Addresses, IP and IPX Addresses, and IP Aliases

Some commands require a MAC address that you must designate in a standard format. The MAC address format must be six hexadecimal numbers separated by hyphens, as shown in this example:

```
00-00-0c-24-d2-fe
```

Some commands require an IP address. The IP address format is 32 bits, written as four octets separated by periods (dotted decimal format). IP addresses are made up of a network section, an optional subnet section, and a host section, as shown in this example:

```
126.2.54.1
```

If DNS is configured properly on the switch, you can use IP host names instead of IP addresses. For information on configuring DNS, refer to the *Catalyst 6500 Series Switch Software Configuration Guide*.

If the IP alias table is configured, you can use IP aliases in place of the dotted decimal IP address. This is true for most commands that use an IP address, except commands that define the IP address or IP alias.

When entering the IPX address syntax, use the following format:

- IPX net address—1..FFFFFFFE
- IPX node address—x.x.x where x is 0..FFFF
- IPX address—ipx_net.ipx_node (for example 3.0034.1245.AB45, A43.0000.0000.0001)

Using Command Completion Features

The command completion features consist of these functions:

- Using Command Self-Repeat
- Using Keyword Lookup
- Using Partial Keyword Lookup
- Using Command Completion

Using Command Self-Repeat

Use the command self-repeat function to display matches to all possible keywords if a string represents a unique match. If a unique match is not found, the longest matching string is provided. To display the matches, enter a space after the last parameter and enter **?**. Once the matches are displayed, the system comes back to the prompt and displays the last command without the **?**. In the following example, notice how the system repeats the command entered without the **?**:

```
Console> (enable) set mls nde
  disable              Disable multilayer switching data export filter
  enable               Enable multilayer switching data export filter
  engineer             Engineer setting of the export filter
  flow                 Setting multilayer switching export filter
  <collector_ip>       IP address
Console> (enable) set mls nde
```

Using Keyword Lookup

Use the keyword-lookup function to display a list of valid keywords and arguments for a command. To display the matches, enter a space after the last parameter and enter **?**. For example, five parameters are used by the **set mls** command. To see these parameters, enter **set mls ?** at the privileged prompt. In the following example, notice how the system repeats the command entered without the **?**:

```
Console> (enable) set mls ?
  agingtime                  Set agingtime for MLS cache entry
  exclude                    Set MLS excluded protocol ports
  flow                       Set minimum flow mask
  nde                        Configure Netflow Data Export
  statistics                 Add protocols to protocol statistics list
Console> (enable) set mls
```

Using Partial Keyword Lookup

Use the partial keyword-lookup function to display a list of commands that begin with a specific set of characters. To display the matches, enter **?** immediately after the last parameter. For example, enter **co?** at the privileged prompt to display a list of commands that start with **co**. The system displays all commands that begin with **co** and repeats the command entered without the **?**:

```
Console> (enable) co?
  commit               Commit ACL to hardware and NVRAM
  configure            Configure system from network
  copy                 Copy files between TFTP/RCP/module/flash devices
Console> (enable) co
```

Using Command Completion

Use the command completion function to complete a command or keyword. When you enter a unique partial character string and press **Tab**, the system completes the command or keyword on the command line. For example, if you enter **co** at the privileged prompt and press **Tab**, the system completes the command as **configure** because it is the only command that matches the criteria.

If no completion can be done, no action is carried out and the system returns to the prompt and the last command. The cursor appears immediately after the keyword, allowing you to enter additional information.

Using the CLI String Search

The pattern in the command output is referred to as a string. The CLI string search feature allows you to search or filter any **show** or **more** command output and allows you to search and filter at --More-- prompts. This feature is useful when you need to sort though large amounts of output or if you want to exclude output that you do not need to see.

With the search function, you can begin unfiltered output at the first line that contains a regular expression you specify. You can then specify a maximum of one filter per command or start a new search from the --More-- prompt.

A regular expression is a pattern (a phrase, number, or more complex pattern) that software uses to match against **show** or **more** command output. Regular expressions are case sensitive and allow for complex matching requirements. Examples of simple regular expressions are Serial, misses, and 138. Examples of complex regular expressions are 00210..., (is), and [Oo]utput.

You can perform three types of filtering:

- Use the **begin** keyword to begin output with the line that contains a specified regular expression.
- Use the **include** keyword to include output lines that contain a specified regular expression.
- Use the **exclude** keyword to exclude output lines that contain a specified regular expression.

You can then search this filtered output at the --More-- prompts.

Note The CLI string search function does not allow you to search or filter backward through previous output; filtering cannot be specified using HTTP access to the CLI.

Regular Expressions

A regular expression can be a single character that matches the same single character in the command output or multiple characters that match the same multiple characters in the command output. This section describes how to create both single-character patterns and multiple-character patterns and how to create more complex regular expressions using multipliers, alternation, anchoring, and parentheses.

Single-Character Patterns

The simplest regular expression is a single character that matches the same single character in the command output. You can use any letter (A-Z, a-z) or digit (0-9) as a single-character pattern. You can also use other keyboard characters (such as ! or ~) as single-character patterns, but certain keyboard characters have special meaning when used in regular expressions. Table 1-4 lists the keyboard characters with special meaning.

Table 1-4 Characters with Special Meaning

Character	Special Meaning
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the pattern.
+	Matches 1 or more sequences of the pattern.
?	Matches 0 or 1 occurrences of the pattern.

8.6 EFT Copy

Table 1-4 Characters with Special Meaning (continued)

Character	Special Meaning
^	Matches the beginning of the string.
$	Matches the end of the string.
_ (underscore)	Matches a word delimiter. All alphanumeric characters and the underscore itself (_) form a word.

To enter these special characters as single-character patterns, remove the special meaning by preceding each character with a backslash (\). These examples are single-character patterns matching a dollar sign, an underscore, and a plus sign, respectively.

\$ _ \+

You can specify a range of single-character patterns to match against command output. For example, you can create a regular expression that matches a string containing one of the following letters: a, e, i, o, or u. One and only one of these characters must exist in the string for pattern matching to succeed. To specify a range of single-character patterns, enclose the single-character patterns in square brackets ([ ]). For example,

[aeiou]

matches any one of the five vowels of the lowercase alphabet, while

[abcdABCD]

matches any one of the first four letters of the lower- or uppercase alphabet.

You can simplify ranges by entering only the end points of the range separated by a dash (-). Simplify the previous range as follows:

[a-dA-D]

To add a dash as a single-character pattern in your range, include another dash and precede it with a backslash:

[a-dA-D\-]

You can also include a right square bracket (]) as a single-character pattern in your range. To do so, enter the following:

[a-dA-D\-\]]

The previous example matches any one of the first four letters of the lower- or uppercase alphabet, a dash, or a right square bracket.

You can reverse the matching of the range by including a caret (^) at the start of the range. This example matches any letter except the ones listed:

[^a-dqsv]

This example matches anything except a right square bracket (]) or the letter d:

[^\]d]

Multiple-Character Patterns

When creating regular expressions, you can also specify a pattern containing multiple characters. You create multiple-character regular expressions by joining letters, digits, or keyboard characters that do not have special meaning. For example, a4% is a multiple-character regular expression. Put a backslash in front of the keyboard characters that have special meaning when you want to remove their special meaning.

With multiple-character patterns, order is important. The regular expression a4% matches the character a followed by a 4 followed by a % sign. If the string does not have a4%, in that order, pattern matching fails. This multiple-character regular expression

a.

uses the special meaning of the period character to match the letter a followed by any single character. With this example, the strings ab, a!, or a2 are all valid matches for the regular expression.

You can remove the special meaning of the period character by putting a backslash in front of it. In the following expression

a\.

only the string a. matches this regular expression.

You can create a multiple-character regular expression containing all letters, all digits, all keyboard characters, or a combination of letters, digits, and other keyboard characters. These examples are all valid regular expressions:

telebit 3107 v32bis

Multipliers

You can create more complex regular expressions to match multiple occurrences of a specified regular expression by using some special characters with your single- and multiple-character patterns. Table 1-5 lists the special characters that specify “multiples” of a regular expression.

Table 1-5 Special Characters Used as Multipliers

Character	Description
*	Matches 0 or more single- or multiple-character patterns.
+	Matches 1 or more single- or multiple-character patterns.
?	Matches 0 or 1 occurrences of the single- or multiple-character patterns.

This example matches any number of occurrences of the letter a, including none:

a*

This pattern requires that at least one letter a in the string is matched:

a+

This pattern matches the string bb or bab:

ba?b

This string matches any number of asterisks (*):

******

8.6 EFT Copy

To use multipliers with multiple-character patterns, you enclose the pattern in parentheses. In the following example, the pattern matches any number of the multiple-character string ab:

(ab)*

As a more complex example, this pattern matches one or more instances of alphanumeric pairs (but not none; that is, an empty string is not a match):

([A-Za-z][0-9])+

The order for matches using multipliers (*, +, or ?) is to put the longest construct first. Nested constructs are matched from outside to inside. Concatenated constructs are matched beginning at the left side of the construct. Thus, the regular expression matches A9b3 but not 9Ab3 because the letters are specified before the numbers.

Alternation

Alternation allows you to specify alternative patterns to match against a string. You separate the alternative patterns with a vertical bar (|). Exactly one of the alternatives can match the string. For example, the regular expression

codex | telebit

matches the string codex or the string telebit but not both codex and telebit.

Anchoring

You can match a regular expression pattern against the beginning or the end of the string. That is, you can specify that the beginning or end of a string contains a specific pattern. You “anchor” these regular expressions to a portion of the string using the special characters shown in Table 1-6.

Table 1-6 Special Characters Used for Anchoring

Character	Description
^	Matches the beginning of the string.
$	Matches the end of the string.

This regular expression matches a string only if the string starts with abcd:

^abcd

In contrast, this expression is in a range that matches any single letter, as long as it is not the letters a, b, c, or d:

[^abcd]

With this example, the regular expression matches a string that ends with .12:

$\.12

Contrast these anchoring characters with the special character underscore (_). The underscore matches the beginning of a string (^), the end of a string ($), parentheses ( ), space ( ), braces { }, comma (,), or underscore (_). With the underscore character, you can specify that a pattern exist anywhere in the string.

For example:

_1300_

matches any string that has 1300 somewhere in the string. The string's 1300 can be preceded by or end with a space, brace, or comma. For example:

{1300- or **{1300:**

matches the regular expression, but 21300 and 13000 do not.

Using the underscore character, you can replace long regular expression lists, such as the following:

^1300$ ^1300(space) (space)1300 {1300, ,1300, {1300} ,1300, (1300

with

_1300_

ROM Monitor CLI

The ROM monitor is a ROM-based program that executes upon platform startup, reset, or when a fatal exception occurs.

Accessing the ROM Monitor CLI

The system enters ROM-monitor mode if the switch does not find a valid system image, if the NVRAM configuration is corrupted, or if the configuration register is set to enter ROM-monitor mode. From the ROM-monitor mode, you can load a system image manually from Flash memory, from a network server file, or from bootflash. You can also enter ROM-monitor mode by restarting the switch and pressing the **Break** key during the first 60 seconds of startup.

Note Break is always enabled for 60 seconds after rebooting the system, regardless of whether Break is configured to be off by configuration register settings.

To connect through a terminal server, escape to the Telnet prompt, and enter the **send break** command to break back to the ROM-monitor mode.

Operating the ROM Monitor CLI

The ROM monitor commands are used to load and copy system images, microcode images, and configuration files. System images contain the system software. Microcode images contain microcode to be downloaded to various hardware devices. Configuration files contain commands to customize Catalyst 6500 series software.

8.6 EFT Copy

The manual **boot** command has the following syntax:

Note Enter the **copy** *file-id* {**tftp** | **flash** | *file-id*} command to obtain an image from the network.

- **boot**—Boot from ROM
- **boot** [*-xv*] [*device***:**][*imagename*]—Boot from the local device. If you do not specify an image name, the system defaults to the first valid file in the device. The image name is case sensitive.

Once you are in ROM-monitor mode, the prompt changes to rommon 1>. While you are in ROM-monitor mode, each time you enter a command, the number in the prompt increments by one.

CHAPTER 2

Catalyst 6500 Series Switch and ROM Monitor Commands

This chapter contains an alphabetical listing of all switch and ROM monitor commands available on the Catalyst 6500 series switches.

For information regarding ATM module-related commands, refer to the *ATM Configuration Guide and Command Reference—Catalyst 5000 and 6000 Family Switches*.

For information regarding IDS module-related commands, refer to the *Catalyst 6500 Series Intrusion Detection System Module Installation and Configuration Note*.

Except where specifically differentiated, the Layer 3 switching engine refers to one of the following:

- Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card)
- Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2)

alias

To set and display command aliases, use the **alias** command.

alias [*name*=*value*]

Syntax Description

name=	(Optional) Name you give to the alias.
value	(Optional) Value of the alias.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

If *value* contains white space or other special (shell) characters, you must use quotation marks. If *value* has a space as its last character, the next command line word is checked for an alias. (Normally, only the first word on a command line is checked.)

Without an argument, this command prints a list of all aliased names with their values.

An equal sign (=) is required between the name and value of the alias.

You must issue a **sync** command to save your change. If you do not issue a **sync** command, the change is not saved, and a **reset** removes your change.

Examples

This example shows how to display a list of available **alias** commands and how to create an alias for the **set** command:

```
rommon 1 > alias
r=repeat
h=history
?=help
b=boot
ls=dir
i=reset
k=stack
rommon 2 > alias s=set
rommon 3 > alias
r=repeat
h=history
?=help
b=boot
ls=dir
i=reset
```

```
k=stack
s=set
rommon 4 > s
PS1=rommon ! >
BOOT=bootflash:RTSYNC_llue_11,1;slot0:f1,1;
==========================================================================
```

Related Commands

unalias

boot

To boot up an external process, use the **boot** command.

boot [**-x**] [**-v**] [*device***:**][*imagename*]

Syntax Description

-x	(Optional) Loads the image but does not execute.
-v	(Optional) Toggles verbose mode.
*device***:**	(Optional) ID of the device.
imagename	(Optional) Name of the image.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

If you do not enter any arguments, the **boot** command boots the first image in bootflash. To specify an image, enter the image name. To specify the device, enter the device ID.

If a device is not entered with an image name*,* the image is not booted.

If a device name is not recognized by the monitor, the monitor passes the device ID to the boot helper image.

This command will not boot the MSFC if the PFC is not present in the Catalyst 6500 series switch.

Examples

This example shows how to use the **boot** command:

```
rommon 2 > boot bootflash:cat6000-sup.6-1-1.bin
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Uncompressing file:
##########################################################################################
##########################################################################################
################################################################################
```

cd

To set the default Flash device for the system, use the **cd** command.

cd [[*m/*]*device***:**]

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device***:**	(Optional) Valid devices include **bootflash** and **slot0**.

Defaults

The default Flash device is bootflash.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

A colon (:) is required after the specified device.

With commands where the device is an option, if the default device is not specified, the device set by the **cd** command is used.

Examples

This example shows how to set the system default Flash device to bootflash:

```
Console> cd bootflash:
Default flash device set to bootflash.
Console>
```

Related Commands

pwd

clear acllog

To disable ACL log rate limiting, use the **clear acllog** command.

clear acllog

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to disable ACL log rate limiting:

```
Console> (enable) clear acllog
ACL log rate limit is cleared.
If the ACLs-LOG were already applied, the rate limit mechanism will be disabled on system
restart, or after shut/no shut the interface.
Console> (enable)
```

Related Commands

set acllog ratelimit
show acllog

clear acl mac-packet-classify

To match only MAC packets with MAC ACLs, use the **clear acl mac-packet-classify** command.

clear acl mac-packet-classify {*vlans* | **all**}

Syntax Description

vlans	VLAN list; valid values are 1 to 4094.
all	Specifies all VLANs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The MAC-based ACL feature is available only on a system with a PFC3B or a PFC3BXL. This feature affects both security ACLs and QoS MAC ACLs.

The specified VLAN reverts back to matching only MAC packets with MAC ACLs. The **set acl mac-packet-classify** command sets MAC-based ACL lookups for all packet types on a VLAN.

Examples

This example shows how to revert the specified VLAN back to matching only MAC packets with MAC ACLs:

```
Console> (enable) clear acl mac-packet-classify 5
Disabled mac-packet-classify on vlan(s) 5.
Console> (enable)
```

Related Commands

set acl mac-packet-classify
show acl mac-packet-classify

clear alias

To clear the abbreviated versions of commands, use the **clear alias** command.

clear alias {*name* | **all**}

Syntax Description

name	Alternate identifier of the command.
all	Clears every alternate identifier previously created.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to erase the arpdel alias:

```
Console> (enable) clear alias arpdel
Command alias deleted.
Console> (enable)
```

This example shows how to erase all the aliases:

```
Console> (enable) clear alias all
Command alias table cleared. (1)
Console> (enable)
```

(1) indicates the number of command aliases cleared.

Related Commands

set alias
show alias

clear arp

To delete a specific entry or all entries from the ARP table, use the **clear arp** command.

clear arp [**all** | **dynamic** | **permanent** | **static**] {*ip_addr*}

Syntax Description

all	(Optional) Clears all ARP entries.
dynamic	(Optional) Clears all dynamic ARP entries.
permanent	(Optional) Clears all permanent ARP entries.
static	(Optional) Clears all static ARP entries.
ip_addr	IP address to clear from the ARP table.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove IP address 198.133.219.209 from the ARP table:

```
Console> (enable) clear arp 198.133.219.209
ARP entry deleted.
Console> (enable)
```

This example shows how to remove all entries from the ARP table:

```
Console> (enable) clear arp all
ARP table cleared. (1)
Console> (enable)
```

(1) indicates the number of entries cleared.

This example shows how to remove all dynamically learned ARP entries:

```
Console> (enable) clear arp dynamic
Unknown host
Dynamic ARP entries cleared. (3)
Console> (enable)
```

This example shows how to clear all permanently entered ARP entries:

```
Console> (enable) clear arp permanent
Unknown host
Permanent ARP entries cleared.(5)
Console> (enable)
```

Related Commands

set arp
show arp

clear autoshut

To clear the runtime counters or reset the automatic module shutdown settings to the default settings, use the **clear autoshut** command.

clear autoshut {{**counters** *mod*} | **frequency** | **period**}

Syntax Description

counters *mod*	Clears the runtime counters for the specified module.
frequency	Resets the autoshut frequency to the default setting.
period	Resets the autoshut period to the default setting.

Defaults

The defaults are as follows:

- **frequency** is three times.
- **period** is two minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can shut down a module manually using the **set module disable** or the **set module power down** commands.

This command is supported on Ethernet modules only.

Examples

This example shows how to clear the runtime counters on a specific module:

```
Console> (enable) clear autoshut counters 3
Automatic shutdown counters cleared for module 3
Console> (enable)
```

This example shows how to reset the autoshut frequency to the default setting:

```
Console> (enable) clear autoshut frequency
Console> (enable)
```

This example shows how to reset the autoshut period to the default setting:

```
Console> (enable) clear autoshut period
Console> (enable)
```

Related Commands

set autoshut
set module autoshut
show autoshut

clear banner motd

To clear the message-of-the-day banner, use the **clear banner motd** command.

clear banner motd

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the message-of-the-day banner:

```
Console> (enable) clear banner motd
MOTD banner cleared
Console> (enable)
```

Related Commands

set banner motd

clear boot auto-config

To clear the contents of the CONFIG_FILE environment variable used to specify the configuration files used during bootup, use the **clear boot auto-config** command.

clear boot auto-config [*mod*]

Syntax Description

mod	(Optional) Module number of the supervisor engine containing the Flash device.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the auto-config file:

```
Console> (enable) clear boot auto-config
CONFIG_FILE variable =
Console> (enable)
```

Related Commands

set boot auto-config
show boot

clear boot device

To clear the contents of the CONFIG_FILE environment variable used to specify the NAM startup configuration files, use the **clear boot device** command.

clear boot device *mod*

Syntax Description

mod	Number of the module containing the Flash device.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported by the NAM module only.

Examples

This example shows how to clear the NAM boot string from NVRAM for module 2:

```
Console> (enable) clear boot device 2
Device BOOT variable =
Console> (enable)
```

Related Commands

set boot device
show boot device

clear boot system

To clear the contents of the BOOT environment variable and the configuration register setting, use the **clear boot system** command.

clear boot system all [*mod*]

clear boot system flash *device*:[*filename*] [*mod*]

Syntax Description

all	Clears the whole BOOT environment variable.
mod	(Optional) Module number of the supervisor engine containing the Flash device.
flash	(Optional) Clears the Flash device.
device:	Name of the Flash device.
filename	(Optional) Filename of the Flash device.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the whole BOOT environment variable:

```
Console> (enable) clear boot system all
BOOT variable =
Console> (enable)
```

This example shows how to clear a specific device; note that the specified device is not listed:

```
Console> (enable) clear boot system flash bootflash:cat6000-sup.5-5-1.bin
BOOT variable = bootflash:cat6000-sup.6-1-1.bin,1;bootflash:cat6000-sup.5-5-2.
bin,1;
Console> (enable)
```

Related Commands

set boot system flash
show boot

clear cam

To delete a specific entry or all entries from the CAM table, use the **clear cam** command.

clear cam *mac_addr* [*vlan*]

clear cam {**dynamic** | **static** | **permanent**} [*vlan*]

Syntax Description

mac_addr	One or more MAC addresses.
vlan	(Optional) Number of the VLAN; valid values are from 1 to 4094.
dynamic	Clears the dynamic CAM entries from the CAM table.
static	Clears the static CAM entries from the CAM table.
permanent	Clears the permanent CAM entries from the CAM table.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove MAC address 00-40-0b-a0-03-fa from the CAM table:

```
Console> (enable) clear cam 00-40-0b-a0-03-fa
CAM table entry cleared.
Console> (enable)
```

This example shows how to clear dynamic entries from the CAM table:

```
Console> (enable) clear cam dynamic
Dynamic CAM entries cleared.
Console> (enable)
```

Related Commands

set cam
show cam

clear cam monitor

To clear the configuration for the MAC-address limits and actions, use the **clear cam monitor** command.

clear cam monitor {**all** | *mod/port* | *vlan*}

clear cam monitor high-threshold {*mod/port* | *vlan*}

clear cam monitor low-threshold {*mod/port* | *vlan*}

Syntax Description

all	Clears all CAM table monitoring and MAC-address limit configurations from all ports.
*mod/por*t	Number of the module and the port on the module.
vlan	VLAN number; valid values are from 1 to 4094.
high-threshold	Clears the upper limit for MAC address learning.
low-threshold	Clears the lower limit for MAC address learning.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear all CAM table monitoring and MAC-address limit configurations from all ports:

```
Console> (enable) clear cam monitor all
Cleared all cam monitor configuration
Console> (enable)
```

This example shows how to clear the high threshold on port 3/1:

```
Console> (enable) clear cam monitor high-threshold 3/1
Successfully cleared high-threshold on 3/1
Console> (enable)
```

Related Commands

set cam monitor
show cam monitor

clear cam notification

To clear the CAM notification counters and history log, use the **clear cam notification** command.

clear cam notification {**all** | **counters** | **history**}

clear cam notification move counters [**all** | *vlan*]

Syntax Description

all	Clears the CAM notification counters and history log.
counters	Clears the CAM notification counters.
history	Clears the CAM notification history log.
move counters	Clears MAC move counters.
all	(Optional) Clears the MAC move counters for all VLANs.
vlan	(Optional) Number of the VLAN; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The MAC move counters are not supported on EARL 4 and earlier.

Examples

This example shows how to clear the CAM notification counters and history log:

```
Console> (enable) clear cam notification all
MAC address notification counters and history log cleared.
Console> (enable)
```

This example shows how to clear the CAM notification counters:

```
Console> (enable) clear cam notification counters
MAC address notification counters cleared.
Console> (enable)
```

This example shows how to clear the CAM notification history log:

```
Console> (enable) clear cam notification history
MAC address notification history log cleared.
Console> (enable)
```

This example shows the output if you enter the command when MMC is disabled:

```
Console> (enable) clear cam notification move counters
MAC move counters are disabled
Console> (enable)
```

These examples show the output if you enter the command when MMC is enabled and you enter the **all** keyword:

```
Console> (enable) clear cam notification move counters all
This will clear the mac move counters for all the vlans.
Do you want to continue (y/n)? y
MAC move counters for all Vlans cleared
Console> (enable)

Console> (enable) clear cam notification move counters all
This will clear the mac move counters for all the vlans.
Do you want to continue (y/n)? n
MAC move counters not cleared
Console> (enable)
```

These examples show the output if you enter the command and specify a VLAN:

```
Console> (enable) clear cam notification move counters 2
This will clear the mac move counters for vlan 2.
Do you want to continue (y/n)? y
MAC move counters for Vlan 1 cleared
Console> (enable)

Console> (enable) clear cam notification move counters 2
This will clear the mac move counters for vlan 2.
Do you want to continue (y/n)? n
MAC move counters not cleared
Console> (enable)
```

Related Commands

set cam notification
set snmp trap
show cam notification

clear channel statistics

To clear PAgP statistical information, use the **clear channel statistics** command.

clear channel statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear PAgP statistical information:

```
Console> (enable) clear channel statistics
PAgP statistics cleared.
Console> (enable)
```

Related Commands

show channel

clear config

To clear the system or module configuration information stored in NVRAM, use the **clear config** command.

clear config {**all** [**factory-defaults**] | *mod* | **acl nvram** | **interface** | **sysinfo-log** | **pvlan** | **rmon** | **snmpv3**}

Syntax Description

all	Clears all module and system configuration information, including the IP address.
factory-defaults	(Optional) Clears the profile configuration.
mod	Number of the module.
acl nvram	Clears all ACL configurations.
interface	Clears all interface configurations.
sysinfo-log	Clears all system information logging configurations.
pvlan	Clears private VLAN configurations.
rmon	Clears all RMON configurations, including the historyControlTable, the alarmTable, the eventTable, and the ringStation ControlTable.
snmpv3	Clears all SNMP version 3 configurations.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you use a Multilayer Switch Module (MSM), you can enter the **clear config** command to clear the portion of the MSM configuration retained by the Catalyst 6500 series switch supervisor engine. You must clear the portion of the configuration kept by the MSM at the router level (at the router CLI prompt).

Before using the **clear config all** command, save a backup of the configuration using the **copy** command.

When you enter the **clear config all** command, the system loads the profile configuration if there is one. When you enter the **clear config all factory-defaults** command, both the system configuration and the profile configuration are cleared.

Examples

This example shows how to delete the configuration information in NVRAM on module 2:

```
Console> (enable) clear config 2
This command will clear module 2 configuration.
Do you want to continue (y/n) [n]? y
.............................
Module 2 configuration cleared.
Console> (enable)
```

This example shows how to delete the configuration information stored in NVRAM on module 1 (the supervisor engine):

```
Console> (enable) clear config 1
This command will clear module 1 configuration.
Do you want to continue (y/n) [n]? y
......
Module 1 configuration cleared.
host%
```

This example shows how to delete all the configuration information for the Catalyst 6500 series switches:

```
Console> (enable) clear config all
This command will clear all configuration in NVRAM.
Do you want to continue (y/n) [n]? y
...........................................
Connection closed by foreign host
host%
```

This example shows how to delete all the SNMP configuration information for the Catalyst 6500 series switches:

```
Console> (enable) clear config snmpv3
This command will clear SNMPv3 configuration in NVRAM.
Do you want to continue (y/n) [n]? y
...........................................
Connection closed by foreign host
host%
```

This example shows how to delete all ACL configuration information from NVRAM:

```
Console> (enable) clear config acl nvram
ACL configuration has been deleted from NVRAM.
Warning:Use the copy commands to save the ACL configuration to a file
and the 'set boot config-register auto-config' commands to configure the
auto-config feature.
Console> (enable)
```

This example shows how to delete all system information logging configurations and return them to their default settings:

```
Console> (enable) clear config sysinfo-log
Successfully cleared the system information logging configuration.
Console> (enable)
```

This example shows how to clear both the system configuration and the profile configuration:

```
Console> (enable) clear config all factory-default
System configuration and profile configuration is cleared.
Console> (enable)
```

Related Commands

clear system info-log command
clear system profile
set config acl nvram
set system info-log
set system profile
show config qos acl
show system profile

clear config checkpoint

To clear all checkpoint configuration files or a particular configuration checkpoint file, use the **clear config checkpoint** command.

clear config checkpoint {**all** | *name*}

Syntax Description

all	Clears all configuration checkpoint files.
name	Name of a particular configuration checkpoint file to clear.

Defaults

This command has no default settings.

Command Modes

Switch command.

Command Types

Privileged.

Usage Guidelines

When a configuration checkpoint filename is cleared from the system, the associated checkpoint configuration file is deleted. You should squeeze the device to reclaim space.

The checkpoint configuration is not cleared when you enter the **clear config all** command.

Examples

This example shows how to clear all configuration checkpoint files:

```
Console> (enable) clear config checkpoint all
All configuration checkpoints cleared.
Console> (enable)
```

This example shows how to clear a particular configuration checkpoint file:

```
Console> (enable) clear config checkpoint SARAH_07122002
Cleared configuration checkpoint SARAH_07122002
Console> (enable)
```

Related Commands

set config checkpoint
set config rollback
show config checkpoints

clear config pvlan

To clear all private VLAN configurations in the system including port mappings, use the **clear config pvlan** command.

clear config pvlan

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear all private VLAN configurations in the system:

```
Console> (enable) clear config pvlan
This command will clear all private VLAN configurations.
Do you want to continue (y/n) [n]? y
VLAN 15 deleted
VLAN 16 deleted
VLAN 17 deleted
VLAN 18 deleted
Private VLAN configuration cleared.
Console> (enable)
```

Related Commands

clear pvlan mapping
clear vlan
configure
set vlan
set pvlan
set pvlan mapping
show config
show pvlan
show pvlan mapping
show vlan

clear cops

To clear Common Open Policy Service (COPS) configurations, use the **clear cops** command.

clear cops roles *role1* [*role2*]...

clear cops all-roles

clear cops server all [**diff-serv** | **rsvp**]

clear cops server *ipaddr* [**diff-serv** | **rsvp**]

clear cops domain-name

Syntax Description

roles *role#*	Specifies the roles to clear.
all-roles	Clears all roles.
server	Specifies the COPS server.
all	Clears all server tables.
diff-serv	(Optional) Specifies the differentiated services server table.
rsvp	(Optional) Specifies the RSVP+ server table.
ipaddr	IP address or IP alias of the server.
domain-name	Specifies the domain name of the server.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can use the **clear cops all-roles** command to clear all roles from all ports.

Examples

This example shows how to clear specific roles:

```
Console> (enable) clear cops roles backbone_port main_port
Roles cleared.
Console> (enable)
```

This example shows how to clear all roles:

```
Console> (enable) clear cops all-roles
All roles cleared.
Console> (enable)
```

This example shows how to clear all COPS servers:

```
Console> (enable) clear cops server all
All COPS servers cleared.
Console> (enable)
```

This example shows how to clear a specific COPS server:

```
Console> (enable) clear cops server my_server1
All COPS servers cleared.
Console> (enable)
```

This example shows how to clear the COPS domain name:

```
Console> (enable) clear cops domain-name
Domain name cleared.
Console> (enable)
```

Related Commands

set cops
show cops

clear counters

To clear MAC counters, EtherChannel MAC counters, port counters, and the channel traffic percentile, use the **clear counters** command.

clear counters all

clear counters *mod/ports*

clear counters supervisor

clear counters channel {**all** | *channel_id*}

clear counters lacp-channel {**all** | *channel_id*}

Syntax Description

all	Clears MAC and port counters for all ports.
mod/ports	Number of the module and the ports on the module.
supervisor	Clears error counters for the supervisor engine.
channel	Clears PAgP channel MAC and port counters.
all	Clears all PAgP channel counters.
channel_id	Number of a specific PAgP channel.
lacp-channel	Clears LACP channel counters.
all	Clears all LACP channel counters.
channel_id	Number of a specific LACP channel.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a range of ports to be cleared, then all ports on the switch are cleared.

To clear channel-based counters on a per-channel basis, use the channel ID number. Enter the **show port channel** command to find the channel ID number for PAgP channels. Enter the **show port lacp-channel** command to find the channel ID number for LACP channels.

If you enter a *channel-id* argument that conflicts with the protocol type for the command, this message displays:

```
Wrong protocol type for the command.
```

If you enter a *channel-id* argument that is not in the correct *channel-id* range, this message displays:

```
Valid channel Id range 1665..1792.
```

Examples

This example shows how to reset MAC and port counters to zero:

```
Console> (enable) clear counters
This command will reset all MAC and port counters reported in CLI and SNMP.
Do you want to continue (y/n) [n]? y

MAC and Port counters cleared.
Console> (enable)
```

This example shows how to reset MAC and port counters to zero for a specific module and port:

```
Console> (enable) clear counters 5/1
This command will reset MAC and port counters reported by the CLI for port(s) 5/1.
Do you want to continue (y/n) [n]? y

MAC and Port counters cleared.
Console> (enable)
```

This example shows how to reset all PAgP channel counters:

```
Console> (enable) clear counters channel all
This command will reset MAC and port counters reported by the CLI for all ports.
Counters reported by SNMP will not be affected.
Do you want to continue (y/n) [n]? y
MAC and Port counters cleared.
Console> (enable)
```

This example shows how to reset the counters for a specific PAgP channel:

```
Console> (enable) clear counters channel 769
This command will reset MAC and port counters reported by the CLI for PAGP channel 769
Counters reported by SNMP will not be affected.
Do you want to continue (y/n) [n]? y
MAC and Port counters cleared.
Console> (enable)
```

Related Commands

restore counters
show channel traffic
show port channel
show port counters
show port lacp-channel

clear crypto key rsa

To remove all RSA public-key pairs, use the **clear crypto key rsa** command.

clear crypto key rsa

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **crypto** commands are supported on systems that run these image types only:

- supk9 image—for example, cat6000-supk9.6-1-3.bin
- supcvk9 image—for example, cat6000-supcvk9.6-1-3.bin

Examples

This example shows how to clear RSA key pairs:

```
Console> (enable) clear crypto key rsa
Do you really want to clear RSA keys (y/n) [n]? y
RSA keys has been cleared.
Console> (enable)
```

Related Commands

set crypto key rsa
show crypto key

clear dhcp-snooping bindings

To clear DHCP snooping binding table entries, use the **clear dhcp-snooping bindings** command.

clear dhcp-snooping bindings [*ip_addr*] [*mac_addr*] [**vlan** *vlan*] [**port** *mod/port*]

Syntax Description

ip_addr	(Optional) IP address.
mac_addr	(Optional) MAC address.
vlan *vlan*	(Optional) Specifies the VLAN.
port *mod/port*	(Optional) Specifies the module number and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not enter any arguments of keywords, all DHCP-bindings are cleared.

You should use caution when using this command because clearing a binding can affect Dynamic ARP Inspection (DAI), IP Source Guard, and other features that depend on DHCP snooping.

Examples

This example shows how to clear the DHCP snooping bindings on a specific IP address:

```
Console> (enable) clear dhcp-snooping bindings 172.20.22.191
DHCP Snooping binding entries cleared.
Console> (enable)
```

This example shows how to clear the DHCP snooping bindings on a specific MAC address:

```
Console> (enable) clear dhcp-snooping bindings 0-0-0-0-0-1
DHCP Snooping binding entries cleared.
Console> (enable)
```

This example shows how to clear the DHCP snooping bindings on a specific VLAN:

```
Console> (enable) clear dhcp-snooping bindings vlan 2
DHCP Snooping binding entries cleared.
Console> (enable)
```

This example shows how to clear the DHCP snooping bindings on a specific port:

```
Console> (enable) clear dhcp-snooping bindings port 2/2
DHCP Snooping binding entries cleared.
Console> (enable)
```

Related Commands

set port dhcp-snooping
show dhcp-snooping bindings

clear dhcp-snooping statistics

To clear DHCP snooping statistics, use the **clear dhcp-snooping statistics** command.

clear dhcp-snooping statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you use the **clear dhcp-snooping statistics** command, all statistics except the number of bindings are cleared. To clear the bindings see the **clear dhcp-snooping bindings** command.

Examples

This example shows how to clear the DHCP snooping statistics:

```
Console> (enable) clear dhcp-snooping statistics
DHCP Snooping statistics cleared
Console> (enable)
```

Related Commands

show dhcp-snooping statistics

clear diagnostic

To clear the online diagnostic test configuration, use the **clear diagnostic** command.

clear diagnostic bootup level

clear diagnostic event-log size

clear diagnostic monitor {**interval module** *mod_num* **test** {**all** | *test_ID_num* | *test_list*} | **module** *mod_num* **test** {**all** | *test_ID_num* | *test_list*} | **syslog**}

clear diagnostic schedule module *mod_num* **test** {**all** | *test_ID_num* | *test_list*} {**port** {*port_num* | *port_range* | **all**} **daily** *hh:mm* | **on month** *days_of_month range_of_years hh:mm* | **weekly day** *hh:mm*}

Syntax Description

bootup level	Restores the diagnostic bootup level to bypass mode.
event-log size	Restores the diagnostic event log size to 500 events (default size).
monitor	Clears diagnostics monitoring.
interval module	Clears online diagnostic monitoring test intervals.
mod_num	Number of the module.
test	Specifies diagnostic tests.
all	Clears all online diagnostic tests.
test_ID_num	Number of a specific online diagnostic test.
test_list	List of tests to be cleared.
module	Disables diagnostic monitoring for a specific module.
syslog	Disables the syslog for online diagnostic tests.
schedule	Clears diagnostic test schedule
port	Specifies the ports on which the online diagnostic tests are run.
port_num	Number of the port.
port_range	Range of ports.
all	Specifies all ports.
daily	Specifies a daily schedule.
hh:mm	Hour and minute.
on	Specifies an absolute schedule.
month	Specifies the month.
days_of_month	Days of the month; valid values are from 1 to 31.
range_of_years	Range of years; valid values are from 1993-2035.
weekly	Specifies a weekly schedule.
day	Specifies a day of the week.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Note GOLD is supported on the Supervisor Engine 720 and the Supervisor Engine 32 only. Earlier diagnostic commands are still supported on the Supervisor Engine 1 and the Supervisor Engine 2.

Examples

This example shows how to clear the bootup online diagnostics level:

```
Console> (enable) clear diagnostic bootup level
Diagnostic level set to bypass
Console> (enable)
```

This example shows how to clear the online diagnostics event log size:

```
Console> (enable) clear diagnostic event-log size
Diagnostic event-log size set to default(500)
Console> (enable)
```

These examples show how to clear the online diagnostics monitoring configuration:

```
Console> (enable) clear diagnostic monitor interval module 7 test 3
Clear diagnostic monitor interval for module 7 test 3
Console> (enable)

Console> (enable) clear diagnostic monitor module 7 test 1
Module 7 test 1 diagnostic monitor disable.
Console> (enable)

Console> (enable) clear diagnostic monitor syslog
Diagnostic monitor syslog disable.
Console> (enable)
```

This example shows how to clear the online diagnostic scheduling configuration for tests 1 and 2 on module 7:

```
Console> (enable) clear diagnostic schedule module 7 test 1-2 daily 12:12
Clear diagnostic schedule at daily 12:12 for module 7 test 1-2
Console> (enable)
```

Related Commands

diagnostic start
diagnostic stop
set diagnostic bootup level
set diagnostic diagfail-action
set diagnostic event-log size
set diagnostic monitor
set diagnostic ondemand
set diagnostic schedule
show diagnostic

clear dot1x config

To disable 802.1X on all ports and return values to the default settings, use the **clear dot1x config** command.

clear dot1x config

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to disable 802.1X and return values to the default settings:

```
Console> (enable) clear dot1x config
This command will disable Dot1x and take values back to factory default.

Do you want to continue (y/n) [n]? y
Dot1x config cleared.
Console> (enable)
```

Related Commands

set port dot1x
show dot1x
show port dot1x

clear dot1x vlan-group

To clear a VLAN from a VLAN group, use the **clear dot1x vlan-group** command.

clear dot1x vlan-group {**all** | *vlan_group_name* [*vlan* | **all**]}

Syntax Description

all	Clears all 802.1X VLAN groups.
vlan_group_name	802.1X VLAN group to be cleared.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
all	(Optional) Clears all VLANs from the 802.1X VLAN group.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Types

Privileged.

Usage Guidelines

When an existing VLAN is cleared from the VLAN group name, none of the ports authenticated in the VLAN are cleared, but the mappings are removed from the existing VLAN group.

If you clear the last VLAN from the VLAN group name, the VLAN group is deleted.

You can clear a VLAN group even when active VLANs are mapped to the group. When a VLAN group is cleared, none of the ports or users that are in the authenticated state in any VLAN within the group are cleared, but the VLAN mappings to the VLAN group are cleared.

If you enter the **clear dot1x vlan-group** *vlan_group_name* command without a *vlan* value or the **all** keyword, the entire VLAN group is cleared.

Examples

This example shows how to clear a VLAN from a VLAN group:

```
Console> (enable) clear dot1x vlan-group engg-dept 4
Vlan 4 is successfully cleared from vlan group engg-dept
Console> (enable)
```

This example shows the message that displays when you clear the last VLAN from a VLAN group:

```
Console> (enable) clear dot1x vlan-group engg-dept 3
No active vlans are mapped to this vlan group engg-dept, Clearing this vlan group
Console> (enable)
```

This example shows how to clear an entire VLAN group:

```
Console> (enable) clear dot1x vlan-group engg-dept all
Dot1x vlan group engg-dept is cleared.
Console> (enable)
```

Related Commands

set dot1x
show dot1x

clear eou

To clear the Extensible Authentication Protocol over User Datagram Protocol (EoU) configuration, use the **clear eou** command.

clear eou all

clear eou config

clear eou authorize ip *ip_addr* [*ip_mask*] **policy** *policy_name*

clear eou authorize mac-address *mac_addr* [*mac_mask*] **policy** *policy_name*

clear eou clientless {**password** | **username**}

clear eou host {*ip_addr* | *mac_addr*}

clear eou max-retry

clear eou ratelimit

clear eou timeout {**aaa** | **hold-period** | **retransmit** | **revalidate** | **status-query**}

Syntax Description

all	Clears EoU sessions for all hosts.
config	Disables EoU on all ports and restores EoU parameters back to factory defaults.
authorize	Clears EoU authorization information.
ip	Clears the specified IP from the exception list.
ip_addr	IP address to be cleared.
ip_mask	(Optional) IP mask to be cleared.
policy	Clears a specified policy name.
policy_name	Policy name.
mac-address	Clears the specified MAC address.
mac_addr	MAC address to be cleared.
mac_mask	(Optional) MAC mask to be cleared.
clientless	Clears clientless password or username.
password	Clears the password.
username	Clears the username.
host	Clears the EoU session for the specified host.
max-retry	Clears maximum number of reattempts on a global basis.
ratelimit	Clears rate limit value on a global basis.
timeout	Restores timeout values to their default values on a global basis.
aaa	Clears EoU AAA timeout value.
hold-period	Clears EoU hold-period value.
retransmit	Clears EoU retransmit value.

revalidate	Clears EoU revalidate value.
status-query	Clears EoU status-query value.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear EoU sessions for all hosts:

```
Console> (enable) clear eou all
EOU sesssions of all hosts are cleared.
Console> (enable)
```

This example shows how to clear the current EoU configuration and to restore the EoU factory default settings:

```
Console> (enable) clear eou config
This command will disable EoU on all ports and take EoU parameter values back to
factory defaults.
Do you want to continue (y/n) [n]? y
Console> (enable)
```

This example shows how to clear an EOU session for a host with a specified IP address:

```
Console> (enable) clear eou host 9.9.10.10
EOU session of host with IP 9.9.10.10 cleared.
Console> (enable)
```

This example shows how to clear an IP address from an exception group:

```
Console> (enable) clear eou authorize ip 10.1.1.1 255.255.255.240 policy pol1
Cleared host 10.1.1.1 255.255.255.240 from exception group and removed its policy mapping.
Console> (enable)
```

Related Commands

set eou
clear eou
set security acl ip
show eou
show port eou

clear ethernet-cfm

To clear Connectivity Fault Management (CFM) parameters, use the **clear ethernet-cfm** command.

clear ethernet-cfm continuity-check level *level* **vlan** *vlan*

clear ethernet-cfm domain *domain_name* **level** *level*

clear ethenet-cfm vlan *vlan* **domain** *domain_name*

Syntax Description

continuity-check	Clears CFM continuity check information for a specified level.
level *level*	Specifies the maintenance level; valid values are from 0 to 7.
vlan *vlans*	Specifies a VLAN or range of VLANs; valid values are from 1 to 4094.
domain *domain_name*	Clears a CFM domain.
vlan *vlans*	Specifes a VLAN to clear from a domain.
domain *domain_name*	Clears a specified VLAN from the specified domain.

Defaults

This command restores all CFM parameters to their defaults. See the **set** commands in the “Related Commands” section to learn defaults settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

[Need examples.]

clear ftp

To clear File Transfer Protocol (FTP) parameters, use the **clear ftp** command.

clear ftp [**username** | **password**]

Syntax Description

username	(Optional) Clears the username for FTP connections.
password	(Optional) Clears the password for FTP connections.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not enter any keywords, the system clears all FTP parameters.

Examples

This example shows how to clear the username for FTP connections:

```
Console> (enable) clear ftp username
Console> (enable)
```

This example shows how to clear the password for FTP connections:

```
Console> (enable) clear ftp password
Console> (enable)
```

Related Commands

set ftp
show ftp

clear gmrp statistics

To clear all the GMRP statistics information from a specified VLAN or all VLANs, use the **clear gmrp statistics** command.

clear gmrp statistics {*vlan* | **all**}

Syntax Description

vlan	Number of the VLAN; valid values are from 1 to 4094.
all	Specifies all VLANs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear GMRP statistical information from all VLANs:

```
Console> (enable) clear gmrp statistics all
GMRP statistics cleared.
Console> (enable)
```

This example shows how to clear GMRP statistical information from VLAN 1:

```
Console> (enable) clear gmrp statistics 1
GMRP statistics cleared from VLAN 1.
Console> (enable)
```

Related Commands

show gmrp statistics

clear gvrp statistics

To clear all the GVRP statistics information, use the **clear gvrp statistics** command.

clear gvrp statistics {*mod/port* | **all**}

Syntax Description

mod/port	Number of the module and port.
all	Specifies all ports.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear all GVRP statistical information:

```
Console> (enable) clear gvrp statistics all
GVRP statistics cleared for all ports.
Console> (enable)
```

This example shows how to clear GVRP statistical information for module 2, port 1:

```
Console> (enable) clear gvrp statistics 2/1
GVRP statistics cleared on port 2/1.
Console> (enable)
```

Related Commands

set gvrp
show gvrp configuration

clear igmp statistics

To clear IGMP snooping statistical information, use the **clear igmp statistics** command.

clear igmp statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear IGMP statistical information:

```
Console> (enable) clear igmp statistics
IGMP statistics cleared.
Console> (enable)
```

Related Commands

set igmp
show igmp statistics

clear ip alias

To clear IP aliases that were set using the **set ip alias** command, use the **clear ip alias** command.

clear ip alias {*name* | **all**}

Syntax Description

name	IP address alias to delete.
all	Specifies that all previously set IP address aliases be deleted.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to delete a previously defined IP alias named babar:

```
Console> (enable) clear ip alias babar
IP alias deleted.
Console> (enable)
```

Related Commands

set ip alias
show ip alias

clear ip dns domain

To clear the default DNS domain name, use the **clear ip dns domain** command.

clear ip dns domain

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the default DNS domain name:

```
Console> (enable) clear ip dns domain
Default DNS domain name cleared.
Console> (enable)
```

Related Commands

set ip dns domain
show ip dns

clear ip dns server

To remove a DNS server from the DNS server listing, use the **clear ip dns server** command.

clear ip dns server {*ip_addr* | **all**}

Syntax Description

ip_addr	IP address of the DNS server you want to remove. An IP alias or a host name that can be resolved through DNS can also be used.
all	Specifies all the IP addresses in the DNS server listing to be removed.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove the DNS server at IP address 198.92.30.32 from the DNS server listing:

```
Console> (enable) clear ip dns server 198.92.30.32
198.92.30.32 cleared from DNS table.
Console> (enable)
```

This example shows how to remove all DNS servers from the DNS server listing:

```
Console> (enable) clear ip dns server all
All DNS servers cleared
Console> (enable)
```

Related Commands

set ip dns server
show ip dns

clear ip permit

To remove a specified IP address and mask or all IP addresses and masks from the permit list, use the **clear ip permit** command.

clear ip permit all

clear ip permit {*ip_addr*} [*mask*] [**telnet** | **ssh** | **snmp** | **all**]

Syntax Description

ip_addr	IP address to be cleared. An IP alias or a host name that can be resolved through DNS can also be used.
mask	(Optional) Subnet mask of the specified IP address.
telnet	(Optional) Clears the entries in the Telnet permit list.
ssh	(Optional) Clears the entries in the SSH permit list.
snmp	(Optional) Clears the entries in the SNMP permit list.
all	(Optional) Clears all permit lists.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear ip permit all** command clears the permit list but does not change the state of the IP permit feature. A warning is displayed if all IP addresses are cleared from the permit list, and the feature is enabled. If a mask other than the default (255.255.255.255) has been configured, you must provide both the address and mask to clear a specific entry.

If the **telnet**, **ssh**, **snmp**, or **all** keyword is not specified, the IP address is removed from both the SNMP and Telnet permit lists.

Examples

These examples show how to remove IP addresses:

```
Console> (enable) clear ip permit 172.100.101.102
172.100.101.102 cleared from IP permit list.
Console> (enable)

Console> (enable) clear ip permit 172.160.161.0 255.255.192.0 snmp
172.160.128.0 with mask 255.255.192.0 cleared from snmp permit list.
Console> (enable)

Console> (enable) clear ip permit 172.100.101.102 telnet
172.100.101.102 cleared from telnet permit list.
Console> (enable)
Console> (enable) clear ip permit all
IP permit list cleared.
WARNING
IP permit list is still enabled.
Console> (enable)
```

Related Commands

set ip permit
show ip permit

clear ip route

To delete IP routing table entries, use the **clear ip route** command.

clear ip route *destination gateway*

Syntax Description

destination	IP address of the host or network. An IP alias or a host name that can be resolved through DNS can also be used.
gateway	IP address or alias of the gateway router.

Defaults

The default is *destination*. If the destination is not the active default gateway, the actual destination is the default.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to delete the routing table entries using the **clear ip route** command:

```
Console> (enable) clear ip route 134.12.3.0 elvis
Route deleted.
Console> (enable)
```

Related Commands

set ip route
show ip route

clear kerberos clients mandatory

To disable mandatory Kerberos authentication for services on the network, use the **clear kerberos clients mandatory** command.

clear kerberos clients mandatory

Syntax Description

This command has no arguments or keywords.

Defaults

Kerberos clients are not set to mandatory.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not make Kerberos authentication mandatory and Kerberos authentication fails, the application attempts to authenticate users using the default method of authentication for that network service. For example, Telnet prompts for a password.

Examples

This example shows how to clear mandatory Kerberos authentication:

```
Console> (enable) clear kerberos clients mandatory
Kerberos clients mandatory cleared
Console> (enable)
```

Related Commands

set kerberos clients mandatory
show kerberos

clear kerberos credentials forward

To disable credentials forwarding, use the **clear kerberos credentials forward** command.

clear kerberos credentials forward

Syntax Description

This command has no arguments or keywords.

Defaults

The default is forwarding is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you have a ticket granting ticket (TGT) and are authenticated to a Kerberized switch, you can use the TGT to authenticate to a host on the network. If forwarding is not enabled and you try to list credentials after authenticating to a host, the output will show no Kerberos credentials are present.

Examples

This example shows how to disable Kerberos credentials forwarding:

```
Console> (enable) clear kerberos credentials forward
Kerberos credentials forwarding disabled
Console> (enable)
```

Related Commands

set kerberos clients mandatory
set kerberos credentials forward
show kerberos

clear kerberos creds

To delete all the Kerberos credentials, use the **clear kerberos creds** command.

clear kerberos creds

Syntax Description

This command has no arguments or keywords.

Defaults

The command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you have a TGT and are authenticated to a Kerberized switch, you can use the TGT to authenticate to a host on the network.

Examples

This example shows how to delete all Kerberos credentials:

```
Console> (enable) clear kerberos creds
Console> (enable)
```

Related Commands

set kerberos credentials forward
show kerberos

clear kerberos realm

To clear an entry that maps the name of a Kerberos realm to a DNS domain name or a host name, use the **clear kerberos realm** command.

clear kerberos realm {*dns_domain* | *host*} *kerberos_realm*

Syntax Description

dns_domain	DNS domain name to map to a Kerberos realm.
host	IP address or name to map to a Kerberos realm.
kerberos_realm	IP address or name of a Kerberos realm.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can map the name of a Kerberos realm to a DNS domain name or a host name with the **set kerberos realm** command.

Examples

This example shows how to clear an entry mapping a Kerberos realm to a domain name:

```
Console> (enable) clear kerberos realm CISCO CISCO.COM
Kerberos DnsDomain-Realm entry CISCO - CISCO.COM deleted
Console> (enable)
```

Related Commands

set kerberos local-realm
set kerberos realm
show kerberos

clear kerberos server

To clear a specified Key Distribution Center (KDC) entry, use the **clear kerberos server** command.

clear kerberos server *kerberos_realm* {*hostname* | *ip_address*} [*port_number*]

Syntax Description

kerberos_realm	Name of a Kerberos realm.
hostname	Name of the host running the KDC.
ip_address	IP address of the host running the KDC.
port_number	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can specify to the switch which KDC to use in a Kerberos realm. This command clears a server entry from the table.

Examples

This example shows how to clear a KDC server entered on the switch:

```
Console> (enable) clear kerberos server CISCO.COM 187.0.2.1 750
Kerberos Realm-Server-Port entry CISCO.COM-187.0.2.1-750  deleted
Console> (enable)
```

Related Commands

set kerberos server
show kerberos

clear key config-key

To remove a private 3DES key, use the **clear key config-key** command.

clear key config-key *string*

Syntax Description

string	Name of the 3DES key; the name should be no longer than eight bytes.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove a private 3DES key:

```
Console> (enable)  clear key config-key abcd
Kerberos config key deleted
Console> (enable)
```

Related Commands

set key config-key

clear l2protocol-tunnel cos

To clear the Layer 2 protocol tunneling CoS value for all ingress tunneling ports, use the **clear l2protocol-tunnel cos** command.

clear l2protocol-tunnel cos

Syntax Description

This command has no arguments or keywords.

Defaults

The CoS value is restored to **5**.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the Layer 2 protocol tunneling CoS value:

```
Console> (enable) clear l2protocol-tunnel cos
Default Cos set to 5.
Console> (enable)
```

Related Commands

clear l2protocol-tunnel statistics
set l2protocol-tunnel cos
set port l2protocol-tunnel
show l2protocol-tunnel statistics
show port l2protocol-tunnel

clear l2protocol-tunnel statistics

To clear Layer 2 protocol tunneling statistics on a port or on all tunneling ports, use the **clear l2protocol-tunnel statistics** command.

clear l2protocol-tunnel statistics [*mod/port*]

Syntax Description

mod/port	(Optional) Number of the module and port on the module. See the "Usage Guidelines" section for more information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a module and port number, the Layer 2 protocol tunneling statistics for all tunneling ports and all VLANs are cleared.

Examples

This example shows how to clear the Layer 2 protocol tunneling statistics for a single port:

```
Console> (enable) clear l2protocol-tunnel statistics 7/1
Layer 2 Protocol Tunneling statistics cleared on port 7/1.
Console> (enable)
```

Related Commands

clear l2protocol-tunnel cos
set l2protocol-tunnel cos
set port l2protocol-tunnel
show l2protocol-tunnel statistics
show port l2protocol-tunnel

clear lacp-channel statistics

To clear Link Aggregation Control Protocol (LACP) statistical information, use the **clear lacp-channel statistics** command.

clear lacp-channel statistics

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

For differences between PAgP and LACP, refer to the “Guidelines for Port Configuration” section of the “Configuring EtherChannel” chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example shows how to clear LACP statistical information:

```
Console> (enable) clear lacp-channel statistics
LACP channel counters are cleared.
Console> (enable)
```

Related Commands

set channelprotocol
set lacp-channel system-priority
set port lacp-channel
set spantree channelcost
set spantree channelvlancost
show lacp-channel
show port lacp-channel

clear lda

To remove the accelerated server load balancing (ASLB) multilayer switching (MLS) entries or MAC addresses from the switch, use the **clear lda** command.

clear lda mls

clear lda mls [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol* **src-port** *src_port* **dst-port** *dst_port*]

clear lda vip {**all** | *vip* | *vip tcp_port*}

clear lda mac {**all** | *router_mac_address*}

Syntax Description

mls	Removes a LocalDirector Accelerator (LDA) MLS entry.
destination *ip_addr_spec*	(Optional) Full destination IP address or a subnet address in these formats: *ip_addr*, *ip_addr/netmask,* or *ip_addr/maskbit*.
source *ip_addr_spec*	(Optional) Full source IP address or a subnet address in these formats: *ip_addr*, *ip_addr/netmask,* or *ip_addr/maskbit*.
protocol *protocol*	(Optional) Specifies additional flow information (protocol family and protocol port pair) to be matched; valid values include **tcp**, **udp**, **icmp**, or a decimal number for other protocol families.
src-port *src_port*	(Optional) Specifies the number of the TCP/UDP source port (decimal). Used with **dst-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates “do not care.”
dst-port *dst_port*	(Optional) Specifies the number of the TCP/UDP destination port (decimal). Used with **src-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates “do not care.”
vip all	Removes all VIP couples (set using the **set lda** command).
vip *vip*	Specifies a VIP.
vip *vip tcp_port*	Specifies a VIP and port couple.
mac all	Clears all ASLB router MAC addresses.
mac *router_mac_address*	Clears a specific router MAC address.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported only on switches configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card).

Entering the **destination** keyword specifies the entries matching the destination IP address specification, entering the **source** keyword specifies the entries matching the source IP address specification, and entering an *ip_addr_spec* can specify a full IP address or a subnet address. If you do not specify a keyword, it is treated as a wildcard, and all entries are displayed.

When entering the *ip_addr_spec*, use the full IP address or a subnet address in one of the following formats: *ip_addr, ip_addr/netmask,* or *ip_addr/maskbit*.

If you do not enter any keywords, the LD is removed from the switch, and the LD configuration is removed from NVRAM.

If you do not enter any keywords with the **clear lda mls** command, all ASLB MLS entries are cleared.

Examples

This example shows how to clear the ASLB MLS entry at a specific destination address:

```
Console> (enable) clear lda mls destination 172.20.26.22
MLS IP entry cleared.
Console> (enable)
```

This example shows how to delete a VIP and port pair (VIP 10.0.0.8, port 8):

```
Console> (enable) clear lda vip 10.0.0.8 8
Successfully deleted vip/port pairs.
Console> (enable)
```

This example shows how to clear all ASLB router MAC addresses:

```
Console> (enable) clear lda mac all
Successfully cleared Router MAC address.
Console> (enable)
```

This example shows how to clear a specific ASLB router MAC address:

```
Console> (enable) clear lda mac 1-2-3-4-5-6
Successfully cleared Router MAC address.
Console> (enable)
```

Related Commands

commit lda
set lda
show lda

clear localuser

To delete a local user account from the switch, use the **clear localuser** command.

clear localuser *name*

Syntax Description

name	Specifies the local user account.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to delete a local user account:

```
Console> (enable) clear localuser troy
Local user cleared.
Console> (enable)
```

Related Commands

set localuser
show localuser

clear log

To delete module, system error log, or dump log entries, use the **clear log** command.

clear log [*mod*]

clear log dump

Syntax Description

mod	(Optional) Module number.
dump	Clears dump log entries.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a module number, the system error log for the entire system is erased.

Examples

This example shows how to clear the system error log:

```
Console> (enable) clear log
System error log cleared.
Console> (enable)
```

This example shows how to clear the dump log:

```
Console> (enable) clear log dump
Console> (enable)
```

Related Commands

show log

clear log command

To clear the command log entry table, use the **clear log command** command.

clear log command [*mod*]

Syntax Description

mod	(Optional) Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The command log entry table is a history log of the commands sent to the switch from the console or Telnet.

Examples

This example shows how to clear the command log table for the switch:

```
Console> (enable) clear log command
Local-log cleared
Console> (enable)
```

This example shows how to clear the command log table for the supervisor engine:

```
Console> (enable) clear log command 5
Module 5 log cleared.
Console> (enable)
```

Related Commands

show log command

clear logging buffer

To clear the system logging buffer, use the **clear logging buffer** command.

clear logging buffer

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the system logging buffer:

```
Console> (enable) clear logging buffer
System logging buffer cleared.
Console> (enable)
```

Related Commands

show logging buffer

clear logging callhome

To retore the CallHome default values or to clear a destination address used in the CallHome feature, use the **clear logging callhome** command.

clear logging callhome all

clear logging callhome destination {*E_addr* | **all**}

Syntax Description

all	Restores default values for CallHome functionality.
destination	Clears destination address for CallHome messages.
E_addr	E-mail or E-pager address to receive syslog messages.
all	Clears all destination addresses.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to restore all default values for CallHome functionality:

```
Console> (enable) clear logging callhome all
Removed all addresses from the callhome destination address table.
Cleared the from address field of callhome messages.
Cleared the reply-to address field of callhome messages.
Cleared callhome severity level to its default value of 2 (LOG_CRIT).
Removed all IP address from the callhome SMTP server table.
Callhome functionality is disabled.
Console> (enable)
```

This example shows how to clear the destination address **adminboss@cisco.com** from the list of addresses receiving CallHome messages:

```
Console> (enable) clear logging callhome destination adminboss@cisco.com
Removed adminboss@cisco.com from the table of callhome destination addresses.
Console> (enable)
```

This example shows how to clear all destination addresses from the list of addresses receiving CallHome messages:

```
Console> (enable) clear logging callhome destination all
Removed all addresses from the callhome destination address table.
Console> (enable)
```

Related Commands

clear logging callhome from
clear logging callhome reply-to
clear logging callhome severity
clear logging callhome smtp-server
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome severity
set logging callhome smtp-server
show logging callhome
show logging callhome destination

clear logging callhome from

To clear the From address used by the CallHome feature, use the **clear logging callhome from** command.

clear logging callhome from

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the From address:

```
Console> (enable) clear logging callhome from
Cleared the from address field of callhome messages.
Console> (enable)
```

Related Commands

clear logging callhome
clear logging callhome reply-to
clear logging callhome severity
clear logging callhome smtp-server
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome severity
set logging callhome smtp-server
show logging callhome
show logging callhome from

clear logging callhome reply-to

To clear the Reply-to address used by the CallHome feature, use the **clear logging callhome reply-to** command.

clear logging callhome reply-to

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the Reply-to address:

```
Console> (enable) clear logging callhome reply-to
Cleared the reply-to address field of callhome messages.
Console> (enable)
```

Related Commands

clear logging callhome
clear logging callhome from
clear logging callhome severity
clear logging callhome smtp-server
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome severity
set logging callhome smtp-server
show logging callhome
show logging callhome reply-to

clear logging callhome severity

To clear the severity level used by the CallHome feature and return it to the default value of 2, use the **clear logging callhome severity** command.

clear logging callhome severity

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the CallHome severity:

```
Console> (enable) clear logging callhome severity
Cleared callhome severity level to its default value of 2(LOG_CRIT).
Console> (enable)
```

Related Commands

clear logging callhome
clear logging callhome from
clear logging callhome reply-to
clear logging callhome smtp-server
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome severity
set logging callhome smtp-server
show logging callhome
show logging callhome severity
show logging callhome smtp-server

clear logging callhome smtp-server

To clear an SMTP server from the list of CallHome SMTP servers, use the **clear logging callhome smtp-server** command.

clear logging callhome smtp-server {*IP_addr* | **all**}

Syntax Description

IP_addr	IP address of the SMTP server.
all	Clears all IP addresses.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the SMTP server 172.20.8.16 from the list of CallHome servers:

```
Console> (enable) clear logging callhome smtp-server 172.20.8.16
Removed 172.20.8.16 from the table of callhome SMTP servers.
Console> (enable)
```

This example shows how to clear all IP addresses from the list of CallHome servers:

```
Console> (enable) clear logging callhome smtp-server all
Removed all addresses from the callhome SMTP server table.
Console> (enable)
```

Related Commands

clear logging callhome
clear logging callhome from
clear logging callhome reply-to
clear logging callhome severity
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome severity
set logging callhome smtp-server
show logging callhome
show logging callhome smtp-server

clear logging level

To reset the logging level for a facility or for all facilities to their default settings, use the **clear logging level** command.

clear logging level {*facility* | **all**}

Syntax Description

facility	Name of the facility to reset; facility types are listed in Table 2-1.
all	Resets all facilities.

Table 2-1 Facility Types

Facility Name	Definition
all	All facilities
acl	access control list
cdp	Cisco Discovery Protocol
cops	Common Open Policy Service Protocol
dtp	Dynamic Trunking Protocol
dvlan	Dynamic VLAN
earl	Enhanced Address Recognition Logic
filesys	file system facility
gvrp	GARP VLAN Registration Protocol
ip	Internet Protocol
kernel	Kernel
ld	ASLB facility
mcast	Multicast
mgmt	Management
mls	Multilayer Switching
pagp	Port Aggregation Protocol
protfilt	Protocol Filter
pruning	VTP pruning
privatevlan	Private VLAN facility
qos	Quality of Service
radius	Remote Access Dial-In User Service
rsvp	ReSerVation Protocol
security	Security
snmp	Simple Network Management Protocol

Table 2-1 Facility Types (continued)

Facility Name	Definition
spantree	Spanning Tree Protocol
sys	System
tac	Terminal Access Controller
tcp	Transmission Control Protocol
telnet	Terminal Emulation Protocol
tftp	Trivial File Transfer Protocol
udld	User Datagram Protocol
vmps	VLAN Membership Policy Server
vtp	Virtual Terminal Protocol

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to reset a specific facility back to its default settings:

```
Console> (enable) clear logging level dtp
Current session and default severities of facility <dtp> set to factory default values.
Console> (enable)
```

This example shows how to reset all facilities back to their default settings:

```
Console> (enable) clear logging level all
Current session and default severities of all facilities set to factory default values.
Console> (enable)
```

Related Commands

set logging level
show logging

clear logging server

To delete a syslog server from the system log server table, use the **clear logging server** command.

clear logging server *ip_addr*

Syntax Description

ip_addr	IP address of the syslog server to be deleted.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to delete a syslog server from the configuration:

```
Console> (enable) clear logging server 171.69.192.207
System log server 171.69.192.207 removed from system log server table.
Console> (enable)
```

Related Commands

set logging server
show logging

clear macro

To clear user-defined SmartPorts macros, use the **clear macro** command.

clear macro name *macro_name*

clear macro all

clear macro variable {**all** | *variable_name* [*mod/port*]}

Syntax Description

name	Clears a user-defined SmartPorts macro.
macro_name	Name of the macro.
all	Clears all user-defined SmartPorts macros.
variable	Clears a user-defined SmartPorts variable.
all	Clears all user-defined variables on all ports.
variable_name	Name of the variable.
mod/port	(Optional) Number of the module and the port on the module.

Command Default

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you clear a macro using the **clear macro name** *name_of_macro* command, you clear the commands from the macro and remove the macro from the switch. The configurations that were applied using the macro that is being cleared are retained. If the macro that is being cleared is using any variables, and if the variables are not being used by any other macros, the variables are automatically cleared.

Examples

This example shows how to clear a specific macro and its variables (when those variables are not used by other macros):

```
Console> (enable) clear macro name videophone

Clearing macro videophone....
Cleared Macro videophone ....
Console> (enable)
```

This example shows how to clear all macros and their variables:

```
Console> (enable) clear macro all

Clearing all macros....
All macros are cleared
Console> (enable)
```

This example shows a specific variable from all ports:

```
Console> (enable) clear macro variable $DATAVLAN

Clearing variable $DATAVLAN for all mod/ports...

Deleting Variable: DATAVLAN ...
Cleared variable DATAVLAN
Console> (enable)
```

This example shows how to clear a specific macro from a specific port:

```
Console> (enable) clear macro variable $AUXVLAN 3/7

Clearing variable $AUXVLAN for mod/port.3/7..
Console> (enable)
```

This example shows how to clear all macro variables from all ports:

```
Console> (enable) clear macro variable all

Clearing all variables for all mod/ports...

All variables in the switch are cleared
Console> (enable)
```

Related Commands

set macro
set port macro
show macro

clear mls cef

To clear Cisco Express Forwarding (CEF) summary statistics, use the **clear mls cef** command.

clear mls cef

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported on Catalyst 6500 series switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to clear CEF summary information:

```
Console> (enable) clear mls cef
CEF statistics cleared.
Console> (enable)
```

Related Commands

show mls cef summary

clear mls cef rpf statistics

To clear the counters for packets and bytes that failed the hardware RPF check, use the **clear mls cef rpf statistics** command.

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command only clears the counters related to the hardware RPF check. To configure RPF, you must access the CLI on the MSFC. For more information about accessing the CLI on the MSFC, refer to the "Command Line Interface" chapter of the *Catalyst 6500 Series MSFC Cisco IOS Command Reference, 12.2SX*.

Examples

This example shows how to clear MLS CEF RPF statistics:

```
Console> (enable) clear mls cef rpf statistics
RPF statistics cleared.
Console> (enable)
```

Related Commands

show mls cef rpf

clear mls entry

To clear MLS entries in the Catalyst 6500 series switches, use the **clear mls entry** command.

clear mls entry [**ip** | **ipx**] **all**

clear mls entry ip destination *ip_addr_spec* [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*]

clear mls entry ipx destination *ipx_addr_spec*

Syntax Description

ip	(Optional) Specifies IP MLS.
ipx	(Optional) Specifies IPX MLS.
all	Clears all MLS entries.
destination	Specifies the destination IP address.
ip_addr_spec	Full IP address or a subnet address in these formats: *ip_addr, ip_addr/netmask,* or *ip_addr/maskbit*.
source *ip_addr_spec*	(Optional) Specifies the source IP address.
protocol *protocol*	(Optional) Specifies additional flow information (protocol family and protocol port pair) to be matched; valid values are 0 to 255 or **ip**, **ipinip**, **icmp**, **igmp**, **tcp**, and **udp**.
src-port *src_port*	(Optional) Specifies the source port IP address; valid values are 1 to 65535, **dns**, **ftp**, **smtp**, **telnet**, **x** (X-Windows), **www**.
dst-port *dst_port*	(Optional) Specifies the destination port IP address; valid values are 1 to 65535, **dns**, **ftp**, **smtp**, **telnet**, **x** (X-Windows), **www**.
ipx_addr_spec	Full IPX address or a subnet address in these formats: *src_net/*[*mask*], *dest_net.dest_node,* or *dest_net/mask*.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2). To clear entries on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2), you must enter the **clear mls entry cef** command.

When entering the IPX address syntax, use the following format:

- IPX net address—1..FFFFFFFE
- IPX node address—x.x.x where x is 0..FFFF
- IPX address—ipx_net.ipx_node (for example 3.0034.1245.AB45, A43.0000.0000.0001)

Up to 16 routers can be included explicitly as MLS-RPs.

To use a router as an MLS, you must meet these conditions:

- The router must be included (either explicitly or automatically) in the MLS-SE.
- The MLS feature must be enabled in the Catalyst 6500 series switches.
- The Catalyst 6500 series switches must know the router's MAC-VLAN pairs.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the short subnet address format. The trailing decimal number 00 in an IP address YY.YY.YY.00 specifies the boundary for an IP subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 173.24.00.00/255.255.0.0). However, this format can identify only a subnet address of 8, 16, or 24 bits.
- *ip_addr/subnet_mask*—This is the long subnet address format. For example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip_addr* is a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip_addr* is a full host address, such as 193.22.253.1/22, which has the same subnet address as the *ip_subnet_addr*.

If you do not use the **all** argument in the **clear mls entry** command, you must specify at least one of the other three keywords (**source**, **destination**, or **protocol**) and its arguments.

If no value or 0 is entered for *src_port* and *dest_port*, all entries are cleared.

When you remove a Multilayer Switch Module (MSM) from the Catalyst 6500 series switch, it is removed immediately from the inclusion list and all the MLS entries for the MSM are removed.

Examples

This example shows how to clear the MLS entries with destination IP address 172.20.26.22:

```
Console> (enable) clear mls entry destination 172.20.26.22
Multilayer switching entry cleared.
Console> (enable)
```

This example shows how to clear specific IP MLS entries for destination IP address 172.20.26.22:

```
Console> (enable) clear mls entry ip destination 172.20.26.22 source 172.20.22.113 protocol tcp 520 320
Multilayer switching entry cleared
Console> (enable)
```

This example shows how to clear specific IPX MLS entries for a destination IPX address:

```
Console> (enable) clear mls entry ipx destination 1.00e0.fefc.6000 source 3.0034.1245.AB45
IPX Multilayer switching entry cleared
Console> (enable)
```

Related Commands

show mls entry

clear mls entry cef

To clear CEF adjacency statistics, use the **clear mls entry cef** command.

clear mls entry cef adjacency

clear mls entry cef ip [[*ip_addr*]/*mask_len*] **adjacency**

clear mls entry cef ipx [[*ipx_addr*]/*mask_len*] **adjacency**

Syntax Description

ip	Specifies IP entries.
ipx	Specifies IPX entries.
ip_addr	(Optional) IP address of the entry.
/mask_len	(Optional) Mask length associated with the IP or IPX address of the entry; valid values are from 0 to 32.
ipx_addr	(Optional) IPX address of the entry.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported on Catalyst 6500 series switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2).

To clear MLS entries on systems configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card), enter the **clear mls entry** command.

The *ipx_addr* value is entered as 32-bit hexadecimal digits.

Examples

This example shows how to clear all adjacencies associated with CEF entries:

```
Console> (enable) clear mls cef entry adjacency
Adjacency statistics has been cleared.
Console> (enable)
```

Related Commands

show mls entry cef

clear mls exclude protocol

To remove a protocol port that has been excluded from shortcutting using the **set mls exclude protocol** command, use the **clear mls exclude protocol** command.

clear mls exclude protocol tcp | udp | both *port*

Syntax Description

tcp	Specifies a TCP port.
udp	Specifies a UDP port.
both	Specifies that the port be applied to both TCP and UDP traffic.
port	Number of the port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set TCP packets in a protocol port to be hardware switched:

```
Console> (enable) clear mls exclude protocol tcp 25
TCP packets with protocol port 25 will be MLS switched.
Console> (enable)
```

Related Commands

set mls exclude protocol
show mls exclude protocol

clear mls multicast statistics

To remove MLS multicast statistics maintained by the MSFC on the switch, use the **clear mls multicast statistics** command.

clear mls multicast statistics [*mod*]

Syntax Description

mod	(Optional) Number of the MSFC; valid values are **15** and **16**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter the **clear mls multicast statistics** command on a Catalyst 6500 series switch without MLS, this warning message is displayed:

```
MLS Multicast is not supported on feature card.
```

If you place the MFSC on a supervisor engine installed in slot 1, the MFSC is recognized as module 15. If you install the supervisor engine in slot 2, the MFSC is recognized as module 16.

The *mod* option is not supported on switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2).

Examples

This example shows how to clear MLS statistics on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card):

```
Console> (enable) clear mls multicast statistics
All statistics for the MLS routers in include list are cleared.
Console> (enable)
```

This example shows how to clear MLS statistics on a switch configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> (enable) clear mls multicast statistics
All statistics cleared.
Console> (enable)
```

Related Commands

set port vlan-mapping
show mls statistics

clear mls nde

To clear primary and secondary NDE collector destinations and to disable NDE, use the **clear mls nde** command.

clear mls nde [*IP_address port*]

Syntax Description

IP_address	(Optional) IP address of a specific NDE collector destination.
port	(Optional) Port of a specific NDE collector destination.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Entering the **clear mls nde** command without an IP address and port number clears both primary and secondary NDE collector destinations and disables NDE. To clear a specific NDE collector destination, you must specify an IP address and port for the destination. If the IP address does not specify a valid NDE collector destination, the command is rejected.

Examples

This example shows how to clear both the primary and secondary collectors:

```
Console> (enable) clear mls nde
Collector’s IP address cleared.
Secondary Collector IP address cleared.
Console> (enable)
```

This example shows how to clear a specific collector destination:

```
Console> (enable) clear mls nde 10.6.1.10 9939
Cleared Collector IP 10.6.1.10 port 9939
Console> (enable)
```

This example shows the message that displays when the IP address does not specify a valid NDE collector destination:

```
Console> (enable) clear mls nde 10.6.1.10 1111
Specified address not a valid collector
Console> (enable)
```

Related Commands

set mls nde
show mls nde

clear mls nde flow

To reset the NDE filters in the Catalyst 6500 series switches, use the **clear mls nde flow** command.

clear mls nde flow

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Clearing both exclusion and inclusion filters results in exporting of all flows.

Examples

This example shows how to clear the NDE exclusion and inclusion filters and export all flows:

```
Console> (enable) clear mls nde flow
Netflow data export filter cleared.
Console> (enable)
```

Related Commands

set mls nde
show mls exclude protocol

clear mls statistics

To clear hardware-installed MLS statistics entries, use the **clear mls statistics** command.

clear mls statistics

clear mls statistics protocol {*protocol port*} | **all**

Syntax Description

statistics	Clears total packets switched and total packets exported (for NDE).
statistics protocol	Clears protocols for statistics collection.
protocol	Number of the protocol in the protocol statistics list.
port	Number of the port.
all	Clears all entries from the statistics protocol list.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To use a router as an MLS, you must meet these conditions:

- The router must be included (either explicitly or automatically) in the MLS-SE.
- The MLS feature must be enabled in the Catalyst 6500 series switches.
- Catalyst 6500 series switches must know the MAC-VLAN pairs on the router.

If you enter any of the **clear mls statistics** commands on a Catalyst 6500 series switch without MLS, this warning message displays:

```
Feature not supported in hardware.
```

When you remove an MSM from the Catalyst 6500 series switch, it is removed immediately from the inclusion list and all the MLS entries for the MSM are removed.

Examples

This example shows how to clear IP MLS statistics, including total packets switched and total packets exported (for NDE):

```
Console> (enable) clear mls statistics
Netflow data export statistics cleared.
Console> (enable)
```

This example shows how to clear protocol 17, port 19344 from the statistics collection:

```
Console> (enable) clear mls statistics protocol 17 19344
Protocol 17 port 1934 cleared from protocol statistics list.
Console> (enable)
```

Related Commands

set mls statistics protocol
show mls statistics

clear mls statistics entry

To clear statistics for MLS entries, use the **clear mls statistics entry** command.

clear mls statistics entry [**ip** | **ipx**] **all**

clear mls statistics entry ip [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*]
[**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*]

clear mls statistics entry ipx destination *ipx_addr_spec*

Syntax Description

ip	(Optional) Specifies IP MLS.
ipx	(Optional) Specifies IPX MLS.
all	Purges all matching MLS entries.
destination	(Optional) Specifies the destination IP address.
ip_addr_spec	(Optional) Full IP address or a subnet address in these formats: *ip_addr, ip_addr/netmask,* or *ip_addr/maskbit*.
source	(Optional) Specifies the source IP address.
protocol *protocol*	(Optional) Specifies additional flow information (protocol family and protocol port pair) to be matched; valid values are from 0 to 255 or **ip**, **ipinip**, **icmp**, **igmp**, **tcp**, and **udp**.
src-port *src_port*	(Optional) Specifies the source port IP address; valid values are from 1 to 65535, **dns**, **ftp**, **smtp**, **telnet**, **x** (X-Windows), **www**.
dst-port *dst_port*	(Optional) Specifies the destination port IP address; valid values are from 1 to 65535, **dns**, **ftp**, **smtp**, **telnet**, **x** (X-Windows), **www**.
ipx_addr_spec	Full IPX address or a subnet address in these formats: *src_net/*[*mask*], *dest_net.dest_node,* or *dest_net/mask*.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you specify the **ip** keyword or do not enter a keyword, the command supports IP MLS. If you specify the **ipx** keyword, the command supports IPX only.

When you remove an MSM from the Catalyst 6500 series switch, it is removed immediately from the inclusion list and all the MLS entries for the MSM are removed.

When entering the IPX address syntax, use the following format:

- IPX net address—1..FFFFFFFE
- IPX node address—x.x.x where x is 0..FFFF
- IPX address—ipx_net.ipx_node (for example 3.0034.1245.AB45, A43.0000.0000.0001)

Up to 16 routers can be included explicitly as MLS-RPs.

To use a router as an MLS, you must meet these conditions:

- The router must be included (either explicitly or automatically) in the MLS-SE.
- The MLS feature must be enabled in the Catalyst 6500 series switches.
- Catalyst 6500 series switches must know the router's MAC-VLAN pairs.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the short subnet address format. The trailing decimal number 00 in an IP address YY.YY.YY.00 specifies the boundary for an IP subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 173.24.00.00/255.255.0.0). However, this format can identify only a subnet address of 8, 16, or 24 bits.
- *ip_addr/subnet_mask*—This is the long subnet address format. For example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip_addr* is a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip_addr* is a full host address, such as 193.22.253.1/22, which has the same subnet address as the *ip_subnet_addr*.

A 0 value for *src_port* and *dest_port* clears all entries. Unspecified options are treated as wildcards, and all entries are cleared.

If you enter any of the **clear mls** commands on a Catalyst 6500 series switch without MLS, this message is displayed:

```
Feature not supported in hardware.
```

Examples

This example shows how to clear all specific MLS entries:

```
Console> (enable) clear mls statistics entry ip all
Multilayer switching entry cleared
Console> (enable)
```

This example shows how to clear specific IPX MLS entries for a destination IPX address:

```
Console> (enable) clear mls statistics entry ipx destination 1.0002.00e0.fefc.6000
MLS IPX entry cleared.
Console> (enable)
```

Related Commands

show mls

clear module password

To clear the password set by the **password** *username* NAM command, use the **clear module password** command.

clear module password *mod*

Syntax Description

mod	Number of the NAM.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported by the NAM only.

The **password** *username* command is a NAM command and not a supervisor engine console command.

A message is displayed when the password is successfully cleared. See the "Examples" section for an example of the message.

Examples

This example shows how to clear the password from the NAM:

```
Console> (enable) clear module password 6
Module 6 password cleared.
Console> (enable) 2000 Apr 07 11:03:06 %SYS-5-MOD_PASSWDCLR:Module 6 password cl
eared from telnet/10.6.1.10/tester
Console> (enable)
```

Related Commands

password (Refer to the *NAM Installation and Configuration Note.*)

clear msfcautostate

To clear the MSFC autostate configuration, use the **clear msfcautostate** command.

clear msfcautostate {**all** | *mod/ports*}

Syntax Description

all	Clears the MSFC autostate configuration on all ports.
mod/ports	Module numbers and port numbers for which the MSFC autostate configuration is cleared.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear all MSFC autostate configurations:

```
Console> (enable) clear msfcautostate all
Console> (enable)
```

This example shows how to clear the MSFC autostate configuration on a specific port:

```
Console> (enable) clear msfcautostate 3/1
MSFC autostate config cleared on excluded port 3/1
Console> (enable)
```

Related Commands

set msfcautostate
show msmautostate

clear multicast router

To clear manually configured multicast router ports from the multicast router port list, use the **clear multicast router** command.

clear multicast router {*mod/port* | **all**}

Syntax Description

mod/port	Number of the module and the port on the module.
all	Specifies all multicast router ports to be cleared.

Defaults

The default configuration has no multicast router ports configured.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear multicast router port 1 on module 3:

```
Console> (enable) clear multicast router 3/1
Port 3/1 cleared from multicast router port list.
Console> (enable)
```

Related Commands

set multicast router
show multicast router

clear ntp server

To remove one or more servers from the NTP server table, use the **clear ntp server** command.

clear ntp server {*ip_addr* | **all**}

Syntax Description

ip_addr	IP address of the server to remove from the server table.
all	Specifies all server addresses in the server table to be removed.

Defaults

The default configuration has no NTP servers configured.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove a specific NTP server from the server table:

```
Console> (enable) clear ntp server 172.20.22.191
NTP server 172.20.22.191 removed.
Console> (enable)
```

This example shows how to remove all NTP servers from the server table:

```
Console> (enable) clear ntp server all
All NTP servers cleared.
Console> (enable)
```

Related Commands

set ntp server
show ntp

clear ntp timezone

To return the time zone to its default, UTC, use the **clear ntp timezone** command.

clear ntp timezone

Syntax Description

This command has no arguments or keywords.

Defaults

The default time zone is UTC.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear ntp timezone** command functions only when NTP is running. If you set the time manually and NTP is disengaged, the **clear ntp timezone** command has no effect.

Examples

This example shows how to clear the time zone:

```
Console> (enable) clear ntp timezone
This command will clear NTP timezone and summertime zonename
Do you want to continue (y/n) [n]? y
Timezone name and offset cleared
Console> (enable)
```

Related Commands

set ntp timezone
show ntp

8.6 EFT Copy

clear pbf

To remove the MAC address for the PFC2, use the **clear pbf** command.

clear pbf

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Refer to the “Configuring Policy-Based Forwarding” section of Chapter 16, “Configuring Access Control,” in the *Catalyst 6500 Series Switch Software Configuration Guide* for detailed information about PBF.

Examples

```
Console> (enable) clear pbf
PBF cleared
Console> (enable)
```

Related Commands

set pbf
show pbf

clear packet-capture

To restore packet-capturing settings to their defaults for the Mini Protocol Analyzer feature, use the **clear packet-capture** command.

clear packet-capture {**dump-file** | **filter** | **snap-length** | **limit** | **all**}

Syntax Description

dump-file	Clears the packet-capture file name setting.
filter	Clears the packet-capture filter setting.
snap-length	Clears the packet-capture length setting.
limit	Clears the packet-capture limit setting.
all	Clears all the packet capture settings.

Defaults

This commands has not default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command restores default settings for the Mini Protocol Analyzer feature. See the commands that are listed in the “Related Commands” section for default settings.

Examples

This example shows how to clear the the dump file name:

```
Console> (enable) clear packet-capture dump-file
Packet capture File name cleared.
Console> (enable)
```

This example shows how to clear the packet-capture filter setting:

```
Console> (enable) clear packet-capture filter
Packet-capture filter(s) cleared.
Console> (enable)
```

This example shows how to clear the snap length:

```
Console> (enable) clear packet-capture snap-length
Packet-capture snap length cleared. The complete packet will be captured.
Console> (enable)
```

This example shows how to clear the default setting for the limit:

```
Console> (enable) clear packet-capture limit
Packet-capture limit cleared. Packets will be captured until the
specified flash device is full.
Console> (enable)
```

This example sets the default setting for all the packet capture settings:

```
Console> (enable) clear packet-capture all
Packet-capture settings cleared.
Console> (enable)
```

Related Commands

set packet-capture
set packet-capture dump-file
set packet-capture filter
set packet-capture limit
set packet-capture snap-length
show packet-capture

clear pbf arp-inspection

To clear the ARP-inspection ACE from the ACL for a client list or a gateway, use the **clear pbf arp-inspection** command.

clear pbf arp-inspection *list_name*

Syntax Description

list_name	Client list or gateway list.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If the ARP-inspection ACE is removed from the PBF ACL, the supervisor engine will no longer answer the ARP requests.

Examples

This example shows how to clear the ARP-inspection ACE from the ACL of a client list:

```
Console> (enable) clear pbf arp-inspection cl1
.ccl1 editbuffer modified. Use 'commit' command to save changes.
Console> (enable) ACL commit in progress.

ACL '.ccl1' successfully committed.
Console> (enable)
```

Related Commands

set pbf arp-inspection
show pbf arp-inspection

clear pbf client

To clear a client or all clients from the list, use the **clear pbf client** command.

clear pbf client *client_list* [*ip_addr*]

Syntax Description

client_list	Client list name.
ip_addr	(Optional) IP address.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear pbf client** command can be used only if there is no PBF map in place.

Examples

This example shows how to clear a client list:

```
Console> (enable) clear pbf client cl1
.c0001cl1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) Commit operation successfull.
Console> (enable)
```

This example shows the message that displays if you try to clear a client list when there is a PBF map in place:

```
Console> (enable) clear pbf client cl1
Operation failed: clear pbf-map first.
Console> (enable)
```

Related Commands

clear pbf gw
clear pbf-map
set pbf client
set pbf gw
set pbf-map
show pbf client
show pbf gw
show pbf-map

clear pbf gw

To clear a gateway or all gateways, use the **clear pbf gw** command.

clear pbf gw *gw_name* [*ip_addr*]

Syntax Description

gw_name	Gateway name.
ip_addr	(Optional) IP address.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear pbf gw** command can be used only if there is no PBF map in place.

Examples

This example shows how to clear a gateway list:

```
Console> (enable) clear pbf gw gw1
.g0002gw1 editbuffer modified. Use 'commit' command to apply changes.
Commit operation successfull.
Console> (enable)
```

Related Commands

clear pbf client
clear pbf-map
set pbf client
set pbf gw
set pbf-map
show pbf client
show pbf gw
show pbf-map

clear pbf-map

To clear PBF map information, use the **clear pbf-map** command.

clear pbf-map {**vlan** *vlan*} | **all** | {*ip_addr_1*} {*mac_addr_1*} {*vlan_1*} {*ip_addr_2*} {*mac_addr_2*} {*vlan_2*}

clear pbf-map {*client_list*} {*gw_name*}

Syntax Description

vlan *vlan*	Clears the ACL with the name PBF_MAP_ACL_*vlan* and the adjacency table used by this ACL.
all	Clears all adjacency information and ACLs that were created by entering the **set pbf-map** command.
ip_addr_1	IP address of host 1.
mac_addr_1	MAC address of host 1.
vlan_1	Number of the first VLAN.
ip_addr_2	IP address of host 2.
mac_addr_2	MAC address of host 2.
vlan_2	Number of the second VLAN.
client_list	Client list name.
gw_name	Gateway list name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enter **clear pbf-map** {*ip_addr_1*} {*mac_addr_1*} {*vlan_1*} {*ip_addr_2*} {*mac_addr_2*} {*vlan_2*}, all ACEs that were created by entering the **set pbf-map** command are cleared, except **permit ip any any**. This command removes entries that enable traffic between hosts with ip_addr_1 and ip_addr_2 on the two specified VLANs.

Use the **clear pbf-map** command to delete the redirect-to-adjacency ACEs and adjacency information contained in the PBF_MAP_ACL_(VLAN_ID) ACL.

Use the **clear security acl** command to clear all other ACE types that are part of the PBF_MAP_ACL_*vlan* ACL.

If entries were already deleted by using the **clear security acl** command, a message appears that states that the specified entries were already cleared.

Examples

This example shows how to clear the ACL with the name PBF_MAP_ACL_11:

```
Console> (enable) clear pbf-map vlan 11
ACL 'PBF_MAP_ACL_11' successfully deleted.
Console> (enable) Commit operation successfull.
Console> (enable)
```

This example shows how to clear all adjacency information and ACLs that were created by entering the **set pbf-map** command:

```
Console> (enable) clear pbf-map all
ACL 'PBF_MAP_ACL_11' successfully deleted.
Console> (enable)
ACL 'PBF_MAP_ACL_22' successfully deleted.
Console> (enable)
```

This example shows how to clear all entries that enable traffic between the two specified hosts:

```
Console> (enable) clear pbf-map 1.1.1.1 0-0-0-0-0-1 11 2.2.2.2 0-0-0-0-0-2 22
ACL 'PBF_MAP_ACL_11' successfully committed.
Console> (enable)
ACL 'PBF_MAP_ACL_22' successfully committed.
Console> (enable)
```

This example shows how to clear the PBF mapping:

```
Console> (enable) clear pbf-map cl1 gw1
.ccl1 editbuffer modified. Use 'commit' command to save changes.
.ggw1 editbuffer modified. Use 'commit' command to save changes.
Console> (enable) ACL commit in progress.
Console> (enable) ACL commit in progress.

ACL '.ccl1' successfully deleted.
Console> (enable)
ACL '.ggw1' successfully deleted.
Console> (enable)
```

Related Commands

clear pbf client
clear pbf gw
clear security acl
set pbf client
set pbf gw
set pbf-map
show pbf client
show pbf gw
show pbf-map

clear pbf vlan

To clear PBF-enabled VLANs and remove them from NVRAM, use the **clear pbf vlan** command.

clear pbf vlan *vlan*

Syntax Description

vlan	VLAN number.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Using the **clear pbf** command does not clear the VLANs enabled for PBF. The **clear pbf** command does clear the Layer 2 table entries associated with the VLANs (because the MAC address is no longer valid). You must explicitly clear the PBF-enabled VLANs to remove them from NVRAM by entering the **clear pbf vlan** *vlan* command.

You can specify a range of VLANs in the CLI.

Examples

This example shows how to clear PBF on VLANs 11 and 12:

```
Console> (enable) clear pbf vlan 11-12
PBF disabled on vlan(s) 11-12
Console> (enable)
```

Related Commands

set pbf vlan
show pbf

clear policy

To clear an IP address from a policy group or to clear a policy group from a policy template, use the **clear policy** command.

clear policy group *group_name* **ip-address** *ip_addr*

clear policy name *policy_name* **group** *group_name*

clear policy name *policy_name* **url-redirect**

Syntax Description

group *group_name*	Clears policy group memberships.
ip-address *ip_addr*	Specifies IP address to be cleared from group membership.
name *policy_name*	Clears a policy group from a policy template.
url-redirect	Clears the URL redirect string that is associated with the policy name.

Command Default

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear an IP address from a policy group:

```
Console> (enable) clear policy group grp1 ip-address 100.1.1.1
Cleared IP 100.1.1.1 from policy group grp1.
Console> (enable)
```

This example shows how to clear a policy group from a policy template:

```
Console> (enable) clear policy name pol1 group grp1
Cleared group grp1 from policy template pol1.
Console> (enable)
```

This example shows how to clear the URL redirect string that is associated with a policy name:

```
Console> (enable) clear policy name exception_policy url-redirect
Unmapped Url-redirect http://cisco.com from policy name exception_policy
Console> (enable)
```

Related Commands

set policy
show policy

clear port broadcast

To disable broadcast/multicast suppression on one or more ports, use the **clear port broadcast** command.

clear port broadcast *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

The default configuration has broadcast/multicast suppression cleared (that is, unlimited broadcast/multicast traffic allowed).

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to disable broadcast/multicast suppression:

```
Console> (enable) clear port broadcast 2/1
Broadcast traffic unlimited on ports 2/1.
Console> (enable)
```

Related Commands

set port broadcast
show port broadcast

clear port cops

To clear port roles, use the **clear port cops** command.

clear port cops *mod/port* **roles** *role1* [*role2*]...

clear port cops *mod/port* **all-roles**

Syntax Description

mod/port	Number of the module and the port on the module.
roles *role#*	Specifies the roles to clear.
all-roles	Clears all roles.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear port cops** command detaches the roles from the port only; it does not remove them from the global table.

Examples

This example shows how to remove specific roles from a port:

```
Console> (enable) clear port cops 3/1 roles backbone_port main_port
Roles cleared for port(s) 3/1-4.
Console> (enable)
```

This example shows how to remove all roles from a port:

```
Console> (enable) clear port cops 3/1 all-roles
All roles cleared for port 3/1-4.
Console> (enable)
```

Related Commands

set port cops
show port cops

clear port eou

To clear the mapping of an AAA fail policy for EoU on a specified port, use the **clear port eou** command.

clear port eou *mod*[/*port*] **aaa-fail-policy**

Syntax Description

mod[/*port*]	Number of the module and optionally, the port on the module.
aaa-fail-policy	Clears the mapping of a AAA fail policy.

Defaults

This command has not default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear an AAA fail policy on module 5, port 10:

```
Console> (enable) clear port eou 5/10 aaa-fail-policy
aaa-fail-policy cleared successfully on port 5/10
Console> (enable)
```

Related Commands

set port eou
show port eou

clear port ethernet-cfm

To clear the MEPs or MIPs for a specific port, use the **clear port ethernet-cfm** command.

clear port ethernet-cfm *mod/port* **mep level** *level* [**vlan** *vlan*]

clear port ethernet-cfm *mod/port* **mip**

Syntax Description

mod/port	Number of the module and the port on the module.
mep	Clears the Maintenance End Point (MEP) counfiguration on the specified port.
level *level*	Clears the specified maintenance level; valid values are from 0 to 7.
vlan *vlan*	(Optional) Clears the specified VLAN; valid values are from 1 to 4094.
mip	Clears the Maintenance Intermediate Point (MIP) configuration.

Defaults

[What are the defaults restored to? Does **set port ethernet-cfm** have default settings?]

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example clears the MEP configuration for module 2, port 1 with a maintenance level of 4:

```
Console> (enable) clear port ethernet-cfm 2/1 mep level 4
MEP config on Port 2/1 is cleared.
Console> (enable)
```

This example clears the MIP configuration for module 6, port 1:

```
Console> (enable) clear port ethernet-cfm 2/1 mip
MIP config on Port 6/1 is cleared.
Console> (enable)
```

clear port ethernet-oam

To clear the IEEE 802.3ah Operations, Administrations, and Maintenance (OAM) configuration on a specified port, use the **clear port ethernet-oam** command.

clear port ethernet-oam [*mod/port*]

clear port ethernet-oam [*mod/port*] **statistics**

clear port ethernet-oam *mod/port* {**critical-event** | **link-fault**} **action**

clear port ethernet-oam *mod/port* **link-monitor** {**frame** | **frame-period** | **symbol-period**}

{**window** | **low-threshold** | **high-threshold**}

Syntax Description

mod/port	Number of the module and the port on the module.
statistics	Clears OAM-related statistics.
critical-event	Clears the critical-event configuration.
link-fault	Clears the link-fault configuration.
action	Clears the specified action (critical-event or link-fault).
link-monitor	Clears the link-monitor configuration.
frame	Specifies monitoring by the number of frames with errors.
frame-period	Specifies monitoring by frame period.
symbol-period	Specifies monitoring by the number of symbols with errors.
window	Clears monitoring window.
low-threshold	Clears the low threshold and the corresponding action.
high-threshold	Clears the high threshold and the corresponding action.

Command Default

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter the **clear port ethernet-oam** *mod/port* without the **statistics** keyword, all OAM-related configurations are cleared on the specified ports. If you do not specify a port, all OAM-related configurations are cleared on all ports.

If you enter the **statistics** keyword, OAM-related counters are cleared on the specified port. If you do not specify a port, all OAM-related counters are cleared on all ports.

When you enter the **low-threshold** keyword or the **high-threshold** keyword, the corresponding associated action is also cleared.

Examples

This example shows how to clear OAM-related statistics on a specified port:

```
Console> (enable) clear port ethernet-oam 1/1 statistics
OAM counters cleared on port 1/1.
Console> (enable)
```

This example shows how to clear the high-threshold configuration for frame-period link monitoring:

```
Console> (enable) clear port ethernet-oam 1/1 link-monitor frame-period high-threshold
OAM errored frame period high-threshold set to default on port 1/1, and action set to
default.
Console> (enable)
```

This example shows how to clear the action that a specified port takes in response to a link fault:

```
Console> (enable) clear port ethernet-oam 1/1 link-fault action
OAM link-fault event action set to default.
Console> (enable)
```

Related Commands

set port ethernet-oam
set port ethernet-oam action
set port ethernet-oam link-monitor
set port ethernet-oam mode
set port ethernet-oam remote-loopback
show port ethernet-oam

clear port flexlink

To clear an active-backup (peer) Flexlink pair of ports, use the **clear port flexlink** command.

clear port flexlink *mod/port* [**peer** *mod/port*]

Syntax Description

mod/port	Number of the module and the port on the module.
peer	(Optional) Specifies the peer port for the Flexlink active port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear port 3/48 as the Flexlink active port and port 3/47 as the Flexlink backup (peer) port:

```
Console> (enable) clear port flexlink 3/48 peer 3/47
Port 3/48 and 3/47 flexlink pair cleared
Console> (enable)
```

Related Commands

set port flexlink
show port flexlink

clear port host

To clear the port configuration for optimizing a host connection, use the **clear port host** command.

clear port host *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

The **clear port host** command sets channel mode to auto, disables spanning tree PortFast, and sets the trunk mode to auto.

Examples

This example shows how to remove specific roles from a port:

```
Console> (enable) clear port host 5/5
Port(s)  5/5 trunk mode set to auto.
Spantree port  5/5 fast start disabled.
Port(s) 5/5 channel mode set to auto.
Console> (enable)
```

Related Commands

set port host

clear port qos autoqos

To clear the automatic QoS configuration on a per-port basis, use the **clear port qos autoqos** command.

clear port qos *mod/ports..* **autoqos**

Syntax Description

mod/ports..	Number of the module and ports on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged mode.

Usage Guidelines

The **clear port qos autoqos** command is supported on all ports supporting port-based automatic QoS **set** commands. All QoS settings configured through the automatic QoS port-based command revert back to factory default settings, except for QoS ACLs. QoS ACLs created for automatic QoS purposes are cleared through the global **clear** command.

All QoS ACLs mapped to the port are unmapped from the port, even if the QoS ACL is not related to automatic QoS.

Examples

This example shows how to clear the automatic QoS configuration on module 3, port 1:

```
Console> (enable) clear port qos 3/1 autoqos
Port based QoS settings will be restored back to factory defaults for port 3/1.
Do you want to continue (y/n) [n]? y
Port 3/1 autoqos settings have been cleared.
It is recommended to execute the "clear qos autoqos" global command if
not executed previously to clear global autoqos settings.
Console> (enable)
```

Related Commands

clear qos autoqos
set port qos autoqos
set qos autoqos
show port qos
show qos info

clear port qos cos

To return the values set by the **set port qos cos** command to the default settings for all specified ports, use the **clear port qos cos** command.

clear port qos *mod/ports..* **cos**

Syntax Description

mod/ports..	Number of the module and ports on the module.

Defaults

The default CoS for a port is 0.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to return the values set by the **set port qos cos** command to the default settings for module 2, port 1:

```
Console> (enable) clear port qos 2/1 cos
Port 2/1 qos cos setting cleared.
Console> (enable)
```

Related Commands

set port qos cos
show port qos

clear port security

To clear all MAC addresses or a specific MAC address from the list of secure MAC addresses on a port, use the **clear port security** command.

clear port security *mod/port mac_addr* [**all** | *vlan_list*]

clear port security *mod/port* **all** [*vlan_list*]

Syntax Description

mod/port	Number of the module and the port on the module.
mac_addr	MAC address to be deleted.
all	(Optional) Clears secure MAC address for all VLANs on the port.
vlan_list	(Optional) List of VLANs for which the secure MAC address is cleared.
all	Clears all secure MAC addresses for the port.
vlan_list	(Optional) List of VLANs for which all secure MAC addresses are cleared.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A secure MAC address can be part of different VLANs on a single port. The **clear port security** *mod/port mac_addr* [**all** | *vlan_list*] command allows you to clear a secure MAC address on all the VLANs of the port by entering the **all** keyword or on a set of VLANs by entering a *vlan_list* argument. If you do not enter the **all** keyword or a *vlan_list* argument, the secure MAC address is cleared on the native VLAN of the port, if a native VLAN exists.

The **clear port security** *mod/port* **all** [*vlan_list*] command allows you to clear all secure MAC addresses on either a per-VLAN basis or a per-port basis. If you enter the **clear port security** *mod/port* **all** command but do not enter a *vlan_list* argument, all secure MAC address on the port are cleared.

Examples

This example shows how to remove a specific MAC address from a list of secure addresses on the port:

```
Console> (enable) clear port security 4/1 00-11-22-33-44-55
00-11-22-33-44-55 cleared from secure address list list for port 4/1.
Console> (enable)
```

This example shows how to remove a secure MAC address from a list of VLANs:

```
Console> (enable) clear port security 3/37 00-00-aa-00-00-aa 20,30
Secure MAC address 00-00-aa-00-00-aa cleared for port 3/37 and Vlan 20.
Secure MAC address 00-00-aa-00-00-aa cleared for port 3/37 and Vlan 30.
Console> (enable)
```

This example shows how to remove a secure MAC address for all VLANs on a port:

```
Console> (enable) clear port security 3/37 00-00-aa-00-00-aa all
Secure MAC address 00-00-aa-00-00-aa cleared for port 3/37 and Vlan 1.
Secure MAC address 00-00-aa-00-00-aa cleared for port 3/37 and Vlan 20.
Secure MAC address 00-00-aa-00-00-aa cleared for port 3/37 and Vlan 30.
Console> (enable)
```

This example shows what happens if you clear a secure MAC address without specifying the **all** keyword or a specific list of VLANs. The MAC address is cleared on the native VLAN.

```
Console> (enable) clear port security 3/37 00-00-aa-00-00-aa
Secure MAC address 00-00-aa-00-00-aa cleared for port 3/37 and Vlan 1.
Console> (enable)
```

This example shows how to remove all secure MAC addresses from a specific VLAN:

```
Console> (enable) clear port security 3/37 all 20
All secure mac addresses cleared on port 3/37 for vlan 20.
Console> (enable)
```

Related Commands

set port security
show port security

clear port vlan-mapping

To clear the VLAN mapping on a per-port basis, use the **clear port vlan-mapping** command.

clear port vlan-mapping {**all** | *mod/port* {*source_vlan_id* | **all**}}

Syntax Description

all	Clears VLAN mappings for all ports.
mod/port	Number of the module and the port on the module.
source_vlan_id	Number of the source VLAN; valid values are from 1 to 4094.
all	Clears VLAN mappings for the specified port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

On some modules, VLAN mapping is supported on a per-ASIC basis; the mapping is not stored on a per-port basis. For these modules, entering **clear port vlan-mapping** *mod/port* clears the VLAN mapping on all ports on the ASIC.

When you enter a *source_vlan_id* argument, only the VLAN mapping for that source VLAN is cleared from the VLAN mapping table of the specified port or ASIC (if the port is an ASIC-based port).

Examples

This example shows how to clear the VLAN mapping for a specified port:

```
Console> (enable) clear port vlan-mapping 7/1 2002
VLAN mapping for VLAN 2002 removed from port 7/1-12.
Console> (enable)
```

Related Commands

set port vlan-mapping
show port vlan-mapping

8.6 EFT Copy

clear port web-auth

To clear the mapping of an AAA fail policy for web-based authentication proxy on a specified port, use the **clear port web-auth** command.

clear port web-auth *mod*[/*port*] **aaa-fail-policy**

Syntax Description

mod[/*port*]	Number of the module and optionally, the port on the module.
aaa-fail-policy	Clears the mapping of a AAA fail policy.

Defaults

This command has not default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear an AAA fail policy on module 5, port 10:

```
Console> (enable) clear port web-auth 5/10 aaa-fail-policy
aaa-fail-policy cleared successfully on port 5/10
Console> (enable)
```

Related Commands

set port web-auth
show port web-auth

clear pvlan mapping

To delete a private VLAN mapping, use the **clear pvlan mapping** command.

clear pvlan mapping *primary_vlan* {*isolated_vlan* | *community_vlan* | *twoway_community_vlan*} *mod/port*

clear pvlan mapping *mod/port*

Syntax Description

primary_vlan	Number of the primary VLAN.
isolated_vlan	Number of the isolated VLAN.
community_vlan	Number of the community VLAN.
twoway_community_vlan	Number of the two-way community VLAN.
mod/port	Number of the module and promiscuous port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify the mapping to clear, all the mappings of the specified promiscuous ports are cleared.

Examples

This example shows how to clear the mapping of VLAN 902 to 901, previously set on ports 3/2-5:

```
Console> (enable) clear pvlan mapping 901 902 3/2-5
Successfully cleared mapping between 901 and 902 on 3/2-5
Console> (enable)
```

Related Commands

clear config pvlan
clear vlan
set pvlan
set pvlan mapping
set vlan
show pvlan
show pvlan mapping
show vlan

clear qos acl

To remove various ACL configurations, use the **clear qos acl** command.

clear qos acl *acl_name* [*editbuffer_index*]

clear qos acl default-action {**ip** | **ipx** | **mac** | **all**}

clear qos acl map {*acl_name*} {*mod/port* | *vlan*} [**input**]

clear qos acl map {*acl_name* | *mod/port* | *vlan* | **all**} [**input**]

clear qos acl map {*acl_name*} {*vlan* | **all**} **output**

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
editbuffer_index	(Optional) ACE position in the ACL.
default-action	Removes default actions.
ip	Clears IP ACE default actions.
ipx	Clears IPX ACE default actions.
mac	Clears MAC-layer ACE default actions.
all	Clears all ACE default actions.
map	Detaches an ACL.
mod/port	Number of the module and the port on the module.
vlan	Number of the VLAN; valid values are from 1 to 4094.
all	Detaches an ACL from all interfaces.
input	(Optional) Removes the ACL from the ingress interface. See the “Usage Guidelines” section for more information.
output	Removes the ACL from the egress interface.

Defaults

The default is no ACLs are attached.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Changes you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command.

Use the **show qos acl editbuffer** command to display the ACL list.

If you do not specify a direction keyword (**input** or **output**), the system automatically specifies **input**.

Examples

This example shows how to detach an ACL from all interfaces:

```
Console> (enable) clear qos acl map my_acl all
Hardware programming in progress...
ACL my_acl is detached from all interfaces.
Console> (enable)
```

This example shows how to detach an ACL from a specific VLAN:

```
Console> (enable) clear qos acl map ftp_acl 4
Hardware programming in progress...
ACL ftp_acl is detached from vlan 4.
Console> (enable)
```

This example shows how to delete a specific ACE:

```
Console> (enable) clear qos acl my_ip_acl 1
ACL my_ip_acl ACE# 1 is deleted.
my_ip_acl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

This example shows how to delete an ACL:

```
Console> (enable) clear qos acl my_ip_acl
ACL my_ip_acl is deleted.
my_ip_acl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

This example shows how to detach a specific ACL from all interfaces:

```
Console> (enable) clear qos acl map my_acl all
Hardware programming in progress...
ACL my_acl is detached from all interfaces.
Console> (enable)
```

This example shows how to detach a specific ACL from a specific VLAN:

```
Console> (enable) clear qos acl map ftp_acl 4
Hardware programming in progress...
ACL ftp_acl is detached from vlan 4.
Console> (enable)
```

This example shows how to delete IP ACE default actions configured by the **set qos acl default-action** command:

```
Console> (enable) clear qos acl default-action ip
Hardware programming in progress...
QoS default-action for IP ACL is restored to default setting.
Console> (enable)
```

This example shows how to clear Qos ACL mapping between an ACL named “test” and VLAN 1 on the ingress interface:

```
Console> (enable) clear qos acl map test 1
Successfully cleared mapping between ACL test and VLAN 1 on input side.
Console> (enable)
```

This example shows how to clear QoS ACL mapping between an ACL named “test2” and VLAN 1 on the egress interface:

```
Console> (enable) clear qos acl map test2 1 output
Successfully cleared mapping between ACL test2 and VLAN 1 on output side.
Console> (enable)
```

Related Commands	
	commit rollback set qos acl map show qos acl editbuffer

clear qos autoqos

To return the global automatic QoS configuration to the factory default settings, use the **clear qos autoqos** command.

Syntax Description

This command has no arguments or keywords.

Defaults

This commands has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

QoS ACLs created through the **set port autoqos** commands are cleared through the global automatic **clear qos autoqos** command. Also, any policers used by automatic QoS ACLs are cleared.

The global automatic QoS **clear** command searches for automatic QoS ACL names. The search algorithm looks for names beginning with the following strings:

- ACL_IP-PHONES (for ciscoipphone)
- ACL_IP-SOFTPHONE (for ciscosoftphone)
- ACL_IP-TRUSTCOS (for trust cos)
- ACL_IP-TRUSTDSCP (for trust dscp)

Any QoS ACL starting with the above strings is considered an automatic QoS ACL and is cleared. If one is found and the QoS ACL is committed and not mapped to a port or a VLAN, it is deleted.

Similarly, the search algorithm looks for aggregate QoS policers starting with this name:

POLICE_SOFTPHONE-DSCP (for ciscosoftphone).

The global **clear** command searches for aggregate policer names that begin with POLICE_SOFTPHONE-DSCP. If a policer is found, and there is no QoS ACL associated with it, it is deleted. If a policer is found, and there is a QoS ACL associated with it, a warning is displayed indicating the policer is still in use.

Various error conditions can occur when the global **clear** command is used. If you have properly executed the port-based **clear** commands before using the global **clear** command, no error conditions should occur. However, if you execute the global **clear** command first or have modified the automatic QoS configuration, the following error conditions could occur:

- Automatic QoS ACLs still mapped to a port or VLAN

  The global **clear** command will not clear automatic QoS ACLs that are still mapped to a VLAN or port. Instead, it displays a warning indicating the name of the QoS ACL still mapped to a port or VLAN.

- Aggregate policers still in use

  If the automatic QoS policers found are still in use (referenced by a QoS ACL), the global **clear** command does not remove them. Instead, it displays the name of the aggregate policer.

- Uncommitted automatic QoS ACLs

  The global **clear** command only removes committed automatic QoS ACLs; it ignores uncommitted automatic QoS ACLS.

Examples

This example shows how to return the global automatic QoS configuration to the factory default settings:

```
Console> (enable) clear qos autoqos
Its highly recommended to execute clear port autoqos commands prior
to the global clear command:
    clear port qos <mod/port> autoqos

Do you want to continue (y/n) [n]? y
........................
Autoqos ACL 'ACL_IP-SOFTPHONE-3-1' successfully deleted.
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP46-3-1'
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP26-3-1'

All ingress and egress QoS scheduling parameters set to factory default.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps
configured.  Global Autoqos QoS cleared.
Console> (enable)
```

This example shows what is displayed under the various error conditions described in the “Usage Guidelines” section:

```
Console> (enable) clear qos autoqos
Its highly recommended to execute clear port autoqos commands prior
to the global clear command:
    clear port qos <mod/port> autoqos

Do you want to continue (y/n) [n]? y
........................
Autoqos ACL 'ACL_IP-SOFTPHONE-3-2' successfully deleted.
Autoqos ACL 'ACL_IP-SOFTPHONE-3-3' successfully deleted.
Autoqos ACL 'ACL_IP-SOFTPHONE-3-4' still mapped to port or vlan.
Autoqos ACL 'ACL_IP-SOFTPHONE-3-5' still mapped to port or vlan.
Autoqos ACL 'ACL_IP-SOFTPHONE-3-6' still mapped to port or vlan.
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP46-3-2'
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP26-3-2'
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP46-3-3'
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP26-3-3'
Could not clear Autoqos policer ''POLICE_SOFTPHONE-DSCP46-3-4', still in use.
QoS is disabled.
```

```
All ingress and egress QoS scheduling parameters set to factory default.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps
configured.  Global Autoqos QoS cleared.
Console> (enable)
```

Related Commands

clear port qos autoqos
set port qos autoqos
set qos autoqos
show port qos
show qos info

clear qos config

To return the values that were set by the **set qos** command to the default settings and delete the CoS assigned to MAC addresses, use the **clear qos config** command.

Syntax Description

This command has no arguments or keywords.

Defaults

The default is QoS is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to return the values set by the **set qos** command to the default settings and delete the CoS assigned to MAC addresses:

```
Console> (enable) clear qos config
This command will disable QoS and take values back to factory default.
Do you want to continue (y/n) [n]? y
QoS config cleared.
Console> (enable)
```

Related Commands

set qos
show qos info

clear qos cos-cos-map

To return the CoS-to-CoS map to the default setting, use the **clear qos cos-cos-map** command.

clear qos cos-cos-map

Syntax Description

This command has no arguments or keywords.

Defaults

The default CoS-to-CoS configuration is listed in Table 2-2.

Table 2-2 CoS-to-CoS Mapping

CoS	0	1	2	3	4	5	6	7
CoS	0	1	2	3	4	5	6	7

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The CoS-to-CoS map is also restored to the default configuration when you enter the **clear config** command or the **clear qos config** command.

Examples

This example shows how to clear the CoS-to-CoS map:

```
Console> (enable) clear qos cos-cos-map
QoS cos-cos-map setting restored to default.
Console> (enable)
```

Related Commands

set qos cos-cos-map
show qos maps

clear qos cos-dscp-map

To clear CoS-to-DSCP mapping set by the **set qos cos-dscp-map** command and return to the default setting, use the **clear qos cos-dscp-map** command.

clear qos cos-dscp-map

Syntax Description

This command has no arguments or keywords.

Defaults

The default CoS-to-DSCP configuration is listed in Table 2-3.

Table 2-3 CoS-to-DSCP Default Mapping

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the CoS-to-DSCP mapping table:

```
Console> (enable) clear qos cos-dscp-map
QoS cos-dscp-map setting restored to default.
Console> (enable)
```

Related Commands

set qos cos-dscp-map
show qos maps

clear qos dscp-cos-map

To clear DSCP-to-CoS mapping set by the **set qos dscp-cos-map** command and return to the default setting, use the **clear qos dscp-cos-map** command.

clear qos dscp-cos-map

Syntax Description

This command has no arguments or keywords.

Defaults

The default DSCP-to-CoS configuration is listed in Table 2-4.

Table 2-4 DSCP-to-CoS Default Mapping

DSCP	0 to 7	8 to 15	16 to 23	24 to 31	32 to 39	40 to 47	48 to 55	56 to 63
CoS	0	1	2	3	4	5	6	7

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the DSCP-to-CoS mapping table:

```
Console> (enable) clear qos dscp-cos-map
QoS dscp-cos-map setting restored to default.
Console> (enable)
```

Related Commands

set qos dscp-cos-map
show qos maps

clear qos dscp-mutation-map

To clear DSCP mutation mapping, use the **clear qos dscp-mutation-map** command.

clear qos dscp-mutation-map {*mutation_table_id* | **all**}

Syntax Description

mutation_table_id	Number of the mutation table to be cleared; valid values are from 1 to 15.
all	Clears all mutation mapping.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is available only on PFC3.

Examples

This example shows how to clear all VLANs in the mutation map with mutation table number 2:

```
Console> (enable) clear qos dscp-mutation-map 2
All VLANS in mutation-table-id 2 are cleared.
Console> (enable)
```

Related Commands

clear qos dscp-mutation-table-map
set qos dscp-mutation-map
set qos dscp-mutation-table-map
show qos maps

clear qos dscp-mutation-table-map

To clear the DSCP mutation table map, use the **clear qos dscp-mutation-table-map** command.

clear qos dscp-mutation-table-map {**all** | *vlan* | {**id** *mutation_table_id*}}

Syntax Description

all	Clears all VLANs from DSCP mutation table mapping.
vlan	Numbers of the VLANs to be cleared from DSCP mutation table mapping.
id *mutation_table_id*	Clears a specified DSCP mutation table; valid values are from 1 to 15.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is available only on PFC3.

Examples

This example shows how to clear VLANs 3 through 33 from the mutation tables:

```
Console> (enable) clear qos dscp-mutation-table-map 3-33
VLAN(s) 3-33 are removed from mutation-id-maps.
Console> (enable)
```

This example shows how to clear all VLANs from the mutation tables:

```
Console> (enable) clear qos dscp-mutation-table-map all
All VLANs are removed from mutation-id-maps.
Console> (enable)
```

This example shows how to clear mutation table 3:

```
Console> (enable) clear qos dscp-mutation-table-map id 3
QoS dscp-mutation-map for mutation-table-id 3 is restored to default.
Console> (enable)
```

Related Commands

clear qos dscp-mutation-map
set qos dscp-mutation-map
set qos dscp-mutation-table-map
show qos maps

clear qos ipprec-dscp-map

To reset the mapping set by the **set qos ipprec-dscp-map** command to the default setting, use the **clear qos ipprec-dscp-map** command.

clear qos ipprec-dscp-map

Syntax Description

This command has no arguments or keywords.

Defaults

The default IP precedence-to-DSCP configuration is listed in Table 2-5.

Table 2-5 IP Precedence-to-DSCP Default Mapping

IPPREC	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the IP precedence-to-DSCP mapping table:

```
Console> (enable) clear qos ipprec-dscp-map
QoS ipprec-dscp-map setting restored to default.
Console> (enable)
```

Related Commands

set qos ipprec-dscp-map
show qos maps

8.6 EFT Copy

clear qos mac-cos

To clear the values set by the **set qos mac-cos** command, use the **clear qos mac-cos** command.

clear qos mac-cos *dest_mac* [*vlan*]

clear qos mac-cos all

Syntax Description

dest_mac	Number of the destination host MAC address.
vlan	(Optional) Number of the VLAN; valid values are from 1 to 4094.
all	Clears CoS values for all MAC/VLAN pairs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If the *vlan* value is not entered, all entries for the MAC address are cleared.

Examples

This example shows how to clear the values set by the **set qos mac-cos** command and return to the default settings for all MAC address and VLAN pairs:

```
Console> (enable) clear qos mac-cos all
All CoS to Mac/Vlan entries are cleared.
Console> (enable)
```

This example shows how to clear the values set by the **set qos mac-cos** command and return to the default settings for a specific MAC address:

```
Console> (enable) clear qos mac-cos 1-2-3-4-5-6 1
CoS to Mac/Vlan entry for mac 01-02-03-04-05-06 vlan 1 is cleared.
Console> (enable)
```

Related Commands

set qos mac-cos
show qos mac-cos

clear qos map

To return the values to the default settings, use the **clear qos map** command.

clear qos map *port_type* **tx** | **rx**

Syntax Description

port_type	Port type; valid values are **2q2t**, **1p3q1t**, and **1p2q2t** for transmit and **1p1q4t** and **1p1q0t** for receive. See the "Usage Guidelines" section for additional information.
tx | **rx**	Specifies the transmit or receive queue.

Defaults

The default mappings for all ports are shown in Table 2-6 and Table 2-7 and apply to all ports.

Table 2-6 Default Transmit Queue and Drop-Threshold Mapping of CoS Values

Port Type	Drop Threshold Type	Low Delay (Queue 2)	High Delay (Queue 1)	Priority Delay (Queue 3)
2q2t	Low drop (Threshold 2)	7, 6	3, 2	N/A
	High drop (Threshold 1)	5, 4	1, 0	N/A
1p2q2t	Low drop (Threshold 2)	7	3, 2	N/A
	High drop (Threshold 1)	5, 4	1, 0	5

Table 2-7 Default Receive Drop-Threshold Mapping of CoS Values

Port Type	Threshold 1 (highest drop)	Threshold 2	Threshold 3	Threshold 4 (lowest drop)	Priority Queue
1p1q0t	0, 1	2, 3	4, 5	7	6
1p1q4t	0, 1	2, 3	4, 5	7	6

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **1p2q1t** and **1p1q8t** port types are not supported.

Examples

This example shows how to return the values to the default settings:

```
Console> (enable) clear qos map 2q2t
This command will take map values back to factory default.
QoS map cleared.
Console> (enable)
```

Related Commands

set qos map
show qos maps

clear qos policed-dscp-map

To reset the policer-to-dscp mapping table to the defaults, use the **clear qos policed-dscp-map**.

clear qos policed-dscp-map [**normal-rate** | **excess-rate**]

Syntax Description

normal-rate	(Optional) Restores the map associated with the normal rate to the default value. See the “Usage Guidelines” section for more information.
excess-rate	(Optional) Restores the map associated with the excess rate to the default value.

Defaults

The default is the identity function; for example, DSCP 63 to policed DSCP 63 and DSCP 62 to policed DSCP 62.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify the **normal-rate** keyword or the **excess-rate** keyword, only normal rate mappings are cleared and restored to the default settings.

Examples

This example shows how to reset the normal rate mapping to the default settings:

```
Console> (enable) clear qos policed-dscp-map
QoS normal-rate policed-dscp-map setting restored to default.
Console> (enable)
```

This example shows how to reset the excess rate mapping to the default settings:

```
Console> (enable) clear qos policed-dscp-map excess-rate
QoS excess-rate policed-dscp-map setting restored to default.
Console> (enable)
```

Related Commands

set qos policed-dscp-map
show qos maps

clear qos policer

To clear policing rules from NVRAM, use the **clear qos policer** command.

clear qos policer microflow *microflow_name* | **all**

clear qos policer aggregate *aggregate_name* | **all**

Syntax Description

microflow *microflow_name*	Specifies the name of the microflow policing rule.
aggregate *aggregate_name*	Specifies the name of the aggregate policing rule.
all	Clears all policing rules.

Defaults

This command has no default setting in systems configured with the Supervisor Engine 1 with Layer 3 Switching Engine (PFC); in systems configured with Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2), the default is to apply the given map to the normal rate only.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Policing is the process by which the switch limits the bandwidth consumed by a flow of traffic. Policing can mark or drop traffic.

You cannot clear an entry that is currently being used in an ACE. You must first detach the ACEs from the interface.

You cannot use the **all** keyword if a microflow rate limit is currently being used in an ACE.

The **normal** and **excess** keywords are supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only. With these keywords, you can specify a map for the normal rate and one for the excess rate. Because this selection is optional in the CLI, the default (unspecified) action is to apply the given map to the normal rate only.

Examples

This example shows how to clear a specific microflow policing rule:

```
Console> (enable) clear qos policer microflow my_micro
my_micro QoS microflow policer cleared.
Console> (enable)
```

This example shows how to clear all microflow policing rules:

```
Console> (enable) clear qos policer microflow all
All QoS microflow policers cleared.
Console> (enable)
```

This example shows how to clear a specific aggregate policing rule:

```
Console> (enable) clear qos policer aggregate my_micro
my_micro QoS microflow policer cleared.
Console> (enable)
```

This example shows how to clear all aggregate policing rules:

```
Console> (enable) clear qos policer aggregate all
All QoS aggregate policer cleared.
Console> (enable)
```

Related Commands

set qos policer
show qos policer

clear qos statistics

To clear QoS statistic counters, use the **clear qos statistics** command.

clear qos statistics [**aggregate-policer** [*policer_name*]]

Syntax Description

aggregate-policer	(Optional) Clears QoS aggregate policer statistics.
policer_name	(Optional) Name of the aggregate policer.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter the **clear qos statistics** command without the entering the **aggregate-policer** keyword, all QoS statistics are cleared, including all QoS aggregate policer statistics.

If you enter the **aggregate-policer** keyword without specifying a policer name, all aggregate policer statistics are cleared.

Examples

This example shows how to clear the QoS statistic counters:

```
Console> (enable) clear qos statistics
QoS statistical cleared.
Console> (enable)
```

This example shows how to clear all QoS aggregate policer statistics:

```
Console> (enable) clear qos statistics aggregate-policer
QoS aggregate policers statistical counters cleared.
Console> (enable)
```

This example shows how to clear the QoS aggregate policer statistics for aggr_1:

```
Console> (enable) clear qos statistics aggregate-policer aggr_1
Aggregate policer 'aggr_1' statistical counters cleared.
Console> (enable)
```

Related Commands

show qos statistics

clear radius

To clear one or all of the RADIUS servers from the RADIUS server table or remove a shared key entry, use the **clear radius** command.

clear radius server all

clear radius server *ipaddr*

clear radius key

Syntax Description

server	Specifies RADIUS servers.
all	Specifies all RADIUS servers.
ipaddr	Number of the IP address or IP alias.
key	Specifies the RADIUS shared key.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The *ipaddr* value is an IP alias or an IP address in dot notation; for example, 101.102.103.104.

Examples

This example shows how to clear the RADIUS key:

```
Console> (enable) clear radius key
Radius server key cleared.
Console> (enable)
```

This example shows how to clear a specific RADIUS server from the RADIUS server table:

```
Console> (enable) clear radius server 128.56.45.32
128.56.45.32 cleared from radius server table.
Console> (enable)
```

Related Commands

set radius key
set radius server
show radius

clear rcp

To clear rcp information for file transfers, use the **clear rcp** command.

clear rcp

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear rcp information:

```
Console> (enable) clear rcp
Console> (enable)
```

Related Commands

set rcp username
show rcp

clear rgmp statistics

To clear RGMP statistics information for all VLANs, use the **clear rgmp statistics** command.

clear rgmp statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the RGMP statistics on the switch:

```
Console> (enable) clear rgmp statistics
RGMP statistics cleared.
Console> (enable)
```

Related Commands

set rgmp
show rgmp statistics

clear security acl

To remove a specific access control entry (ACE) or all ACEs from a VACL and to delete the VACLs from the edit buffer, use the **clear security acl** command.

clear security acl all

clear security acl *acl_name*

clear security acl capture-ports {**all** | *mod/ports*}

clear security acl log flow

clear security acl *acl_name* [*editbuffer_index*]

clear security acl adjacency *adjacency_name*

clear security acl map {*acl_name* [*vlan*] | *vlan* | **all**}

clear security acl arp-inspection statistics [*acl_name*]

Syntax Description

all	Removes ACEs for all the VACLs.
acl_name	Name of the VACL whose ACEs are to be removed.
capture-ports	Removes ports from the capture list.
all	Removes all ports from the capture list.
mod/ports	Variable to remove specific port from the capture list; *mod/num* is the number of the module and the port on the module.
log flow	Removes logging table flow entries.
editbuffer_index	(Optional) Index number of the ACE in the VACL.
adjacency	Removes an adjacency ACE.
adjacency_name	Name of the adjacency ACE.
map	Clears security ACL to a VLAN mapping.
vlan	Variable to clear ACL mappings for a specific VLAN.
all	Clears all ACL VLAN mappings.
arp-inspection statistics	Clears ARP inspection statistics.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Changes you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command.

Use the **show security acl** command to display the VACL list.

The adjacency ACE cannot be cleared before the redirect ACE. The redirect ACE and the adjacency ACE in PBF VACLs should be cleared in the following order:

1. Clear the redirect ACE.
2. Commit the VACL.
3. Clear the adjacency ACE.
4. Commit the adjacency.

When you enter the **clear security acl arp-inspection statistics** command, if you do not specify an ACL name, the system clears all counters for ARP inspection global statistics and ARP inspection statistics for all ACLs.

Examples

This example shows how to remove ACEs for all the VACLs:

```
Console> (enable) clear security acl all
All editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

This example shows how to remove a specific ACE from a specific VACL:

```
Console> (enable) clear security acl IPACL1 2
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

This example shows how to remove an adjacency ACE:

```
Console> (enable) clear security acl adjacency a_1
a_1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

This example shows how to clear the ARP inspection global statistics and the ARP inspection statistics for all ACLs:

```
Console> (enable) clear security acl arp-inspection statistics
Console> (enable)
```

Related Commands

commit
rollback
set security acl arp-inspection
show security acl

clear security acl capture-ports

To remove a port from the capture port list, use the **clear security acl capture-ports** command.

clear security acl capture-ports {*mod/ports...*}

Syntax Description

mod/ports...	Number of the module and the ports on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering this command are saved in NVRAM. This command *does not* require that you enter the **commit** command.

If you have several ports and a few are removed, the remaining ports continue to capture the traffic.

Examples

This example shows how to remove entries from the capture port list:

```
Console> (enable) clear security acl capture-ports 1/1,2/1
Successfully cleared the following ports:
1/1,2/1
Console> (enable)
```

Related Commands

set security acl capture-ports
show security acl capture-ports

clear security acl counters

To clear the statistics for all ACEs on all ACLs, use the **clear security acl counters** command.

clear security acl counters

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command clears all statistics counters that were activated by entering the **set security acl statistics** command.

Examples

This example shows how to clear the statistics for all ACEs on all ACLs:

```
Console> (enable) clear security acl counters
Operation Successful.
Console> (enable)
```

Related Commands

clear security acl statistics
set security acl statistics

clear security acl cram

To disable compression and reordering of ACL masks (CRAM) in automatic mode, use the **clear security acl cram** command.

clear security acl cram {**auto**}

Syntax Description

auto	Disables CRAM in automatic mode.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The CRAM feature can be run in automatic or manual mode. The **clear security acl cram auto** command disables automatic mode. Automatic mode executes the CRAM feature whenever the TCAM is full or whenever a specified CRAM timer interval has elapsed.

Entering this command also returns the CRAM timer back to the default timer interval (300 seconds). If you reenable CRAM by entering the **set security acl cram auto** command, the default timer interval takes effect.

Note With software release 8.4(1), the CRAM feature is only supported for security ACLs. The CRAM feature works for QoS ACLs but you cannot specifically run the feature on QoS ACLs.

Examples

This example shows how to disable CRAM in automatic mode:

```
Console> (enable) clear security acl cram auto
Cram auto mode disabled.
Console> (enable)
```

Related Commands

set security acl cram
show security acl cram

clear security acl log flow

To clear all flows in the security ACL log table, use the **clear security acl log flow** command.

clear security acl log flow

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported on systems configured with Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to clear all flows in the security ACL log table:

```
Console> (enable) clear security acl log flow
Security acl log table cleared successfully
Console> (enable)
```

Related Commands

set security acl log
show security acl log

8.6 EFT Copy

clear security acl map

To remove VACL-to-VLAN mapping, use the **clear security acl map** command.

clear security acl map *acl_name vlan*

clear security acl map {*acl_name* | *vlan* | **all**}

Syntax Description

acl_name	Name of the VACL on which a VLAN is to be deleted.
vlan	Number of the VLAN on which a mapping is to be deleted; valid values are from 1 to 4094.
all	Removes all VACL-to-VLAN mappings.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Changes you make by entering this command are saved to NVRAM; you do not need to enter the **commit** command.

Use the **show security acl** command to display the ACL list.

Examples

This example shows how to remove a VACL-to-VLAN mapping from a specific VLAN:

```
Console> (enable) clear security acl map ip1 3
Map deletion in progress.

Successfully cleared mapping between ACL ip1 and VLAN 3.
Console> (enable)
```

This example shows how to remove a specific VACL-to-VLAN mapping from all VLANs:

```
Console> (enable) clear security acl map ip1
Map deletion in progress.

Successfully cleared mapping between ACL ip1 and VLAN 5.

Successfully cleared mapping between ACL ip1 and VLAN 8.
Console> (enable)
```

This example shows how to remove all VACL-to-VLAN mappings from a specific VLAN:

```
Console> (enable) clear security acl map 5
Map deletion in progress.

Successfully cleared mapping between ACL ipx1 and VLAN 5.

Successfully cleared mapping between ACL mac2 and VLAN 5.
Console> (enable)
```

This example shows how to remove all VACL-to-VLAN mappings from all VLANs:

```
Console> (enable) clear security acl map all
Map deletion in progress.

Successfully cleared mapping between ACL ip2 and VLAN 12.

Successfully cleared mapping between ACL ipx1 and VLAN 12.

Successfully cleared mapping between ACL ipx1 and VLAN 45.

Successfully cleared mapping between ACL ip2 and VLAN 47.

Successfully cleared mapping between ACL ip3 and VLAN 56.
Console> (enable)
```

Related Commands

commit
rollback
show security acl

clear security acl statistics

To disable the collection of statistics for all ACEs in a specified ACL, use the **clear security acl statistics** command.

clear security acl statistics *acl_name*

Syntax Description

acl_name	Name of the ACL.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear security acl statistics** command disables the collection of statistics for all ACEs in the ACL that you specify. This command only works for ACL statistics that are configured on a per-ACL basis. The command does not work for ACL statistics configured on a per-VLAN or per-ACE basis. This command is effective only after you enter the **commit** command to commit all ACEs to NVRAM.

Examples

This example shows how to disable the collection of statistics for all ACEs in the specified ACL:

```
Console> (enable) clear security acl statistics ACL1
ACL1 editbuffer modified. Use 'commit' command to save changes.
Console> (enable) commit security acl ACL1
ACL commit in progress.

ACL 'ACL1' successfully committed.
Console> (enable)
```

Related Commands

clear security acl counters
set security acl statistics

clear snmp access

To remove the access rights of an SNMP group, use the **clear snmp access** command.

clear snmp access [**-hex**] {*groupname*} {**security-model** {**v1** | **v2c**}}

clear snmp access {**security-model v3** {**noauthentication** | **authentication** | **privacy**}} [**context** [**-hex**] *contextname*]

Syntax Description

-hex	(Optional) Displays the *groupname* or *contextname* in a hexadecimal format.
groupname	SNMP access table name.
security-model v1 | **v2c**	Specifies the security model v1 or v2c.
security-model v3	Specifies security model v3.
noauthentication	Specifies groups with security model type set to noauthentication.
authentication	Specifies groups with security model type authentication protocol.
privacy	Specifies groups with security model type privacy.
context *contextname*	(Optional) Specifies the name of a context string.

Defaults

The default *contextname* is a NULL string.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *groupname* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

If you do not enter a context name, a NULL context string is used.

Examples

This example shows how to clear SNMP access for a group:

```
Console> (enable) clear snmp access cisco-group security-model v3 authentication
Cleared snmp access cisco-group version v3 level authentication.
Console> (enable)
```

Related Commands

set snmp access
show snmp access
show snmp context

clear snmp access-list

To clear the IP address of a host that is associated with an access list number, use the **clear snmp access-list** command.

clear snmp access-list *access_number IP_address* [[*IP_address*] ...]

Syntax Description

access_number	Number that specifies a list of hosts that are permitted to use a specific community string; valid values are 1 to 65535.
IP_address	IP address that is associated with the access list. See the "Usage Guidelines" section for more information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you specify more than one IP address, separate each IP address with a space.

Examples

This example shows how to clear the IP address of a host from access list number 2:

```
Console> (enable) clear snmp access-list 2 172.20.60.8
Access number 2 no longer associated with 172.20.60.8
Console> (enable)
```

This example shows how to clear all IP address from access list number 101:

```
Console> (enable) clear snmp access-list 101
All IP addresses associated with access-number 101 have been cleared.
Console> (enable)
```

Related Commands

set snmp access-list

clear snmp community

To clear an SNMP community table, use the **clear snmp community** command.

clear snmp community index [**-hex**] {*index_name*}

Syntax Description

index	Specifies clearing an index.
-hex	(Optional) Displays the *index_name* value in a hexadecimal format.
index_name	Name of the SNMP index.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *index_name* value (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

If you do not enter an *index_name* value, a NULL context string is used.

Examples

This example shows how to clear SNMP access for a group:

```
Console> (enable) clear snmp community index ind1
Cleared snmp community ind1.
Console> (enable)
```

Related Commands

set snmp community
show snmp community

8.6 EFT Copy

clear snmp community-ext

To clear an existing community string, use the **clear snmp community-ext** command.

clear snmp community-ext *community_string*

Syntax Description

community_string	Name of the SNMP community.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you clear a community string, corresponding entries in the vacmAccessTable and vacmSecurityToGroup tables are also removed.

Examples

This example shows how to clear an existing community string:

```
Console> (enable) clear snmp community-ext public1
Community string public1 has been removed.
Console>(enable)
```

Related Commands

set snmp community-ext

clear snmp group

To remove the SNMP user from an SNMP group, use the **clear snmp group** command.

clear snmp group [**-hex**] *groupname* {**user** [**-hex**] *username*} {**security-model** {**v1** | **v2c** | **v3**}}

Syntax Description

-hex	(Optional) Displays the *groupname* and *username* as a hexadecimal format.
groupname	Name of the SNMP group that defines an access control.
user	Specifies the SNMP group username.
username	Name of the SNMP user.
security model v1 | **v2c** | **v3**	Specifies security model v1, v2c, or v3.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *groupname* value or the *username* value (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to remove an SNMP user from a group:

```
Console> (enable) clear snmp group cisco-group user joe security-model v3
Cleared snmp group cisco-group user joe version v3.
Console> (enable)
```

Related Commands

set snmp group
show snmp group

clear snmp ifalias

To clear an SNMP interface alias, use the **clear snmp ifalias** command.

clear snmp ifalias {*ifindex* | **all**}

Syntax Description

ifindex	Interface index number.
all	Clears all interface aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear SNMP interface index 1:

```
Console> (enable) clear snmp ifalias 1
Console> (enable)
```

This example shows how to clear all SNMP interface aliases:

```
Console> (enable) clear snmp ifalias all
Console> (enable)
```

Related Commands

set snmp ifalias
show snmp ifalias

clear snmp inform

To clear the SNMP inform request configuration, use the **clear snmp inform** command.

clear snmp inform all

clear snmp inform *rcvr_address*

clear snmp inform index *rcvr_index*

Syntax Description

all	Clears all SNMP inform request receivers and resets the size of the inform request queue to 100.
rcvr_address	IP address or IP alias of the SNMP inform request receiver to be cleared.
index *rcvr_index*	Clears the unique index that corresponds to the specified index number; valid values are from 1 to 65535.

Defaults

When you enter **clear snmp inform all**, the SNMP inform request queue is reset to 100, which is the default size of the queue.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This examples shows how to clear all SNMP inform request receivers and reset the size of the queue to the default:

```
Console> (enable) clear snmp inform all
All SNMP inform receivers cleared.
Size of inform queue has been reset to default.
Console> (enable)
```

Related Commands

set snmp inform
show snmp inform

clear snmp notify

To clear the SNMP notifyname in the snmpNotifyTable, use the **clear snmp notify** command.

clear snmp notify [**-hex**] {*notifyname*}

Syntax Description

-hex	(Optional) Displays the *notifyname* value as a hexadecimal format.
notifyname	Identifier to index the snmpNotifyTable.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *notifyname* value (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to clear an SNMP notifyname from the snmpNotifyTable:

```
Console> (enable) clear snmp notify joe
Cleared SNMP notify table joe.
Console> (enable)
```

Related Commands

set snmp notify
show snmp notify

clear snmp targetaddr

To clear the SNMP target address entry in the TargetAddressTable, use the **clear snmp targetaddr** command.

clear snmp targetaddr [**-hex**] {*addrname*}

Syntax Description

-hex	(Optional) Displays the *addrname* value as a hexadecimal format.
addrname	Name of the target agent; the maximum length is 32 bytes.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *addrname* value (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to clear an SNMP target address entry in the snmpTargetAddressTable:

```
Console> (enable) clear snmp targetaddr joe
Cleared SNMP targetaddr joe.
Console> (enable)
```

Related Commands

set snmp targetaddr
show snmp targetaddr

clear snmp targetparams

To clear the SNMP target parameters used in the snmpTargetParamsTable, use the **clear snmp targetparams** command.

clear snmp targetparams [**-hex**] {*paramsname*}

Syntax Description

-hex	(Optional) Displays the *paramsname* value as a hexadecimal format.
paramsname	Name of the target parameter in the snmpTargetParamsTable; the maximum length is 32 bytes.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *paramsname* value (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to remove the SNMP target parameters:

```
Console> (enable) clear snmp targetparams joe
Cleared SNMP targetparams table joe.
Console> (enable)
```

Related Commands

set snmp targetparams
show snmp targetparams

clear snmp trap

To clear an entry from the SNMP trap receiver table, use the **clear snmp trap** command.

clear snmp trap {*rcvr_addr*} [**all**]

Syntax Description

rcvr_addr	IP address or IP alias of the trap receiver (the SNMP management station) to clear.
all	(Optional) Specifies every entry in the SNMP trap receiver table.

Defaults

The default configuration has no entries in the SNMP trap receiver table.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear an entry from the SNMP trap receiver table:

```
Console> (enable) clear snmp trap 192.122.173.82
SNMP trap receiver deleted.
Console> (enable)
```

Related Commands

set snmp trap
show port counters
test snmp trap

clear snmp user

To remove an SNMP user, use the **clear snmp user** command.

clear snmp user [**-hex**] {*username*} [**remote** *engineid*]

Syntax Description

-hex	(Optional) Displays the *username* value as a hexadecimal format.
username	Name of the user on the host that connects to the agent.
remote *engineid*	(Optional) Specifies the *username* value on a remote SNMP engine.

Defaults

If a remote engine ID is not provided, the default local SNMP engine ID is used.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *username* value (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to remove a user from an SNMP group:

```
Console> (enable) clear snmp user joe
Cleared SNMP user joe.
Console> (enable)
```

This example shows how to remove a user on a remote SNMP engine:

```
Console> (enable) clear snmp user joe remote 00:00:00:09:00:d0:00:4c:18:00
Cleared SNMP user.
Console> (enable)
```

Related Commands

set snmp user
show snmp user

8.6 EFT Copy

clear snmp view

To remove the MIB view entry from the vacmViewTreeFamilyTable, use the **clear snmp view** command.

clear snmp view [**-hex**] {*viewname subtree*}

Syntax Description

-hex	(Optional) Displays the *viewname* value as a hexadecimal format.
viewname	Name of a MIB view.
subtree	Name of the subtree.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *viewname* value (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

A MIB subtree used with a mask defines a view subtree that can be in OID format or a text name mapped to a valid OID.

Examples

This example shows how to clear the SNMP MIB viewname:

```
Console> (enable) clear snmp view myview 1.1.3
Cleared snmp view myview with subtree 1.1.3
Console> (enable)
```

Related Commands

set snmp view
show snmp view

clear spantree detected-protocols

To detect legacy bridges and the boundary ports of the MST region, use the **clear spantree detected-protocols** command.

clear spantree detected-protocols *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module. See "Usage Guidelines" for more information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear spantree detected-protocols** command is available in MST mode and Rapid-PVST+ mode only and is not saved in NVRAM. If you do not specify a *mod/port* number when you enter the **clear spantree detected-protocols** command, protocol detection occurs on all connected ports.

The **clear spantree detected-protocols** command and the **set spantree mst redetect-protocol** command have the same functionality.

Examples

This example shows how to set protocol detection of legacy bridges and boundary ports on port 2 or module 3:

```
Console> (enable) clear spantree detected-protocols 3/2
Spanning tree protocol detection forced on port 3/2
Console> (enable)
```

Related Commands

clear spantree mst
set spantree mode
set spantree mst config

8.6 EFT Copy

clear spantree mst

To clear the mapping of VLANs to an MST instance or to revert a port that is in pre-standard MST mode back to standard MST mode, use the **clear spantree mst** command.

clear spantree mst *instance* [**vlan** *vlans*]

clear spantree mst *mod/port* **pre-std**

Syntax Description

instance	Number of the instance; valid values are from 0 to 4094.
vlan *vlans*	(Optional) Specifies the VLAN number; valid values are from 1 to 4094.
mod/port	Number of the module and the port on the module
pre-std	Reverts a port that is in pre-standard MST mode back to standard MST mode (IEEE Std 802.1s). See the "Usage Guidelines" section for more information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter only one instance number, you also can enter a VLAN number. If you enter a range of instance numbers, you cannot enter a VLAN number.

If you do not specify a VLAN, all VLANs are unmapped from the specified instance and added to MST instance 0 (IST).

Entering the **clear spantree mst** *mod/port* **pre-std** commands reverts a port that is in pre-standard MST mode back to standard MST mode. Pre-standard MST is the implementation of MST that is not compliant with with IEEE Std 802.1s. MST implementation is pre-standard on Catalyst 6500 series switches that are running software before release 8.3(1) . MST implementation is pre-standard on Catalyst 6500 series switches that are running any Cisco IOS software release. In standard MST mode, a port on a neighbor that is in pre-standard MST mode might become a boundary port, even though both switches have the same MST configuration.

The **set spantree mst** *mod/port* **auto** command also reverts a port back to standard MST mode.

Examples

This example shows how to clear VLAN 2 from MST instance 2:

```
Console> (enable) clear spantree mst 2 vlan 2
Console> (enable)
```

This example shows how to revert a port back to standard MST mode:

```
Console> (enable) clear spantree mst 4/47 pre-std
Pre-Std Neighbor type cleared on port 4/47.
Console> (enable)
```

Related Commands

set spantree mst
show spantree mst

clear spantree portcost

To clear the port cost of a port on the switch, use the **clear spantree portcost** command.

clear spantree portcost *mod/port* [**mst**]

Syntax Description

mod/port	Number of the module and the port on the module.
mst	(Optional) Restores the default path cost to an MST instance on a port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to restore the default path cost on a port:

```
Console> (enable) clear spantree portcost 3/1
Port 3/1 is using the cost 0.
Console> (enable)
```

This example shows how to restore the default path cost to all MST instances on a port:

```
Console> (enable) clear spantree portcost 8/1 mst
Port 8/1 MST is using the cost 20000 in MST mode.
Console> (enable)
```

Related Commands

set spantree portcost
show spantree statistics

clear spantree portinstancecost

To restore the default path cost to an instance on a port, use the **clear spantree portinstancecost** command.

clear spantree portinstancecost *mod/port* [**mst**] *instances*

Syntax Description

mod/port	Number of the module and the port on the module.
mst	(Optional) Restores the default path cost to an MST instance on a port.
instances	Number of the instance; valid values are from 0 to 15.

Defaults

The default path cost is based on port speed; see Table 2-8 for default settings.

Table 2-8 Default Port Cost—Short Mode

Port Speed	Default Port Cost
4 Mb	250
10 Mb	100
16 Mb	62
100 Mb	19
155 Mb	14
1 Gb	4
10 Gb	2

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is valid in MISTP and MST modes only.

Examples

This example shows how to restore the default path cost to an instance on a port:

```
Console> (enable) clear spantree portinstancecost 5/1 2
Port 5/1 mistp-instance 1-16 have path cost 200000.
Console> (enable)
```

This example shows how to restore the default path cost to all MST instances on a port:

```
Console> (enable) clear spantree portinstancecost 8/1 mst 0-15
Port 8/1 MST Instance 0-15 have path cost 20000.
Console> (enable)
```

Related Commands

set spantree portinstancecost
show spantree statistics

clear spantree portinstancepri

To restore the default path cost to an instance on a port, use the **clear spantree portinstancepri** command.

clear spantree portinstancepri *mod/port* [**mst**] [*instances*]

Syntax Description

mod/port	Number of the module and the port on the module.
mst	(Optional) Resets the spanning tree port MST instance priority.
instances	(Optional) Number of the instance; valid values are from 0 to 15.

Defaults

The default is the port priority is set to 0 with no instances specified.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is valid in MISTP and MST modes only.

Examples

This example shows how to reset the spanning tree port instance priority:

```
Console> (enable) clear spantree portinstancepri 5/1 2
Port 5/1 instances 1-16 using portpri 32.
Console> (enable)
```

This example shows how to reset the spanning tree port priority for all MST instances:

```
Console> (enable) clear spantree portinstancepri 8/1 mst 0-15
Port 8/1 MST Instances 0-15 using portpri 32
Console> (enable)
```

Related Commands

set spantree portinstancepri
show spantree

clear spantree portpri

To clear the port priority of a port on the switch, use the **clear spantree portpri** command.

clear spantree portpri *mod/port* [**mst**]

Syntax Description

mod/port	Number of the module and the port on the module.
mst	(Optional) Resets the MST port priority.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the spanning tree port priority:

```
Console> (enable) clear spantree portpri 3/1
Port 3/1 is using the cost 32.
Console> (enable)
```

This example shows how to clear the MST port priority:

```
Console> (enable) clear spantree portpri 8/1 mst
Port 8/1 is using the priority 32 in MST mode.
Console> (enable)
```

Related Commands

set spantree portpri
show spantree

clear spantree portvlancost

To restore the default path cost to a VLAN on a port, use the **clear spantree portvlancost** command.

clear spantree portvlancost *mod/port* [*vlans*]

Syntax Description

mod/port	Number of the module and the port on the module.
vlans	(Optional) Number of the VLAN; valid values are from 1 to 4094.

Defaults

The default path cost is based on port speed; see Table 2-9 and Table 2-10 for default settings.

Table 2-9 Default Port Cost—Short Mode

Port Speed	Default Port Cost
4 Mb	250
10 Mb	100
16 Mb	62
100 Mb	19
155 Mb	14
1 Gb	4
10 Gb	2

Table 2-10 Default Port Cost—Long Mode

Port Speed	Default Port Cost
100 Kb	200,000,000
1 Mb	20,000,000
10 Mb	2,000,000
100 Mb	200,000
1 Gb	20,000
10 Gb	2,000
100 Gb	200
1 Tb	20
10 Tb	2

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is valid in PVST+ mode only.

If you do not specify a VLAN, all VLANs are cleared.

Examples

These examples show how to restore the default path cost to a VLAN on a port:

```
Console> (enable) clear spantree portvlancost 2/10 1-10
Port 2/10 VLANs 11-21 have path cost 6
Port 2/10 VLANs 1-10,22-1000 have path cost 10.
Console> (enable)

Console> (enable) clear spantree portvlancost 2/10
Port 2/10 VLANs 1-1000 have path cost 10.
Console> (enable)
```

Related Commands

set spantree portvlancost
show spantree statistics

clear spantree portvlanpri

To reset the spanning tree port VLAN priority, use the **clear spantree portvlanpri** command.

clear spantree portvlanpri *mod/port* [*vlans*]

Syntax Description

mod/port	Number of the module and the port on the module.
vlans	(Optional) Number of the VLAN; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to reset the spanning tree port VLAN priority:

```
Console> (enable) clear spantree portvlanpri 1/2 23-40
Port 1/2 vlans 3,6-20,23-1000 using portpri 32
Port 1/2 vlans 1-2,4-5,21-22 using portpri 30
Console> (enable)
```

Related Commands

set spantree portvlanpri
show spantree

clear spantree root

To restore the spanning tree bridge priority, hello time, maxage, and forward delay on the switch to their default values, use the **clear spantree root** command.

clear spantree root [*vlans*]

clear spantree root mistp-instance *instances*

clear spantree root mst *instances*

Syntax Description

vlans	(Optional) Number of the VLAN; valid values are from 1 to 4094.
mistp-instance *instances*	Specifies the instance number; valid values are from 1 to 16.
mst *instances*	Specifies the MST instance number; valid values are 0 to 15.

Defaults

The defaults are as follows:

- switch priority is 32768
- forward delay is 15 seconds
- hello time is 2 seconds
- maxage is 20 seconds

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the spanning tree root on a range of VLANs:

```
Console> (enable) clear spantree root 1-20
VLANs 1-20 bridge priority set to 32678.
VLANs 1-20 bridge hello time set to 2 seconds.
VLANs 1-20 bridge max aging time set to 20 seconds.
VLANs 1-20 bridge forward delay set to 15 seconds.
```

This example shows how to clear the spanning tree root on two specific VLANs:

```
Console> (enable) clear spantree root 22,24
VLANs 22,24 bridge priority set to 32678.
VLANs 22,24 bridge hello time set to 2 seconds.
VLANs 22,24 bridge max aging time set to 20 seconds.
VLANs 22,24 bridge forward delay set to 15 seconds.
Console> (enable)
```

This example shows how to clear the spanning tree root on an instance:

```
Console> (enable) clear spantree root mistp-instance 1
Instance 1 bridge priority set to 32768.
Instance 1 bridge max aging time set to 20.
Instance 1 bridge hello time set to 2.
Instance 1 bridge forward delay set to 15.
Console> (enable)
```

This example shows how to clear the spanning tree root on an MST instance:

```
Console> (enable) clear spantree root mst 0
MST Instance s 0 bridge priority set to 32768.
Instances 0 bridge max aging time set to 20.
Instances 0 bridge hello time set to 2.
Instances 0 bridge forward delay set to 15.
Console> (enable)
```

Related Commands

set spantree root
show spantree

8.6 EFT Copy

clear spantree statistics

To clear the spanning tree statistics, use the **clear spantree statistics** command.

clear spantree statistics *mod/port*

clear spantree statistics *vlans*

clear spantree statistics mistp-instance *instances*

clear spantree statistics mst *instances*

clear spantree statistics bpdu

Syntax Description

mod/port	Number of the module and the port on the module.
vlans	(Optional) Number of the VLAN; valid values are from 1 to 4094.
mistp-instance *instances*	Specifies the instance number; valid values are from 1 to 16.
mst *instances*	Specifies the MST instance number; valid values are from 0 to 15.
bpdu	Clears the spanning tree BPDU counters. See the “Usage Guidelines” section for more information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enter the **clear spantree statistics bpdu** command, the counters for transmitted, received, processed, and dropped BPDUs and the rate of these BPDUs are cleared.

Examples

This example shows how to clear the spanning tree statistics for VLAN 1:

```
Console> (enable) clear spantree statistics 1
Cleared all VLAN counters for VLAN 1
Statistics cleared for vlans 1
Console> (enable)
```

This example shows how to clear the spanning tree statistics for a port:

```
Console> (enable) clear spantree statistics 3/1
Statistics cleared for module 3/1
Console> (enable)
```

This example shows how to clear the spanning tree statistics for an instance:

```
Console> (enable) clear spantree statistics mistp-instance 2
Statistics cleared for instances 2
Console> (enable)
```

This example shows how to clear the spanning tree statistics for an MST instance:

```
Console> (enable) clear spantree statistics mst 0
Statistics cleared for MST instance: 0
Console> (enable)
```

This example shows how to clear the counter statistics for spanning tree BPDUs:

```
Console> (enable) clear spantree statistics bpdu
Spanning tree BPDU statistics cleared on the switch.
Console> (enable)
```

Related Commands

show spantree statistics

clear spantree uplinkfast

To turn off the UplinkFast feature and to return the switch priority and port costs to the default settings, use the **clear spantree uplinkfast** command.

clear spantree uplinkfast

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

In some situations, when you use this command, load balancing on the switch might be lost.

Examples

This example shows how to turn off the UplinkFast feature and to return the switch priority to the default settings:

```
Console> (enable) clear spantree uplinkfast
This command will cause all portcosts, portvlancosts, and the
bridge priority on all vlans to be set to default.
Do you want to continue (y/n) [n]? y
VLANs 1-1005 bridge priority set to 32768.
The port cost of all bridge ports set to default value.
The portvlancost of all bridge ports set to default value.
uplinkfast disabled for bridge.
Console> (enable)
```

Related Commands

set spantree uplinkfast
show spantree uplinkfast

clear ssh mode

To clear the Secure Shell (SSH) version and return to compatibility mode, use the **clear ssh mode** command.

clear ssh mode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can return to compatibility mode after operating in SSH version 1 or version 2 mode by entering the **clear ssh mode** command. In compatility mode, both SSH version 1 connections and version 2 connetions are supported.

Examples

This example shows how to clear the SSH version and return to compatibility mode:

```
Console> (enable) clear ssh mode
SSH server mode set to V1 and V2
Console> (enable)
```

Related Commands

set ssh mode
show ssh

8.6 EFT Copy

clear system info-log command

To remove a **show** command from the system information logging index, use the **clear system info-log command** command.

clear system info-log command {**all** | *index_number*}

Syntax Description

all	Removes all **show** commands from the system information logging index.
index_number	Removes a specific **show** command entry from the system information logging index; valid values are from 1 to 15.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To display the index numbers of the **show** commands in the system information logging index, enter the **show system info-log** command.

Examples

This example shows how to remove the second **show** command from the system information logging index:

```
Console> (enable) clear system info-log command 2
Successfully cleared the configured command.
Console> (enable)
```

This example shows how to remove all **show** commands from the system information logging index:

```
Console> (enable) clear system info-log command all
Successfully cleared all the system commands configured.
Console> (enable)
```

Related Commands

clear config
set system info-log
show system info-log

clear system profile

To clear the system profile configuration, use the **clear system profile** command.

clear system profile

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the system profile configuration:

```
Console> (enable) clear system profile
Profile configuration is clear for the system.
Console> (enable)
```

Related Commands

clear config
set system profile
show system profile

clear tacacs key

To remove the key setting used for TACACS+ authentication and encryption, use the **clear tacacs key** command.

clear tacacs key

Syntax Description

This command has no arguments or keywords.

Defaults

The default key value is null.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the key setting used for authentication and encryption:

```
Console> (enable) clear tacacs key
TACACS server key cleared.
Console> (enable)
```

Related Commands

set tacacs key
show tacacs

clear tacacs server

To remove a host from the list of TACACS+ servers, use the **clear tacacs server** command.

clear tacacs server *ip_addr*

Syntax Description

ip_addr	IP address of the server to be removed from the list of TACACS+ servers.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove a server from the list of TACACS+ servers:

```
Console> (enable) clear tacacs server 170.1.2.20
170.1.2.20 cleared from TACACS table
Console> (enable)
```

Related Commands

show tacacs

clear timezone

To return the time zone to its default, UTC, use the **clear timezone** command.

clear timezone

Syntax Description

This command has no arguments or keywords.

Defaults

The default time zone is UTC.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear timezone** command functions only when NTP is running. If you set the time manually and NTP is disengaged, the **clear timezone** command has no effect.

Examples

This example shows how to clear the time zone:

```
Console> (enable) clear timezone
Timezone name and offset cleared.
Console> (enable)
```

Related Commands

set timezone

clear top

To stop the TopN process, use the **clear top** command.

clear top {**all** | *report_num*}

Syntax Description

all	Stops all nonpending TopN results.
report_num	TopN report number to kill; valid values are from 1 to 5.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **clear top all** command will not kill any pending TopN reports. Only the reports with a *done* status are killed.

You can terminate TopN processes without the **background** option (use the **show top background** command to find out if the **background** option is used) by pressing **Ctrl-C** in the same Telnet or console session or by entering the **clear top** [*report_num*] command from a separate Telnet or console session. The prompt is not printed before the TopN report is completely displayed. Other commands will be blocked until the report has been displayed.

Examples

This example shows how to stop the TopN 1 process from a console session:

```
Console> (enable) clear top 1
10/29/1998,12:05:38:MGMT-5: TopN report 1 killed by Console//.
Console> (enable)
```

This example shows how to stop the TopN 4 process from a Telnet session:

```
Console> (enable) clear top 4
10/29/1998,12:06:00:MGMT-5: TopN report 4 killed by telnet/172.22.34.2/.
Console> (enable)
```

Related Commands

show top
show top report

clear trunk

To restore a trunk port to its default trunk type and mode or to clear specific VLANs from the allowed VLAN list for a trunk port, use the **clear trunk** command.

clear trunk *mod/port* [*vlans*]

Syntax Description

mod/port	Number of the module and the port on the module.
vlans	(Optional) Number of the VLAN to remove from the allowed VLAN list; valid values are from 1 to 4094.

Defaults

For all ports except Multilayer Switch Module (MSM) ports, the default is **auto** negotiate. For MSM ports, the default is **off** negotiate mode.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you specify VLANs, those VLANs are removed from the list of VLANs allowed on the trunk. Default VLANs cannot be cleared on the trunk.

Traffic for the removed VLANs are not forwarded over a trunk port. To add VLANs that you have removed, use the **set trunk** *mod/port vlans* command.

If you are trying to clear extended-range VLANs and sufficient space in NVRAM is not available, a warning message displays and the command fails.

Examples

This example shows how to clear VLANs 200 through 500 from the trunk port on port 2 of module 1:

```
Console> (enable) clear trunk 1/2 200-500
Removing Vlan(s) 200-500 from allowed list.
Port 1/2 allowed vlans modified to 1-199,501-1000.
Console> (enable)
```

This example shows the output if you attempt to clear a trunk when not enough NVRAM space is available:

```
Console> (enable) clear trunk 2/18 1030-1999
Failed to clear extended range vlans from allowed list.
Not enough NVRAM space. Use the 'set trunk' command to restore
       some existing entries to the default value.
Console> (enable)
```

Related Commands

set trunk
show trunk

clear vlan

To delete an existing VLAN from a management domain or to clear VLANs that are secured by a Firewall Services Module, use the **clear vlan** command.

clear vlan *vlans*

clear vlan {*vlans*} **firewall-vlan** {*mod*}

Syntax Description

vlans	Number of the VLAN; valid values are from 1 to 4094.
firewall-vlan	Clears VLANs that are secured by a Firewall Services Module.
mod	Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Follow these guidelines for deleting VLANs:

- When you delete a normal-range Ethernet VLAN in VTP server mode, the VLAN is removed from all switches in the same VTP domain.
- When you delete a normal-range VLAN in VTP transparent mode, the VLAN is deleted only on the current switch.
- You can delete an extended-range VLAN only on the switch where it was created.

When you clear a VLAN, all ports assigned to that VLAN become inactive. However, the VLAN port assignments are retained until you move the ports to another VLAN. If the cleared VLAN is reactivated, all ports that are still configured on that VLAN are also reactivated. A warning is displayed if you clear a VLAN that exists in the mapping table.

When you clear a private VLAN (primary, isolated, or community), the ports are set to inactive and are not assigned to any VLAN. The private VLAN mappings for the selected VLAN are also cleared. ACL to VLAN mappings are also deleted.

Examples

This example shows how to clear existing VLAN 4000 from a management domain:

```
Console> (enable) clear vlan 4000
This command will de-activate all ports on vlan 4
in the entire management domain
Do you want to continue(y/n) [n]? y
VLAN 4 deleted
Console> (enable)
```

Related Commands

set vlan
show vlan

clear vlan counters

To return the software-cached counters to 0 for all VLANs, use the **clear vlan counters** command.

clear vlan counters {*vlans* | **all**}

Syntax Description

vlans	Number of the VLAN or range of VLANs; valid values are from 1 to 4094.
all	Clears counters for all VLANs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear counters for VLAN 1005:

```
Console> (enable) clear vlan counters 1005
This command will reset vlan couters for vlan 1005
Do you want to continue (y/n) [n]?y
Console> (enable)
```

Related Commands

show vlan counters

8.6 EFT Copy

clear vlan mapping

To delete existing IEEE 802.1Q VLAN-to-ISL VLAN mappings or reserved-to-nonreserved VLAN mapping, use the **clear vlan mapping** command.

clear vlan mapping dot1q {*dot1q_vlan* | **all**}

clear vlan mapping reserved {*reserved_vlan* | **all**}

Syntax Description

dot1q *dot1q_vlan*	Clears the IEEE 802.1Q VLAN-to-ISL VLAN mapping.
dot1q all	Clears all IEEE 802.1Q VLAN-to-ISL VLAN mappings.
reserved *reserved_vlan*	Clears the specified reserved-to-nonreserved VLAN mapping.
reserved all	Clears all reserved-to-nonreserved VLAN mappings.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you clear a VLAN, all ports assigned to that VLAN become inactive. However, the VLAN port assignments are retained until you move the ports to another VLAN. If the cleared VLAN is reactivated, all ports that are still configured on that VLAN are also reactivated.

Examples

This example shows how to clear an existing mapped VLAN from the dot1q mapping table:

```
Console> (enable) clear vlan mapping dot1q 444
Vlan Mapping 444 Deleted.
Console> (enable)
```

This example shows how to clear all mapped VLANs from the mapping table:

```
Console> (enable) clear vlan mapping dot1q all
All Vlan Mapping Deleted.
Console> (enable)
```

This example shows how to clear mapped reserved VLANs from the mapping table:

```
Console> (enable) clear vlan mapping reserved 1007
Vlan Mapping 1007 Deleted.
Console> (enable)
```

Related Commands

set vlan
show vlan

clear vmps rcp

To delete the VMPS rcp username from the VMPS server table, use the **clear vmps rcp** command.

clear vmps rcp *username*

Syntax Description

username	Username up to 14 characters long.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not enter a username, all rcp usernames are deleted.

Examples

This example shows how to clear a specific VMPS rcp username from the VMPS table:

```
Console> (enable) clear vmps rcp jdoe
Console> (enable)
```

Related Commands

set rcp username

clear vmps server

To delete a VMPS server from the VMPS server table, use the **clear vmps server** command.

clear vmps server *ip_addr*

Syntax Description

ip_addr	IP address or host name of the VMPS server to be deleted.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear a VMPS server from the VMPS table:

```
Console> (enable) clear vmps server 192.168.255.255
VMPS domain server 192.168.255.255 cleared from VMPS table.
Console> (enable)
```

This example shows the results of trying to clear a nonexistent VMPS server from the VMPS table:

```
Console> (enable) clear vmps server 192.168.255.255
VMPS domain server 192.168.255.255 not in VMPS table.
Console> (enable)
```

Related Commands

reconfirm vmps
set vmps server

clear vmps statistics

To delete existing VMPS statistics, use the **clear vmps statistics** command.

clear vmps statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to delete existing VMPS statistics:

```
Console> (enable) clear vmps statistics
VMPS and dynamic vlan statistics cleared.
Console> (enable)
```

Related Commands

show vmps statistics

clear vtp pruneeligible

To specify which VLANs in the VTP domain are ineligible for pruning, use the **clear vtp pruneeligible** command.

clear vtp pruneeligible *vlans...*

Syntax Description

vlans...	Number of VLANs to make pruning ineligible; valid values are from 2 to 1000.

Defaults

The default is VLANs 2 through 1000 are eligible for pruning.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if no stations belong to that VLAN out a particular switch port. Use the **set vtp** command to enable VTP pruning.

By default, VLANs 2 through 1000 are pruning eligible. Use the **clear vtp pruneeligible** command to make VLANs pruning ineligible.

If VLANs are pruning ineligible, use the **set vtp pruneeligible** command to make the VLANs pruning eligible again.

You can enter one or multiple VLANs. The following are examples of valid VLAN lists: 1; 1,2,3; 1-3,7; 2-215.

Examples

This example shows how to make VLANs 200 through 500 pruning ineligible:

```
Console> (enable) clear vtp pruneeligible 200-500
Vlans 1,200-500,1001-1005 will not be pruned on this device.
VTP domain Company modified.
Console> (enable)
```

Related Commands

set vtp
set vtp pruneeligible
show vtp domain

clear vtp statistics

To delete VTP statistics, use the **clear vtp statistics** command.

clear vtp statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear VTP statistics:

```
Console> (enable) clear vtp statistics
vtp statistics cleared.
Console> (enable)
```

Related Commands

set vtp
show vtp statistics

clear web-auth

To clear the configuration of the login or the login fail page, use the **clear web-auth** command.

clear web-auth {**login-page** | **login-fail-page**}

Syntax Description

login-page	Clears the configuration of the Login page.
login-fail-page	Clears the configuration of the Login Fail page.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the configuration of the Login page:

```
Console> (enable) clear web-auth login-page
Console> (enable)
```

This example shows how to clear the configuration of the Login Fail page:

```
Console> (enable) clear web-auth login-fail-page
Console> (enable)
```

Related Commands

set port web-auth
set port web-auth initialize
set web-auth
set web-auth login-attempts
set web-auth login-fail-page
set web-auth login-page
set web-auth quiet-timeout
set web-auth session-timeout
show port web-auth
show web-auth summary

commit

To commit all ACEs or a specific ACE in NVRAM that has not been written to hardware, use the **commit** command.

commit qos acl {*acl_name* | **all** | **adjacency**}

commit security acl {*acl_name* | **all** | **adjacency**}

Syntax Description

qos acl	Specifies QoS ACEs.
acl_name	Name that identifies the VACL whose ACEs are to be committed.
all	Commits ACEs for all the ACLs.
adjacency	Commits adjacency table entries.
security acl	Specifies security ACEs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **commit** command commits *all* ACEs in NVRAM that have not been written to hardware. Any committed ACL with no ACEs is deleted. We recommend that you enter ACEs in batches and enter the **commit** command to save all of them in hardware and NVRAM.

Examples

This example shows how to commit a specific QoS ACE to NVRAM:

```
Console> (enable) commit qos acl my_acl
Hardware programming in progress...
ACL my_acl is committed to hardware.
Console> (enable)
```

This example shows how to commit a specific security ACE to NVRAM:

```
Console> (enable) commit security acl IPACL2
ACL commit in progress.
ACL IPACL2 is committed to hardware.
Console> (enable)
```

This example shows how to commit an adjacency table entry to NVRAM:

```
Console> (enable) commit security acl adjacency
Commit operation in progress.
Adjacency successfully committed.
Console> (enable)
```

Related Commands rollback

commit lda

To commit ASLB configuration that has not been written to hardware to NVRAM, use the **commit lda** command.

commit lda

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to commit ASLB configuration to NVRAM:

```
Console> (enable) commit lda
Commit operation in progress...
Successfully committed Local Director Accelerator.
Console> (enable)
```

Related Commands

clear lda
set lda
show lda

configure

To download a configuration file from an rcp server or the network and execute each command in that file, use the **configure** command.

configure {*host file*}[**rcp**]

configure network

Syntax Description

host	IP address or IP alias of the host.
file	Name of the file.
rcp	(Optional) Specifies rcp as the file transfer method.
network	Specifies interactive prompting for the host and the file.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Refer to the *Catalyst 6500 Series Switch Software Configuration Guide* on how to construct a configuration file to download using the **configure** command.

Following is a sample file called system5.cfg in the /tftpboot directory:

```
begin
show time
set ip alias conc7 198.133.219.207
set ip alias montreux 198.133.119.42
set ip alias cres 192.122.174.42
set prompt system5>
set password
# empty string old password

pingpong
pingpong
end
#
```

Each line contains a command, except lines that begin with ! or #.

Examples

This example shows how to download the system5.cfg configuration file from the 192.122.174.42 host:

```
Console> (enable) configure 192.122.174.42 system5.cfg
Configure using system5.cfg from 192.122.174.42 (y/n) [n]? y
/
Done.  Finished Network Download.  (446 bytes)
>> show time
Wed May 19 1999, 17:42:50
>> set ip alias conc7 198.133.219.207
IP alias added.
>> set ip alias montreux 198.133.219.40
IP alias added.
>> set ip alias cres 192.122.174.42
IP alias added.
>> set prompt system5>
>> set password
Enter old password:
Enter new password: pingpong
Retype new password: pingpong
Password changed.
system5> (enable)
```

Related Commands

copy
show config

confreg

To configure the configuration register utility, use the **confreg** command.

confreg [*num*]

Syntax Description

num	(Optional) Valid values are 0 = ROM monitor, 1 = boot helper image, and 2 to 15 = boot system.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

Executed with the **confreg** argument *num*, the VCR changes to match the number specified.

Without the argument, **confreg** dumps the contents of the VCR in English and allows you to alter the contents.

You are prompted to change or keep the information held in each bit of the VCR. In either case, the new VCR value is written into NVRAM and does not take effect until you reset or power cycle the platform.

You must issue a **sync** command to save your change. Otherwise, the change is not saved and a **reset** removes your change.

Examples

This example shows how to use the **confreg** command:

```
rommon 7 > confreg

Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable  “diagnostic mode”? y/n  [n]: y
enable  “use net in IP bcast address”? y/n  [n]:
enable  “load rom after netboot fails”? y/n  [n]:
enable  “use all zero broadcast”? y/n  [n]:
enable  “break/abort has effect”? y/n  [n]:
enable  “ignore system config info”? y/n  [n]:
change console baud rate? y/n  [n]: y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400  [0]:  0
change the boot characteristics? y/n  [n]: y
```

```
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [0]:  0


Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:


You must reset or power cycle for new config to take effect
```

Related Commands

show boot

context

To display the context of a loaded image, use the **context** command.

context

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

The context from the kernel mode and process mode of a booted image are displayed, if available.

Examples

This example shows how to display the context of a loaded image:

```
rommon 6 > context
Kernel Level Context:
 Reg       MSW        LSW      | Reg       MSW        LSW
------  ---------- ----------  | -----   ---------- ----------
zero   : 00000000   00000000   | s0     : 00000000   34008301
AT     : 00000000   3e800000   | s1     : 00000000   00000001
v0     : 00000000   00000003   | s2     : 00000000   00000003
v1     : 00000000   00000000   | s3     : 00000000   00000000
a0     : 00000000   0000002b   | s4     : 00000000   60276af8
a1     : 00000000   00000003   | s5     : ffffffff   ffffffff
a2     : 00000000   00000000   | s6     : 00000000   60276c58
a3     : 00000000   60276af8   | s7     : 00000000   0000000a
t0     : 00000000   00000b84   | t8     : 00000000   34008300
t1     : 00000000   3e800004   | t9     : ffffffff   ac000000
t2     : 00000000   00000239   | k0     : 00000000   00000400
t3     : 00000000   34008301   | k1     : 00000000   6024eb5c
t4     : ffffffff   ffff83fd   | gp     : 00000000   60252920
t5     : 00000000   0000003f   | sp     : 00000000   60276a98
t6     : 00000000   00000000   | s8     : 00000000   601fbf33
t7     : ffffffff   ffffffff   | ra     : 00000000   6006d380
HI     : 00000000   00000008   | LO     : 00000000   00000000
EPC    : 00000000   60033054   | ErrPC  : ffffffff   bfc070c8
Stat   : 34408302              | Cause  : 00002020

Process Level Context:
 Reg       MSW        LSW      | Reg       MSW        LSW
------  ---------- ----------  | -----   ---------- ----------
zero   : 00000000   00000000   | s0     : 00000000   00000074
AT     : 00000000   3e820000   | s1     : 00000000   60276c58
v0     : 00000000   00000081   | s2     : 00000000   601fbac0
v1     : 00000000   00000074   | s3     : 00000000   00000036
```

```
a0      : 00000000   00000400  | s4     : 00000000   0000000f
a1      : 00000000   60276c58  | s5     : ffffffff   ffffffff
a2      : 00000000   00000074  | s6     : 00000000   60276c58
a3      : 00000000   00000000  | s7     : 00000000   0000000a
t0      : 00000000   00000400  | t8     : 00000000   34008300
t1      : 00000000   00000400  | t9     : ffffffff   ac000000
t2      : 00000000   00000000  | k0     : 00000000   30408401
t3      : ffffffff   ffff00ff  | k1     : 00000000   30410000
t4      : 00000000   600dcc10  | gp     : 00000000   60252920
t5      : 00000000   0000003f  | sp     : ffffffff   80007ce8
t6      : 00000000   00000000  | s8     : 00000000   601fbf33
t7      : ffffffff   ffffffff  | ra     : 00000000   600dfd20
HI      : 00000000   00000008  | LO     : 00000000   00000000
EPC     : 00000000   600dfd38  | ErrPC  : ffffffff   ffffffff
Stat    : 34008303             | Cause  : ffffffff
```

8.6 EFT Copy

copy

To upload or download a Flash image or a switch configuration to or from a Flash device, rcp server, TFTP server, or an SCP server, use the **copy** command.

copy *file-id* {**tftp** | **rcp** | **flash** | *file-id* | **config**}

copy tftp {**flash** | *file-id* | **config**}

copy rcp {**flash** | *file-id* | **config**}

copy flash {**tftp** | **rcp** | *file-id* | **config**}

copy config {**flash** | *file-id* | **tftp** | **rcp**} [**all**]

copy acl config {**flash** | *file-id* | **tftp** | **rcp**}

copy cfg1 {**tftp** | **rcp** | **flash** | **config** | **cfg2**} [**all**]

copy cfg2 {**tftp** | **rcp** | **flash** | **config** | **cfg1**} [**all**]

copy ftp {**flash** | *file-id* | **config**}

copy scp *destination*

copy *source* **scp**

copy log-cmd {**flash** | **ftp** | **rcp** | **scp** | **tftp** | *file-id*}

copy sftp *destination*

copy *source* **sftp**

Syntax Description

file-id	Format used to specify the file on the Flash device, where the format is *m/device***:***filename.* *m/* = Option that gives access to different modules, such as the standby supervisor engine or an Ethernet module. *device***:** = Device where the Flash resides. *filename* = Name of the configuration file.
tftp	Allows you to copy to or from a TFTP server.
rcp	Specifies the file be copied to or from an rcp server.
flash	Supports downloading of multiple modules.
config	Allows you to copy the configuration to Flash memory, another Flash device, or a file on a TFTP server.
acl config	Copies the ACL configuration manually to a file. See the “Usage Guidelines” section before using this command.
cfg1	Specifies the first startup configuration file on the supervisor engine.
cfg2	Specifies the second startup configuration file on the supervisor engine.
all	(Optional) Specifies that the entire configuration be copied to the specified destination configuration file.
ftp	Allows you to copy to or from an FTP server.

8.6 EFT Copy

scp *destination*	Copies a file by using Secure Copy (SCP) to a specified destination on the system.
source **scp**	Copies a file by using SCP from a specified source on the system.
log-cmd	Copies command log to a specified device.
scp	Specifies SCP for secure images.
sftp *destination*	Copies a file by using Secure File Transfer Protocol (SFTP) to a specified destination on the system.
source **sftp**	Copies a file by using SFTP from a specified source on the system.

Defaults

If a source or destination device is not given, the one specified by the **cd** command is used. If a destination filename is omitted, the source filename is used.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use the **copy** command to perform these tasks:

- Download a system image or configuration file from a TFTP or rcp server to a Flash device.
- Upload a system image or configuration file from a Flash device to a TFTP or rcp server.
- Configure the switch using a configuration file on a Flash device or on a TFTP or rcp server.
- Copy the current configuration to a Flash device or to a TFTP or rcp server.
- Manually copy the ACL configuration to a file.
- Upload command log entries to a Flash device or to a TFTP or rcp server.

Caution Manual copying can only be used if **acl config** is set to **flash** and you enable the **auto-config append** option. If you disable the **append** option, the configuration clears before executing the auto-config file; see the **set boot config-register auto-config** command.

If you do not specify the source or destination device, the command uses the ones specified by the **cd** command. If you omit the destination filename, the source filename is used.

The **copy config**, **copy cfg1**, and **copy cfg2** commands copy only nondefault commands to the destination configuration file. Use the keyword **all** to copy both default and nondefault configurations.

If you do not specify a source or destination Flash device, the default Flash device (specified by the **cd** command) is used. Use the **pwd** command to display the current default Flash device. If you omit the destination filename, the system uses the source filename.

The system stores image and configuration files in the *sysname.cfg* file when you define a system name using the **set system name** command; otherwise, it uses the default *myswitch.cfg* file.

A colon (:) is required after the specified device.

8.6 EFT Copy

If you use the **flash** keyword as the copy source or destination, you are prompted for the Flash device name.

If you are copying a software image to multiple intelligent switching modules of the same type, use the **flash** keyword as the copy destination. The switch automatically determines which modules to copy the image to based on the header in the source image file. If you want to copy a software image to a single intelligent switching module in a switch with multiple modules of the same type, you must specify the destination *file-id* as *m***/bootflash:** (do not specify a filename).

Before you begin downloading a software image using SCP, make sure of the following:

- Ensure that the workstation acting as the SCP server supports the Secure Shell (SSH).
- Ensure that the server supports a command shell that has an SSH v1-compatible **scp** command available.
- Ensure that the switch has a route to the SCP server. The switch and the SCP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the SCP server using the **ping** command.
- A power interruption (or other problem) during the download procedure can corrupt the Flash code. If the Flash code is corrupted, you can connect to the switch through the console port and boot from an uncorrupted system image on a Flash PC card.

Before you attempt to upload a software image to an SCP server, do the following:

- Ensure that the workstation acting as the SCP server is configured properly.
- Ensure that the switch has a route to the SCP server. The switch and the SCP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the rcp server using the **ping** command.
- If you are overwriting an existing file (including an empty file, if you had to create one), ensure that the permissions on the file are set correctly. Permissions on the file should be set to write for the specific username.

For more information about downloading and uploading files by using SCP, refer to Chapter 25, “Working with System Software Images,” in the *Catalyst 6500 Series Switch Software Configuration Guide*.

The Secure File Transfer Protocol (SFTP) is available only in crypto images.

SFTP uses the SSH protocol for establishing a secure channel between the client and the server. SFTP is supported only with SSHv2. SFTP with SSHv1 is not supported.

SFTP client functionality is supported. SFTP server functionality is not supported.

[Examples to be provided.]

Examples

This example shows how to use the **copy** command to upload the switch configuration to a file named cat.cfg on the slot0 Flash device:

```
Console> (enable) copy config slot0:cat.cfg
Upload configuration to slot0:cat.cfg
649324 bytes available on device slot0, proceed (y/n) [n]? y
.........
.........
.........
........
.........
.
/
Configuration has been copied successfully. (10200 bytes)
```

8.6 EFT Copy

```
Console> (enable)
```

This example shows how to use the **copy** command to upload the switch configuration to a file named lab2.cfg on the TFTP server:

```
Console> (enable) copy config tftp:lab2.cfg
IP address or name of remote host [172.20.22.7]? y
Upload configuration to tftp:lab2.cfg (y/n) [n]? y
.........
.........
.........
.
/
Configuration has been copied successfully. (10299 bytes).
Console> (enable)
```

This example shows how to use the **copy** command to upload the switch configuration to the cat.cfg file on the slot0 Flash device:

```
Console> (enable) copy config flash
Flash device [bootflash]? slot0:
Name of file to copy to [test_image]? cat.cfg
Upload configuration to slot0:cat.cfg
749124 bytes available on device slot0, proceed (y/n) [n]? y
.........
.........
.........
........
.
/
Configuration has been copied successfully. (200345 bytes).
Console> (enable)
```

These examples show how to use the **copy** command to download a configuration from a TFTP server:

```
Console> (enable) copy slot0:cat.cfg config
Configure using slot0:cat.cfg (y/n) [n]? y
/
Finished download. (10900 bytes)
>> set password $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
Password changed.
>> set enablepass $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
Password changed.
>> set prompt Console>
>> set length 24 default
Screen length set to 24.
>> set logout 20
..........
Console> (enable)

Console> (enable) copy tftp config
IP address or name of remote host? 172.20.22.7
Name of configuration file? cat.cfg
Configure using cat.cfg from 172.20.22.7 (y/n) [n]? y
/
Finished network download. (10900 bytes)
>> set password $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
Password changed.
>> set enablepass $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
Password changed.
>> set prompt Console>
>> set length 24 default
Screen length set to 24.
>> set logout 20
```

8.6 EFT Copy

```
...........
Console> (enable)
Console> (enable) copy flash config
Flash device [bootflash]?
Name of configuration file? test.cfg
Configure using bootflash:test.cfg (y/n) [n]? y
/
Finished download. (10900 bytes)
>> set password $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
Password changed.
>> set enablepass $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
Password changed.
>> set prompt Console>
>> set length 24 default
Screen length set to 24.
>> set logout 20
.....
Console> (enable)
```

This example shows how to copy the running configuration to an rcp server for storage:

```
Console> (enable) copy config rcp
IP address or name of remote host []? 172.20.52.3
Name of file to copy to []? cat6000_config.cfg

Upload configuration to rcp:cat6000_config.cfg, (y/n) [n]? y
.....
..........
.......

..........
...........
..
/
Configuration has been copied successfully.
Console> (enable)
```

This example shows how to configure a Catalyst 6500 series switch using a configuration file downloaded from an rcp server:

```
Console> (enable) copy rcp config
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns-config.cfg

Configure using rcp:dns-config.cfg (y/n) [n]? y
/
Finished network download.  (134 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)
```

This example shows how to upload an image from a remote host into Flash using an rcp server:

```
Console> (enable) copy rcp flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-sup-d.6-1-1.bin
Flash device [bootflash]?
```

```
Name of file to copy to [cat6000-sup-d.6-1-1.bin]?

4369664 bytes available on device bootflash, proceed (y/n) [n]? y
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
File has been copied successfully.
Console> (enable)
```

This example shows how to download a configuration to the first startup configuration file (cfg1) on a supervisor engine:

```
Console> (enable) copy tftp cfg1
IP address or name of remote host [172.20.32.10]?
Name of file to copy from [/tftpboot/my.cfg]?
Download config file from /tftpboot/my.cfg to cfg1 (y/n) [n]?
.........
File has been copied to cfg1.
Console> (enable)
```

This example shows how to copy the ACL configuration to a bootflash file manually:

```
Console> (enable) copy acl config bootflash:switchapp.cfg
Upload configuration to bootflash:dan.cfg
2843644 bytes available on device bootflash, proceed (y/n) [n]? y
.........
.........
/
Configuration has been copied successfully.
Console> (enable)
```

This example shows a complete SCP download procedure of a crypto image to the switch:

```
Console> (enable) copy scp flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-sup720cvk9.8-3-1.bin
Flash device [bootflash]?
Name of file to copy to [cat6000-sup720cvk9.8-3-1.bin]?

4369664 bytes available on device bootflash, proceed (y/n) [n]? y
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
File has been copied successfully.
Console> (enable) set boot system flash bootflash:cat6000-sup720cvk9.8-3-1.bin prepend
BOOT variable =
bootflash:cat6000-sup720cvk9.8-3-1.bin,1;bootflash:cat6000-sup720cvk9.8-3-1.bin
1-csx.bin,1;
Console> (enable) reset system
This command will reset the system.
Do you want to continue (y/n) [n]? y
Console> (enable) 11/25/2003,13:51:39:SYS-5:System reset from Console//

System Bootstrap, Version 4.2
Copyright (c) 1994-2003 by cisco Systems, Inc.
Presto processor with 32768 Kbytes of main memory

Autoboot executing command: "boot bootflash:cat6000-sup720cvk9.8-3-1.bin"
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
Uncompressing file:  ###########################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
```

8.6 EFT Copy

```
################################################################################
################################################################################
################################################################################
################################################################################
#############


System Power On Diagnostics
DRAM Size ....................32 MB
Testing DRAM..................Passed
Verifying Text segment .......Passed
NVRAM Size ...................512 KB
Saving NVRAM .................
Testing NVRAM ................Passed
Restoring NVRAM...............
Level2 Cache ..................Present
Level2 Cache test..............Passed

Leaving power_on_diags

Cafe Daughter Present.

EOBC link up

Boot image: cat6000-sup720cvk9.8-3-1.bin
Flash Size = 0X1000000, num_flash_sectors = 64
readCafe2Version: 0x00000001
RIn Local Test Mode, Pinnacle Synch Retries: 2
Running System Diagnostics from this Supervisor (Module 1)
This may take up to 2 minutes....please wait

Cisco Systems Console

Enter password:
11/25/2003,13:52:51:SYS-5:Module 1 is online
11/25/2003,13:53:11:SYS-5:Module 4 is online
11/25/2003,13:53:11:SYS-5:Module 5 is online
11/25/2003,13:53:14:PAGP-5:Port 1/1 joined bridge port 1/1.
11/25/2003,13:53:14:PAGP-5:Port 1/2 joined bridge port 1/2.
11/25/2003,13:53:40:SYS-5:Module 2 is online
11/25/2003,13:53:45:SYS-5:Module 3 is online
Console> (enable)
```

This example shows how to upload the crypto image to an SCP server:

```
Console> (enable) copy bootflash scp
Flash device [bootflash]? slot0:
Name of file to copy from []? cat6000-sup720cvk9.8-3-1.bin
IP address or name of remote host [172.20.52.3]? 172.20.52.10
Name of file to copy to [cat6000-sup720cvk9.8-3-1.bin]?
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC|
File has been copied successfully.
Console> (enable)
```

8.6 EFT Copy

Related Commands

clear ftp
configure
reset—switch
set boot config-register
set boot config-register auto-config
set boot system flash
set ftp
show ftp
write

delete

To delete a configuration file, use the **delete** command.

delete [[*m/*]*device***:**]*filename*

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device***:**	(Optional) Device where the Flash resides.
filename	Name of the configuration file.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

Examples

This example shows how to delete the cat6000-sup-d.5-5-1.bin configuration file from the Flash device and then verify the deletion by entering the **show flash** command:

```
Console> (enable) delete bootflash:cat6000-sup-d.5-5-1.bin
Console> (enable)
Console> (enable) show flash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
  1 .D ffffffff 5415406e  3300b8   25  3080247 Jan 12 2000 13:22:46
cat6000-sup-d.6-1-1.bin
  2 .. ffffffff 762950d6  6234d0   25  3093399 Jan 13 2000 12:33:14
cat6000-sup-d.6-1-1.bin

1428272 bytes available (6173904 bytes used)
Console> (enable)
```

Related Commands

dir—switch
show flash
squeeze
undelete

8.6 EFT Copy

dev

To list the device IDs available on a switch, use the **dev** command.

dev

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Examples

This example shows how to use the **dev** command:

```
rommon 10 > dev
Devices in device table:
        id  name
 bootflash: bootflash
    slot0:  PCMCIA slot 0
    eprom:  eprom
```

diagnostic start

To start running a specific test based on test ID numbers, use the **diagnostic start** command.

diagnostic start module *mod_num* **test** {**all** | *test_ID_num* | *test_list* | **complete** | **minimal** | **non-disruptive** | **per-port**} [**port** {**all** | *port_num* | *port_list*}]

Syntax Description

module *mod_num*	Specifies the module on which to start running specific tests.
test	Specifies particular online diagnostic tests.
all	Species all online diagnostic tests.
test_ID_num	Number of a specific online diagnostic test.
test_list	List of online diagnostic tests.
complete	Starts complete set of bootup diagnostic tests.
minimal	Starts minimal set of bootup diagnostic tests.
non-disruptive	Starts nondisruptive set of diagnostic tests.
per-port	Starts a per-port set of diagnostic tests.
port	Specifies port selection.
all	Specifies all ports on the module.
port_num	Number of a port.
port_list	Range of ports.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **diagnostic start** command accepts one test ID, a range of test IDs, a subgroup of tests, or **all** for all tests. The test ID for a particular test can be different from one module type to another module type or even from one software release to another software release. You need to obtain the correct test ID and relevant test name using by the **show diagnostic content** command.

To configure generic online diagnostics, use the **set** commands in the “Related Commands” section.

Note GOLD is supported on the Supervisor Engine 720 and the Supervisor Engine 32 only. Earlier diagnostic commands are still supported on the Supervisor Engine 1 and the Supervisor Engine 2.

8.6 EFT Copy

Examples

This example shows how to start online diagnostic test 1 on module 5:

```
Console> diagnostic start module 5 test 1
2005 Aug 18 15:10:08 %DIAG-6-TEST_RUNNING:Module 5: Running FirmwareDiagStatus{ID=1} ...
2005 Aug 18 15:10:08 %DIAG-6-TEST_OK:Module 5: FirmwareDiagStatus{ID=1} has completed
successfully
Console>
```

Related Commands

clear diagnostic
set diagnostic bootup level
set diagnostic diagfail-action
set diagnostic event-log size
set diagnostic monitor
set diagnostic ondemand
set diagnostic schedule
show diagnostic

diagnostic stop

To stop running generic online diagnostics on a specified module, use the **diagnostic stop** command.

diagnostic stop module *mod_num*

Syntax Description

module *mod_num*	Specifies the module on which to stop running specific tests.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Because some memory tests might take hours to complete, if you want to stop them before they conclude, use this command.

Note GOLD is supported on the Supervisor Engine 720 and the Supervisor Engine 32 only. Earlier diagnostic commands are still supported on the Supervisor Engine 1 and the Supervisor Engine 2.

Examples

This example shows the output when you enter the **diagnostic stop** command, but no test is running:

```
Console> diagnostic stop module 5
Diagnostic[Module 5]: Diagnostic is not active.
2005 Aug 18 15:38:30 %DIAG-3-NO_DIAG_RUNNING:Module 5: Diagnostic is not running
Console>
```

Related Commands

clear diagnostic
set diagnostic bootup level
set diagnostic diagfail-action
set diagnostic event-log size
set diagnostic monitor
set diagnostic ondemand
set diagnostic schedule
show diagnostic

dir—ROM monitor

To list the files of the named device, use the **dir** command.

dir *device*

Syntax Description

device	ID of the device.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Examples

This example shows how to use the **dir** command:

```
rommon 11 > dir flash:
         File size           Checksum   File name
        65 bytes (0x41)        0xb49d    clev/oddfile65
   2229799 bytes (0x220627)    0x469e    clev/sierra-k.Z
```

dir—switch

To display a list of files on a Flash memory device, use the **dir** command.

dir [[*m/*]*device***:**][*filename*] [**all** | **deleted** | **long**]

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device***:**	(Optional) Device where the Flash resides.
filename	(Optional) Name of the configuration file.
all	(Optional) Displays all files, deleted or not.
deleted	(Optional) Displays only deleted files.
long	(Optional) Displays files that have not been deleted, in long format.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal and privileged.

Usage Guidelines

A colon (:) is required after the specified device.

When you specify the **all** keyword, the file information is displayed in long format.

When you omit all keywords (**all**, **deleted**, or **long**), the system displays file information in short format. Short format is shown in Table 2-11.

Table 2-11 Short Format

Column Heading	Description
#	File index number
length	File length
date/time	Date and time the file was created
name	Filename

When you use one of the keywords (**all**, **deleted**, or **long**), the system displays file information in long format. The long format is shown in Table 2-12.

Table 2-12 Long Format

Column Heading	Description
#	File index number
ED	Letter to indicate whether the file contains an error (E) or is deleted (D)
type	File type (1 = configuration file, 2 = image file); when the file type is unknown, the system displays a zero or FFFFFFFF in this field
crc	File cyclic redundancy check
seek	Offset into the file system of the next file
nlen	Filename length
length	File length
date/time	Date and time the file was created
name	Filename

Examples

This example shows how to display the file information in short format:

```
Console> (enable) dir
-#- -length- -----date/time------ name
  1  6061822 Mar 03 2000 15:42:49 cat6000-sup.6-1-1.bin
  2  6165044 Mar 13 2000 14:40:15 cat6000-sup.5-5-1.bin

3763660 bytes available (12227124 bytes used)
Console> (enable)
```

This example shows how to display the file information in long format:

```
Console> (enable) dir long
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
  1 .. ffffffff f3a3e7c1  607f80   24  6061822 Mar 03 2000 15:42:49 cat6000-sup.
6-1-1.bin
  2 .. ffffffff aa825ac6  be9234   24  6165044 Mar 13 2000 14:40:15 cat6000-sup.
5-5-1.bin

3763660 bytes available (12227124 bytes used)
Console> (enable)
```

Related Commands

show flash

disable

To return to normal mode from privileged mode, use the **disable** command.

disable

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to return to normal mode:

```
Console> (enable) disable
Console>
```

Related Commands

enable

disconnect

To close a session by session ID number, use the **disconnect** command.

disconnect *session_id*

Syntax Description

session_id	Number of the session.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To identify session ID numbers, enter the **show users** command.

Examples

This example shows how to close a session by entering the session ID number:

```
Console> (enable) disconnect 2
Telnet session from cbin3-view2.cisco.com disconnected.
Console> (enable)
```

Related Commands

show users
telnet

8.6 EFT Copy

download

To copy a software image from a specified host to the Flash memory of a designated module, use the **download** command.

download *host file* [*mod*] [**rcp**]

download serial

download vmps

download boot *flash_device:filename mod_num*

download epld *file* [*mod* [**force**]]

Syntax Description

host	Name or IP address of host.
file	Name of file to be downloaded.
mod	(Optional) Number of the module to receive the downloaded image.
rcp	(Optional) Specifies rcp as the file transfer method.
serial	Specifies download through a serial port.
vmps	Downloads VMPS.
boot	Downloads an image to the boot ROM of a module.
flash_device: *filename*	Name of the software image to be downloaded.
mod_num	Number of the module to receive the downloaded image.
epld	Updates the module’s Erasable Programmable Logic Device (EPLD) image file.
file	Name of the EPLD image file.
force	(Optional) Updates the existing EPLD image file on the module with the new EPLD image regardless of the version of the existing image.

Defaults

If a module number is not specified, the image is downloaded to all modules for which the image is valid.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Catalyst 6500 series switches download new code to the processors using Kermit serial download through the EIA/TIA-232 console port.

The **download** command downloads code to the module Flash memory. Catalyst 6500 series switch software rejects an image if it is not a valid image for the module.

The **download serial** command uses Kermit through the serial EIA/TIA-232 console port. The **download serial** command is not allowed from a Telnet session.

8.6 EFT Copy

Before you can execute the **download vmps** command successfully, you must use the **set vmps downloadserver** command to configure the IP address of the TFTP server and the name of the VMPS configuration file on that server. If the IP address of the TFTP server is not configured, the **download vmps** command reports an error. If the configuration filename is not configured, the **download vmps** command uses the default filename vmps-config-database.1.

The VMPS backup file is overwritten each time a new VMPS configuration is downloaded from the TFTP server by means of a VMPS server reboot or because the **download vmps** command or **set vmps state** {**disable** | **enable**} command was entered. If there are not enough resources to build the new configuration database, the VMPS is made inactive.

If you specify the module number, the download goes to the specified module, but the download will fail if the module is a different type from the one that is indicated by the download header. If you do not specify the module number, the download goes to all modules of that type.

Caution After starting the serial download using Kermit, do not attempt to abort the serial download by pressing **Ctrl-C**. Pressing **Ctrl-C** interrupts the download process and could affect the functionality of the switch. If the functionality of the switch is affected as a result of pressing **Ctrl-C**, reboot the switch.

If you enter the **download epld** *file* command without specifying a module, the new EPLD image is downloaded to all compatible modules where the new EPLD image version is greater than the existing version on the module. If the **download epld** *file mod* command is used with the **force** keyword, the existing EPLD image on a module is upgraded with the new EPLD image regardless of the version level of the existing image.

Caution If you remove the module while the EPLD image is updating, the module might not come back online.

Examples

This example shows how to download the c6000_spv11.bin file from the mercury host to the supervisor engine (by default):

```
Console> (enable) download mercury c6000_spv11.bin
Download image c6000_spv11.bin from mercury to module 1FLASH (y/n) [n]? y
\
Finished network single module download. (2418396 bytes)
FLASH on Catalyst:

Type            Address             Location
Intel 28F008    20000000            NMP (P3) 4MB SIM

Erasing flash sector...done.
Programming flash sector...done.
Erasing flash sector...done.
Programming flash sector...done.
The system needs to be reset to run the new image.
Console> (enable)
```

This example shows how to download the acpflash_1111.bbi file from the mercury host to module 3:

```
Console> (enable) download mercury acpflash_1111.bbi 3
This command will reset Module 3.
Download image acpflash_1111.bbi from mercury to Module 3 FLASH (y/n) [n]? y
/
Done.  Finished network download.  (1964012 bytes)
Console> (enable)
```

8.6 EFT Copy

This sample session shows how to connect to a remote terminal from a Sun workstation and how to use the **download serial** command to copy a software image to the supervisor engine:

```
[At local Sun workstation]
host% kermit
C-Kermit 5A(172) ALPHA, 30 Jun 95, SUNOS 4.0 (BSD)
Type ? or 'help' for help
C-Kermit> set line /dev/ttyb
C-Kermit> c
Connecting to /dev/ttyb, speed 9600.
The escape character is ^ (ASCII 28).
Type the escape character followed by C to get back,
or followed by ? to see other options.

Console> enable
Enter Password:
Console> (enable) set system baud 19200
^\C
[Back at local Sun workstation]
C-Kermit> set speed 19200
/dev/ttyb, 19200 bps
C-Kermit> c
Connecting to /dev/ttyb, speed 19200.
The escape character is ^ (ASCII 28).
Type the escape character followed by C to get back,
or followed by ? to see other options.

Console> (enable) download serial
Download Supervisor image via console port (y/n) [n]? y

Concentrator Boot ROM (Ver 1.00)

Waiting for DOWNLOAD!!
Return to your local Machine by typing its escape sequence
Issue Kermit send command from there[ Send 'Filename']

^\C
[Back at Local System]
C-Kermit> send c6000_xx.bin
                          SF
c6000_xx.bin => C6000_XX.BIN, Size: 1233266

X to cancel file,  CR to resend current packet
Z to cancel group, A for status report
E to send Error packet, Ctrl-C to quit immediately: ..........................
...............................................................................

...... [OK]
ZB
C-Kermit> quit
host%
```

This example shows how to download a ROM image to module 9:

```
Console> (enable) download boot bootflash:boot542.ubin 9
Warning!! This command replaces the existing boot code on Module 9.
Please verify with TAC that the file specified is appropriate for WS-X6408-GBIC.
Use this command with caution.
Do you want to continue (y/n) [n]? y
Download boot image start...
Download boot code completed.
Console> (enable)
```

This example shows how to upgrade the EPLD image in force mode on the module in slot 5:

```
Console> (enable) download epld aq_cr128_art.bin 5 force
CCCCCC
Device found requiring upgrade in slot 5.

########################################################
#                   W A R N I N G                      #
#                                                      #
# Any disruptions to the module during programming may #
# leave the module or system in an inconsistent state. #
# Please ensure that the system or module does not get #
# switched off or reset during the programming process.#
# Programming may take a minute or two, depending on   #
# the number of devices updated.  Please wait for the  #
# module to come back online before continuing.        #
#                                                      #
#                   W A R N I N G                      #
########################################################
This command may reset module 5.
Updating fabric modules may significantly affect system performance while the update is
occurring.

Do you wish to update the devices in slot 5 (y/n) [n]? y


Updating programmable devices in slot 5.  This may take a minute...
  JAM Message -> Device #1 Silicon ID is ALTERA98(00)
  JAM Message -> programming 7K device(s)...
  JAM Message -> verifying 7K device(s)...
  JAM Message -> DONE
Programming successful, updating EPLD revisions.
2002 Aug 09 06:32:22 %SYS-4-NVLOG:EpldUpdate:Module 5 EPLD A updated from rev 1 to rev 1
Waiting for module to come online.
..........2002 Aug 09 06:32:33 %SYS-5-MOD_OK:Module 5 is online
.

################################################################################

                E P L D   P R O G R A M M I N G   C O M P L E T E

    Found 1 devices requiring upgrades, 1 attempted, 1 updated, 0 failed

################################################################################
Console> (enable) 2002 Aug 09 06:32:34 %SYS-4-NVLOG:EpldUpdate:Module 5 EPLD A s
prom updated to rev 1
Console> (enable)
```

Related Commands

reset—switch
set system supervisor-update
show flash
show rcp
show system supervisor-update
show version
show vmps

enable

To activate privileged mode, use the **enable** command. In privileged mode, additional commands are available, and certain commands display additional information.

enable

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The (enable) in the prompt indicates that the system is in privileged mode and that commands can be entered.

Examples

This example shows how to enter privileged mode:

```
Console> enable
Enter password:
Console> (enable)
```

Related Commands

disable

format

To format bootflash or a Flash PC card (a Flash device must be formatted before it can be used), use the **format** command.

format [**spare** *spare-num*] [*m/*]*device1***:** [[*device2***:**][*monlib-filename*]]

Syntax Description

spare *spare_num*	(Optional) Indicates the number of spare sectors to reserve when other sectors fail.
m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device1***:**	Flash device to be formatted.
*device2***:**	(Optional) Flash device that contains the *monlib* file to be used to format *device1***:**.
monlib-filename	(Optional) Name of the monlib file.

Defaults

The default number of spare sectors is 0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

You can reserve up to 16 spare sectors for use when other sectors fail. If you do not reserve a spare sector and later some sectors fail, you will have to reformat the entire Flash memory, which will erase all existing data.

The monlib file is the ROM monitor library used by the ROM monitor to access files in the Flash file system. It is also compiled into the system image. In the command syntax, *device1***:** is the device to format and *device2***:** contains the *monlib* file to use.

When you omit the [[*device2***:**][*monlib-filename*]] argument, the system formats *device1***:** using the *monlib* that is bundled with the system software.

When you omit *device2***:** from the [[*device2***:**][*monlib-filename*]] argument, the system formats *device1***:** using the named *monlib* file from the device specified by the **cd** command.

When you omit *monlib-filename* from the [[*device2***:**][*monlib-filename*]] argument, the system formats *device1***:** using the *monlib* file from *device2***:**. When you specify the whole [[*device2***:**][*monlib-filename*]] argument, the system formats *device1***:** using the specified *monlib* file from the specified device.

You can also specify *device1***:***monlib-filename* as the device and filename to be used, as follows:

format device1: [*device1***:** [*monlib-filename*]]

If *monlib-filename* is omitted, the system formats *device1*: using the built-in monlib file on the device.

Note When the system cannot find a monlib file, the system terminates the formatting process.

Note If the Flash device has a volume ID, you must provide the volume ID to format the device. The volume ID is displayed using the **show flash** *m/device:* **filesys** command.

Examples

This example shows how to format a Flash PC card:

```
Console> (enable) format slot0:
All sectors will be erased, proceed (y/n) [n]?y
Enter volume id (up to 31 characters):
Formatting sector 1
Format device slot0 completed.
Console> (enable)
```

frame

To display an individual stack frame, use the **frame** command.

frame [**-d** | **-p**] [*num*]

Syntax Description

-d	(Optional) Specifies a monitor context.
-p	(Optional) Specifies a booted image process level context.
num	(Optional) Number of the frame to display, where **0** = youngest frame.

Defaults

The default is a booted image kernel context, which is the youngest frame.

Command Types

ROM monitor command.

Command Types

Normal.

Usage Guidelines

The minus sign (-) is required with the **-d** and **-p** options.

Examples

This example shows how to use the **frame** command to specify a booted image process level context, frame 1:

```
rommon 6 > frame -p 1
Stack Frame 1, SP = 0x80007ed8, Size = 32 bytes
[0x80007ed8 : sp + 0x000] = 0x6031de50
[0x80007edc : sp + 0x004] = 0x6031c000
[0x80007ee0 : sp + 0x008] = 0x00000000
[0x80007ee4 : sp + 0x00c] = 0x80007ec4
[0x80007ee8 : sp + 0x010] = 0x00000002
[0x80007eec : sp + 0x014] = 0x00000000
[0x80007ef0 : sp + 0x018] = 0x60008770
[0x80007ef4 : sp + 0x01c] = 0x600087f0
```

fsck

To check a Flash file system for damage and to repair any problems, use the **fsck** command.

fsck [*m***/**]*device***:** [**automatic**]

Syntax Description

*m***/**	(Optional) Number of the module that contains the Flash device.
*device***:**	Name of the Flash device; valid device names are **disk0:** and **disk1:**.
automatic	(Optional) Specifies automatic mode. See the "Usage Guidelines" section for more information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

In automatic mode, problems are fixed automatically and you are not prompted to confirm any changes that will be made to the file system.

Examples

This example shows how to check a file system for damage and to make repairs. First, enter the **dir** command to list files on a device and to display the file that is corrupted:

```
Console> (enable) dir disk0:
      3   -rw-       556    Mar 06 2049 16:26:16 t1
      4   -rw-       556    Mar 06 2049 16:26:16 t2
      5   -rw-       556    Mar 06 2049 16:26:16 t3
      6   -rw-    258048    Mar 06 2049 16:26:16 t4
CORRUPTED
Console> (enable)

128090112 bytes available (16384 bytes used)
```

Then, enter the **fsck** command to repair the corrupted file:

```
Console> (enable) fsck disk0:

Checking the partition table and boot sector...
Checking FAT, Files and Directories...
File size of disk0:/t4 is not correct, correcting it
Reclaiming unused space...
Updating FAT...
Console> (enable)
```

Enter the **dir** command again to see that the corrupted file is corrected:

```
Console> (enable) dir disk0:
      3   -rw-       556    Mar 06 2049 16:26:16 t1
      4   -rw-       556    Mar 06 2049 16:26:16 t2
      5   -rw-       556    Mar 06 2049 16:26:16 t3
      6   -rw-      4096    Mar 06 2049 16:26:16 t4
CORRECT
Console> (enable)
```

Related Commands

dir—switch

history—ROM monitor

To display the command history (the last 16 commands executed in the ROM monitor environment), use the **history** command. This command is aliased to “h” by the ROM monitor for convenience.

history

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Examples

This example shows how to use the **history** command:

```
rommon 13 > history

1   help
2   break -s 0x20090
3   break -s 10090
4   break -s 0xa0001000
5   cont
6   help
7   dev
8   dir
9   dir bootflash:
10  dis
11  dis 0xa0001000
12  dis 0xbe000000
13  history
==============================================================================
```

history—switch

To show the contents of the command history buffer, use the **history** command.

history [**global**]

Syntax Description

global	(Optional) Displays global command history. See the "Usage Guidelines" section for more information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The history buffer size is fixed at 20 commands. See the "Command-Line Interfaces" chapter for detailed information about the command history feature.

The **history** command displays the commands that were entered for the current session (up to 20). The **history global** command displays the last 200 commands that were entered without regard to session.

Examples

In this example, the **history** command lists the contents of the command history buffer:

```
Console> history
       1 help
       2 history
Console> !2
history
       1 help
       2 history
       3 history
Console>
```

l2trace

To display the Layer 2 path taken by the packets that start at a specified source address and end at a specified destination address, use the **l2trace** command.

l2trace *src_mac_addr dest_mac_addr* [*vlan*] [**detail**]

l2trace *src_ip_addr dest_ip_addr* [**detail**]

Syntax Description

src_mac_addr	Source MAC address.
dest_mac_addr	Destination MAC address.
vlan	(Optional) Number of the VLAN.
src_ip_addr	Source IP address or alias.
dest_ip_addr	Destination IP address or alias.
detail	(Optional) Specifies detailed information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Types

Privileged.

Usage Guidelines

All the intermediate devices should be Catalyst 5000 family or Catalyst 6500 series switches running supervisor engine software release 6.1 or later. Catalyst 4500 series switches must be running supervisor engine software release 6.2 or later.

The **l2trace** command displays the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, **l2trace** aborts with an error message.

You must enable CDP on all the Catalyst 4500 series, Catalyst 5000 family, or Catalyst 6500 series switches in the network.

When the switch detects a device (in the Layer 2 path) that does not belong to the Catalyst 4500 series, Catalyst 5000 family, or Catalyst 6500 series switches, the switch continues to send Layer 2 trace queries and lets them time out.

This command is rejected if you enter a multicast source or destination MAC address.

If a source or the destination address belongs to multiple VLANs, you must specify the VLAN to be used for determining the Layer 2 path.

The Layer 2 trace feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors detected on a port). When more than one CDP neighbor is detected on the port, Layer 2 trace is aborted.

If you specify the IP address of the source and destination systems instead of the MAC addresses, the switch looks at the ARP table to determine the IP address to MAC address mapping of the source and destination systems. If an ARP entry exists for the specified IP address, the corresponding MAC address is used. If no matching ARP entry exists, the system does an ARP query and tries to resolve the IP address. If this is the case, a restriction is imposed that requires the source and destination systems to be in the same subnet as the switch in order for the ARP query to be resolved.

Examples

This example shows how to display the Layer 2 packet path for a specified source and destination MAC address:

```
Console> (enable) l2trace 00-01-22-33-44-55 10-22-33-44-55-66 detail
l2trace vlan number is 10.

00-01-22-33-44-55 found in C5500 named wiring-1 on port 4/1 10Mb half duplex
C5500: wiring-1: 192.168.242.10: 4/1 10Mb half duplex -> 5/2 100MB full duplex
C5000: backup-wiring-1: 192.168.242.20: 1/1 100Mb full duplex -> 3/1-4 FEC attached
C5000: backup-core-1: 192.168.242.30: 4/1-4 FEC attached -> 1/1-2 GEC attached
C6000: core-1: 192.168.242.40: 1/1-2 GEC attached -> 2/1 10MB half duplex.
10-22-33-44-55-66 found in C6000 named core-1 on port 2/1 10MB half duplex.
Console> (enable)
```

This example shows how to display the Layer 2 packet path for a specified source and destination IP alias:

```
Console> (enable) l2trace user-1-pc user-2-pc detail
Mapping IP address to MAC Address
user-1-pc -> 00-01-22-33-44-55
user-2-pc -> 10-22-33-44-55-66
l2trace vlan number is 10

00-01-22-33-44-55 found in C5500 named wiring-1 on port 4/1 10Mb half duplex
C5500: wiring-1: 192.168.242.10: 4/1 10Mb half duplex -> 5/2 100MB full duplex
C5000: backup-wiring-1: 192.168.242.20: 1/1 100Mb full duplex -> 3/1-4 FEC attached
C5000: backup-core-1: 192.168.242.30: 4/1-4 FEC attached -> 1/1-2 GEC attached
C6000: core-1: 192.168.242.40: 1/1-2 GEC attached -> 2/1 10MB half duplex.
10-22-33-44-55-66 found in C6000 named core-1 on port 2/1 10MB half duplex.
Console> (enable)
```

This example shows how to display a summary of Layer 2 packet path information for a specified source and destination IP address:

```
Console> (enable) l2trace 9.7.0.7 9.7.0.6
Starting L2 Trace
sc0 :9.7.0.7 : 3/7
4/16 :9.7.0.2 : 4/10
Console> (enable)
```

This example shows how to display a summary of Layer 2 packet path information for a specified source and destination MAC address:

```
Console> (enable) l2trace 00-01-22-33-44-55 10-22-33-44-55-66
Starting L2 Trace
sc0 :9.7.0.7 : 3/7
4/16 :9.7.0.2 : 4/10
Console> (enable)
```

8.6 EFT Copy

meminfo

To display information about the main memory, packet memory, and NVRAM, use the **meminfo** command. With the **-l** option, the supported DRAM configurations are displayed.

meminfo [**-l**]

Syntax Description

-l	(Optional) Specifies the long listing, which displays the DRAM configurations.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

The minus sign (-) is required with the **-l** option.

Examples

This example shows how to use the **meminfo** command:

```
rommon 9 > meminfo

Main memory size: 16 MB in 32 bit mode.
Available main memory starts at 0xa000e000, size 16328KB
IO (packet) memory size: 25 percent of main memory.
NVRAM size: 32KB
```

ping

To send ICMP echo-request packets to another node on the network, use the **ping** command. You can also use the **ping** command without arguments to configure ping.

ping -s *host*

ping -s *host* [*packet_size*] [*packet_count*]

ping

Syntax Description

-s	Causes **ping** to send one datagram per second, printing one line of output for every response received.
host	IP address or IP alias of the host.
packet_size	(Optional) Number of bytes in a packet, from 56 to 1472 bytes.
packet_count	(Optional) Number of packets to send; valid values are from 0 to 2,147,483,647.

Defaults

The defaults for **ping -s** are as follows:

- *packet_size* is 56 bytes
- *packet_count* is 2,147,483,647

The defaults for **ping** with no arguments are as follows:

- *packet_size* is 56 bytes
- *packet_count* is 5
- Wait time is 2 seconds
- Target IP address is none (this is a mandatory field)
- Source address is the host IP address

Command Types

Switch command.

Command Modes

Normal or privileged.

Usage Guidelines

General **ping** command guidelines are as follows:

- Press **Ctrl-C** to stop pinging.
- Continuous ping means that, unless you press **Ctrl-C** to stop pinging, packets are generated continually and dispatched to the host.
- The actual packet size is 8 bytes larger than the size you specify because the switch adds header information.
- Normal response—The normal response occurs in 1 to 10 seconds, depending on network traffic.

The guidelines for the **ping -s** command are as follows:

- The maximum waiting time before timing out is 2 seconds.
- A new ping packet is generated after 1 second of sending the previous packet, regardless of whether or not an echo-reply is received.
- If you do not enter a packet count, continuous ping results.
- Network or host unreachable—The switch found no corresponding entry in the route table.
- Destination does not respond—If the host does not respond, a “no answer from host” appears in 2 seconds.
- Destination unreachable—The gateway for this destination indicates that the destination is unreachable.

The guidelines for the **ping** command without arguments are as follows:

- The **ping** *host* command is accepted in normal mode only. The parameters take the default values automatically.
- The target IP address is a mandatory field to be entered.
- The maximum waiting time is configurable.
- A new ping packet is generated only when an echo-reply is received.
- Entering a packet count of 0 results in continuous ping.
- Returns output only when a response is received or you press **Return**.
- Available in privileged mode only.
- When configuring ping, you must either press **Return** or enter a response. Valid responses and appropriate values are as follows:
  - Target IP address: IP address or host name of the destination node you plan to ping.
  - Number of Packets: Number of ping packets to be sent to the destination address; valid values are from 0 to 2,147,483,647 (0 specifies continuous ping).
  - Datagram size: Size of the ping packet; valid values are from 56 to 1472 bytes.
  - Timeout in seconds: Timeout interval; valid values are from 0 to 3600 seconds.
  - Source IP Address [(default)]: IP address or IP alias of the source.

Examples

This example shows how to ping a host with IP alias elvis a single time:

```
Console> ping elvis
!!!!!

-----172.20.52.19 PING Statistics------
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) min/avg/max = 1/1/1
Console>
```

This example shows how to ping a host with IP alias elvis once per second until you press **Ctrl-C** to stop pinging:

```
Console> ping -s elvis
ping elvis: 56 data bytes
64 bytes from elvis: icmp_seq=0. time=11 ms
64 bytes from elvis: icmp_seq=1. time=8 ms
64 bytes from elvis: icmp_seq=2. time=8 ms
64 bytes from elvis: icmp_seq=3. time=7 ms
```

```
64 bytes from elvis: icmp_seq=4. time=11 ms
64 bytes from elvis: icmp_seq=5. time=7 ms
64 bytes from elvis: icmp_seq=6. time=7 ms
^C

----elvis PING Statistics----
7 packets transmitted, 7 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 7/8/11
Console>
```

This example shows how to configure ping:

```
Console> (enable) ping

Target IP Address []: 172.20.52.19
Number of Packets [5]: 6
Datagram Size [56]: 75
Timeout in seconds [2]: 1
Source IP Address [172.20.52.18]:
!!!!!!

----172.20.52.19 PING Statistics----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 1/1/1
Console> (enable)
```

Related Commands

set interface
set ip route
show interface
show ip route

ping ethernet

To transmit Ethernet CFM loopback messages to a specific destination MAC address, use the **ping ethernet** command.

ping ethernet *dest-mac* **domain** *domain-name* **vlan** *vlan*

ping ethernet *dest-mac* **level** *level* **vlan** *vlan*

ping ethernet *dest-mac* **vlan** *vlan*

Syntax Description

dest-mac	Destination MAC addess for the loopback messages.
domain *domain-name*	Specifies that all maintenance points in a specific domain transmit the ping.
vlan *vlan*	Specifies a VLAN for the traceroute; valid values are from 1 to 4094.
level *level*	Specifies that all maintenance points at a specific maintenance level transmit the ping; valid values are from 0 to 7.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command performs a CFM loopback (Layer 2 ping). It sends a loopback message to a specified MAC address and waits for a response. You must include a VLAN because the switch does not know where a device is located; the same MAC address may be used in different VLANs.

This command only works if CFM is enabled on the switch.

Examples

This example shows how to ping a destination MAC address in VLAN 10:

```
Console> (enable) ping ethernet 00-0a-33-ad-1d-1b vlan 10
Sending 5, 100-byte Ethernet CFM Echoes to aa-bb-cc-dd-ee-ff, timeout is 2 seconds:
.!!!!
Success Rate is 80 percent (4/5), round-trip min/avg/max  = 1/1/4 ms
Console> (enable)
```

pwd

To show the current setting of the **cd** command, use the **pwd** command.

pwd [[*m/*]*device***:**]

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device***:**	(Optional) Device where the Flash resides.

Defaults

If no module number or device is specified, **pwd** defaults to the first module of the active device.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

Examples

This example shows how to use the **pwd** command to display the current listing of the **cd** command:

```
Console> cd slot0:
Default flash device set to slot0.
Console> pwd
slot0
```

Related Commands

cd

quit

To exit a CLI session, use the **quit** command.

quit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **exit** and **logout** commands perform the same function as the **quit** command.

Examples

This example shows how to quit a CLI session:

```
Console> quit
Connection closed by foreign host.
host%
```

reconfirm vmps

To reconfirm the current dynamic port VLAN membership assignments with the VMPS server, use the **reconfirm vmps** command.

reconfirm vmps

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

VMPS database changes are not conveyed automatically to switches participating in VMPS. Therefore, after making a VMPS database change, use this command on VMPS clients and servers to apply the database changes.

Examples

This example shows how to reconfirm the current dynamic port VLAN membership with VMPS:

```
Console> (enable) reconfirm vmps
reconfirm process started
Use 'show dvlan statistics' to see reconfirm status
Console> (enable)
```

Related Commands

show dvlan statistics

reload

To force a module to accept a download through SCP, use the **reload** command. This command resets the module and prompts you to initiate a download when the reset is complete.

reload *module*

Syntax Description

module	Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is used if a module is accidently reset during the downloading of an image. After the reset, a normal download will not work. You must enter the **reload** *module* command followed by the **download** *host file* [*mod*] command.

You cannot use the **reload** command on the MSFC.

Examples

This example shows how to reset module 3 and download the acpflash_1111.bbi file from the mercury host to the module:

```
Console> (enable) reload 3
Console> (enable) download mercury acpflash_1111.bbi 3
This command will reset Module 3.
Download image acpflash_1111.bbi from mercury to Module 3 FLASH (y/n) [n]? y
/
Done.  Finished network download.  (1964012 bytes)
Console> (enable)
```

Related Commands

download

repeat

To repeat a command, use the **repeat** command.

repeat [*num* | *string*]

Syntax Description

number	(Optional) Number of the command.
string	(Optional) Command string.

Defaults

If no argument is specified, the last command is repeated.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

The optional command number (from the history buffer list) or match string specifies which command to repeat.

In the match string, the most recent command to begin with the specified string is executed again.

If the string contains white space, you must use quotation marks.

This command is usually aliased to the letter “r.”

Examples

These examples show how to use the **repeat** command. You use the **history** command to display the list of previously entered commands:

```
rommon 22 > history

8   dir
9   dir bootflash:
10   dis
11   dis 0xa0001000
12   dis 0xbe000000
13   history
14   meminfo
15   meminfo -l
16   meminfo
17   meminfo -l
18   meninfo
19   meminfo
20   meminfo -l
21   meminfo -l
22   history
```

```
rommon 23 > repeat dir
dir bootflash:
         File size           Checksum   File name
   1973032 bytes (0x1e1b28)   0xdadf5e24    llue
rommon 24 > repeat
dir bootflash:
         File size           Checksum   File name
   1973032 bytes (0x1e1b28)   0xdadf5e24    llue
rommon 25 > repeat 15
meminfo -l

Main memory size: 16 MB.
Packet memory size: 0 MB
Main memory size: 0x1000000
Available main memory starts at 0xa000e000, size 0xff2000
NVRAM size: 0x20000

Parity Map for the DRAM Banks
Socket 0 in Bank 0 Has No Parity
Socket 1 in Bank 0 Has No Parity
Socket 0 in Bank 1 Has No Parity
Socket 1 in Bank 1 Has No Parity
==========================================================================
```

reset—ROM monitor

To perform a soft reset of the switch, use the **reset** ROM monitor command.

reset [-**s**]

Syntax Description

-s	(Optional) Resets the entire switch.

Defaults

The default Flash device is slot0.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

This command will not boot the MSFC if the PFC is not present in the Catalyst 6500 series switch.

Examples

This example shows how to use the **reset** command:

```
rommon 26 > reset

System Bootstrap, Version 3.1(1.69)
Copyright (c) 1994-1997 by cisco Systems, Inc.
Supervisor processor with 16384 Kbytes of main memory

rommon 1 >
============================================================================
```

reset—switch

To restart the system or an individual module, schedule a system reset, or cancel a scheduled reset, use the **reset** command.

reset [*mod* | **system** | **mindown**]

reset [**mindown**] **at** {*hh:mm*} [*mm/dd*] [*reason*]

reset [**mindown**] **in** [*hh*:] {*mm*} [*reason*]

reset [**cancel**]

reset {*mod*} [*bootdevice*[,*bootdevice*]]

reset powersupply {**1** | **2**}

Syntax Description

mod	(Optional) Number of the module to be restarted.
system	(Optional) Resets the system.
mindown	(Optional) Performs a reset as part of a minimal downtime software upgrade in a system with a redundant supervisor engine.
at	Schedules a system reset at a specific future time.
hh:mm	Hour and minute of the scheduled reset.
mm/dd	(Optional) Month and day of the scheduled reset.
reason	(Optional) Reason for the reset.
in	Schedules a system reset in a specific time.
hh	(Optional) Number of hours into the future to reset the switch.
mm	Number of minutes into the future to reset the switch.
cancel	(Optional) Cancels the scheduled reset.
mod	Number of the Network Analysis Module (NAM) or Intrusion Detection System Module (IDSM).
bootdevice	(Optional) Boot device identification; for format guidelines, see the “Usage Guidelines” section.
powersupply	Resets the specified power supply.
1 | **2**	Specifies power supply 1 or power supply 2.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a module number (either a switching module or the active supervisor engine module), the command resets the entire system.

You can use the **reset** *mod* command to switch to the redundant supervisor engine, where *mod* is the module number of the active supervisor engine.

You can use the **reset mindown** command to reset the switch as part of a minimal downtime software upgrade in a system with a redundant supervisor engine. For complete information on performing a minimal downtime software upgrade, refer to the *Catalyst 6500 Series Software Configuration Guide* for your switch.

Caution If you make configuration changes after entering the **reset mindown** command but before the active supervisor engine resets, the changes are not saved. Input from the CLI is still accepted by the switch while the redundant supervisor engine is reset. Changes that you make to the configuration between the time when you enter the **reset mindown** command and the time when the supervisor engine comes online running the new software image are not saved or synchronized with the redundant supervisor engine.

If you reset an intelligent module (such as the Catalyst 6500 series MSM or MSFC), both the module hardware and software are completely reset.

When entering the *bootdevice*, use the format *device*[:*device_qualifier*] where:

- *device* = **pcmcia**, **hdd**, **network**
- *device_qualifier* **hdd** = number from 1 to 99
- **pcmcia** = slot0 or slot1

You can only reset a power supply for those power supplies that are capable of power cycling.

Examples

This example shows how to reset the supervisor engine on a Catalyst 6500 series switch with redundant supervisor engines:

```
Console> (enable) reset 1
This command will force a switch-over to the standby supervisor module
and disconnect your telnet session.
Do you want to continue (y/n) [n]? y
Connection closed by foreign host.
host%
```

This example shows how to reset module 4:

```
Console> (enable) reset 4
This command will reset module 4 and may disconnect your telnet session.
Do you want to continue (y/n) [n]? y
Resetting module 4...
Console> (enable)
```

This example shows how to schedule a system reset for a specific future time:

```
Console> (enable) reset at 20:00
Reset scheduled at 20:00:00, Wed Mar 15 2000.
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 20:00:00, Wed Mar 15 2000 (in 0 day 5 hours 40 minutes).
Console> (enable)
```

This example shows how to schedule a reset for a specific future time and include a reason for the reset:

```
Console> (enable) reset at 23:00 3/15 Software upgrade to 6.1(1).
Reset scheduled at 23:00:00, Wed Mar 15 2000.
Reset reason: Software upgrade to 6.1(1).
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 23:00:00, Wed Mar 15 2000 (in 0 day 8 hours 39 minutes).
Console> (enable)
```

This example shows how to schedule a reset with minimum downtime for a specific future time and include a reason for the reset:

```
Console> (enable) reset mindown at 23:00 3/15 Software upgrade to 6.1(1).
Reset scheduled at 23:00:00, Wed Mar 15 2000.
Reset reason: Software upgrade to 6.1(1).
Proceed with scheduled reset? (y/n) [n]? y
Reset mindown scheduled for 23:00:00, Wed Mar 15 2000 (in 0 day 8 hours 39 minutes).
Console> (enable)
```

This example shows how to schedule a reset after a specified time:

```
Console> (enable) reset in 5:20 Configuration update
Reset scheduled in 5 hours 20 minutes.
Reset reason: Configuration update
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 19:56:01, Wed Mar 15 2000 (in 5 hours 20 minutes).
Reset reason: Configuration update
Console> (enable)
```

This example shows how to cancel a scheduled reset:

```
Console> (enable) reset cancel
Reset cancelled.
Console> (enable)
```

This example shows how to reset power supply 1:

```
Console> (enable) reset powersupply 1
This command will reset the powersupply 1 Do you want to continue (y/n) [n]? y
Powersupply 1 reset successful.
Console> (enable)
```

This example shows the message that is displayed when the power supply is not capable of power cycling:

```
Console> (enable) reset powersupply 2
Powersupply 2 is not powercycle capable
Console> (enable)
```

Related Commands

commit
show reset

restore counters

To restore MAC and port counters, use the **restore counters** command.

restore counters [**all** | *mod/ports*]

restore counters channel {**all** | *channel-id*}

restore counters lacp-channel {**all** | *channel-id*}

Syntax Description

all	(Optional) Restores all ports.
mod/ports	(Optional) Number of the module and the ports on the module.
channel	Restores PAgP channel MAC and port counters.
all	Restores MAC and port counters for all PAgP channels.
channel_id	Number of a specific PAgP channel.
lacp-channel	Restores LACP channel MAC and port counters.
all	Restores MAC and port counters for all LACP channels.
channel_id	Number of a specific LACP channel.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a range of ports to be restored, then all ports on the switch are restored.

To restore channel-based counters on a per-channel basis, use the channel ID number. Enter the **show port channel** command to find the channel ID number for PAgP channels. Enter the **show port lacp-channel** command to find the channel ID number for LACP channels.

Examples

This example shows how to restore MAC counters and port counters:

```
Console> (enable) restore counters all
This command will restore all counter values reported by the CLI to the hardware counter
values.
Do you want to continue (y/n) [n]? y
MAC and Port counters restored.
Console> (enable)
```

This example shows how to restore the counters for channel 769:

```
Console> (enable) restore counter channel 769
This command will restore counter values reported by the CLI
for PAGP channel 769 ports to the hardware counter values.
Do you want to continue (y/n) [n]? y
MAC and Port counters restored.
Console> (enable)
```

Related Commands

clear counters
show channel traffic
show port channel
show port counters
show port lacp-channel

rollback

To clear changes made to the ACL edit buffer since its last save, use the **rollback** command. The ACL is rolled back to its state at the last **commit** command.

rollback qos acl {*acl_name* | **all**}

rollback security acl {*acl_name* | **all** | **adjacency**}

Syntax Description

qos acl	Specifies QoS ACEs.
acl_name	Name that identifies the VLAN access control list (VACL) whose ACEs are to be affected.
all	Rolls back all ACLs.
security acl	Specifies security ACEs.
adjacency	Rolls back all adjacency tables.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the edit buffer of a specific QoS ACL:

```
Console> (enable) rollback qos acl ip-8-1
Rollback for QoS ACL ip-8-1 is successful.
Console> (enable)
```

This example shows how to clear the edit buffer of a specific security ACL:

```
Console> (enable) rollback security acl IPACL1
IPACL1 editbuffer modifications cleared.
Console> (enable)
```

Related Commands

commit
show qos acl info

8.6 EFT Copy

session

To open a session with a module (for example, the MSM, NAM, or ATM), use the **session** command. This command allows you to use the module-specific CLI.

session *mod*

Syntax Description

mod	Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After you enter this command, the system responds with the Enter Password: prompt, if one is configured on the module.

To end the session, enter the **quit** command.

Use the **session** command to toggle between router and switch sessions.

For information on ATM commands, refer to the *ATM Software Configuration Guide and Command Reference for the Catalyst 5000 Family and 6500 Series Switches*.

For information on NAM commands, refer to the *Catalyst 6000 Family Network Analysis Module Installation and Configuration Note* and the *Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module Command Reference*.

Examples

This example shows how to open a session with an MSM (module 4):

```
Console> session 4
Trying Router-4...
Connected to Router-4.
Escape character is `^]'.

Router>
```

Related Commands

quit
switch console

set

To display all of the ROM monitor variable names with their values, use the **set** command.

set

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Examples

This example shows how to display all of the ROM monitor variable names with their values:

```
rommon 2 > set
PS1=rommon ! >
BOOT=
?=0
```

Related Commands

varname=

set accounting commands

To enable command event accounting on the switch, use the **set accounting commands** command.

set accounting commands enable {**config** | **enable** | **all**} [**stop-only**] {**tacacs+**}

set accounting commands disable

Syntax Description

enable	Enables the specified accounting method for commands.
config	Permits accounting for configuration commands only.
enable	Permits accounting for enable mode commands only.
all	Permits accounting for all commands.
stop-only	(Optional) Applies the accounting method at the command end.
tacacs+	Specifies TACACS+ accounting for commands.
disable	Disables accounting for commands.

Defaults

The default is accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure the TACACS+ servers before you enable accounting.

Examples

This example shows how to send records at the end of the event only using a TACACS+ server:

```
Console> (enable) set accounting commands enable config stop-only tacacs+
Accounting set to enable for commands-config events in stop-only mode.
Console> (enable)
```

Related Commands

set accounting connect
set accounting exec
set accounting suppress
set accounting system
set accounting update
set tacacs server
show accounting

set accounting connect

To enable accounting of outbound connection events on the switch, use the **set accounting connect** command.

set accounting connect enable {**start-stop** | **stop-only**} {**tacacs+** | **radius**}

set accounting connect disable

Syntax Description

enable	Enables the specified accounting method for connection events.
start-stop	Applies the accounting method at the start and stop of the connection event.
stop-only	Applies the accounting method at the end of the connection event.
tacacs+	Specifies TACACS+ accounting for connection events.
radius	Specifies RADIUS accounting for connection events.
disable	Disables accounting of connection events.

Defaults

The default is accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure the RADIUS or TACACS+ servers and shared secret keys before you enable accounting.

Examples

This example shows how to enable accounting on Telnet and remote login sessions, generating records at stop only using a TACACS+ server:

```
Console> (enable) set accounting connect enable stop-only tacacs+
Accounting set to enable for connect events in stop-only mode.
Console> (enable)
```

Related Commands

set accounting commands
set accounting exec
set accounting suppress
set accounting system
set accounting update
set radius key
set radius server
set tacacs key
set tacacs server
show accounting

set accounting exec

To enable accounting of normal login sessions on the switch, use the **set accounting exec** command.

set accounting exec enable {**start-stop** | **stop-only**} {**tacacs+** | **radius**}

set accounting exec disable

Syntax Description

enable	Enables the specified accounting method for normal login sessions.
start-stop	Specifies the accounting method applies at the start and stop of the normal login sessions.
stop-only	Specifies the accounting method applies at the end of the normal login sessions.
tacacs+	Specifies TACACS+ accounting for normal login sessions.
radius	Specifies RADIUS accounting for normal login sessions.
disable	Disables accounting for normal login sessions.

Defaults

The default is accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure the RADIUS or TACACS+ servers and shared secret keys before you enable accounting.

Examples

This example shows how to enable accounting of normal login sessions, generating records at start and stop using a RADIUS server:

```
Console> (enable) set accounting exec enable start-stop radius
Accounting set to enable for exec events in start-stop mode.
Console> (enable)
```

This example shows how to enable accounting of normal login sessions, generating records at stop using a TACACS+ server:

```
Console> (enable) set accounting exec enable stop-only tacacs+
Accounting set to enable for exec events in stop-only mode.
Console> (enable)
```

Related Commands

set accounting commands
set accounting connect
set accounting suppress
set accounting system
set accounting update
set radius key
set radius server
set tacacs key
set tacacs server
show accounting

8.6 EFT Copy

set accounting suppress

To enable or disable suppression of accounting information for a user who has logged in without a username, use the **set accounting suppress** command.

set accounting suppress null-username {**enable** | **disable**}

Syntax Description

null-username	Specifies users must have a user ID.
enable	Enables suppression for a specified user.
disable	Disables suppression for a specified user.

Defaults

The default is accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure the TACACS+ servers before you enable accounting.

Examples

This example shows how to suppress accounting information for users without a username:

```
Console> (enable) set accounting suppress null-username enable
Accounting will be suppressed for user with no username.
Console> (enable)
```

This example shows how to include users without the username accounting event information:

```
Console> (enable) set accounting suppress null-username disable
Accounting will be not be suppressed for user with no username.
Console> (enable)
```

Related Commands

set accounting commands
set accounting connect
set accounting exec
set accounting system
set accounting update
set tacacs server
show accounting

set accounting system

To enable accounting of system events on the switch, use the **set accounting system** command.

set accounting system enable {**start-stop** | **stop-only**} {**tacacs+** | **radius**}

set accounting system disable

Syntax Description

enable	Enables the specified accounting method for system events.
start-stop	Specifies the accounting method applies at the start and stop of the system event.
stop-only	Specifies the accounting method applies at the end of the system event.
tacacs+	Specifies TACACS+ accounting for system events.
radius	Specifies RADIUS accounting for system events.
disable	Disables accounting for system events.

Defaults

The default is accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure the RADIUS or TACACS+ servers and shared secret keys before you enable accounting.

Examples

This example shows how to enable accounting for system events, sending records only at the end of the event using a RADIUS server:

```
Console> (enable) set accounting system enable stop-only radius
Accounting set to enable for system events in start-stop mode.
Console> (enable)
```

This example shows how to enable accounting for system events, sending records only at the end of the event using a TACACS+ server:

```
Console> (enable) set accounting system enable stop-only tacacs+
Accounting set to enable for system events in start-stop mode.
Console> (enable)
```

Related Commands

set accounting commands
set accounting connect
set accounting exec
set accounting suppress
set accounting update
set radius key
set radius server
set tacacs key
set tacacs server
show accounting

set accounting update

To configure the frequency of accounting updates, use the **set accounting update** command.

set accounting update {**new-info** | {**periodic** [*interval*]}}

Syntax Description

new-info	Specifies an update when new information is available.
periodic	Specifies an update on a periodic basis.
interval	(Optional) Periodic update interval time; valid values are from 1 to 71582 minutes.

Defaults

The default is accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure the TACACS+ servers before you enable accounting.

Examples

This example shows how to send accounting updates every 200 minutes:

```
Console> (enable) set accounting update periodic 200
Accounting updates will be periodic at 200 minute intervals.
Console> (enable)
```

This example shows how to send accounting updates only when there is new information:

```
Console> (enable) set accounting update new-info
Accounting updates will be sent on new information only.
Console> (enable)
```

Related Commands

set accounting commands
set accounting connect
set accounting exec
set accounting suppress
set accounting system
set tacacs server
show accounting

set acllog ratelimit

To limit the number of packets sent to the route processor CPU for bridged ACEs, use the **set acllog ratelimit** command.

set acllog ratelimit *rate*

Syntax Description

rate	Number of packets per second; valid values are 1 to 1000. See the "Usage Guidelines" section for more information.

Defaults

ACL log rate limiting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After entering the **set acllog ratelimit** command or the **clear acllog** command, you must either reset the route processor or perform a shut/not shut on the route processor interfaces that have ACEs with the **log** keyword applied.

After entering the **set acllog ratelimit** command, the reset or shut/no shut action causes the bridged ACEs to be redirected to the route processor with rate limiting.

To disable ACL log rate limiting, enter the **clear acllog** command. After entering the **clear acllog** command, the reset or shut/no shut action causes the system to return to its previous behavior. The bridge action remains unchanged.

If the number of packets per second is greater than the rate that you specify, the packets that exceed the specified rate are dropped.

A *rate* value of 500 is recommended.

Examples

This example shows how to enable ACL logging and to specify a rate of 500 for rate limiting:

```
Console> (enable) set acllog ratelimit 500
If the ACLs-LOG were already applied, the rate limit mechanism will be effective on system
restart, or after shut/no shut the interface.
Console> (enable)
```

Related Commands

clear acllog
show acllog

set acl mac-packet-classify

To set MAC-based ACL lookups for all packet types on a VLAN, use the **set acl mac-packet-classify** command.

set acl mac-packet-classify {*vlans* | **all**}

Syntax Description

vlans	VLAN list; valid values are 1 to 4094.
all	Specifies all VLANs.

Defaults

The MAC-based ACL lookups for all packet types are disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The MAC-based ACL lookup feature is available only on a system with a PFC3B or a PFC3BXL. This feature affects both security ACLs and QoS MAC ACLs.

You should only enable this feature on Layer 2 VLANs. If you want to enable this feature on Layer 3 VLANs, note the following:

- You will lose some Layer 3 features, as indicated by this message, which appears when you enable MAC-based ACLs on a Layer 3 VLAN:

```
Warning: IP RACLs, VACLs & some IP features will be ineffective on these vlans.
```

- You might see an inconsistency in the egress ACL lookup depending on whether the packet is forwarded by the software or by the hardware. We recommend that you enable this feature on all VLANs to eliminate this inconsistency.

Examples

This example shows how to enable the MAC-based ACL feature on a VLAN:

```
Console> (enable) set acl mac-packet-classify 5
Enabled mac-packet-classify on vlan(s) 5.
Warning: IP RACLs, VACLs & some IP features will be ineffective on these vlans.
Console> (enable)
```

Related Commands

clear acl mac-packet-classify
show acl mac-packet-classify

set alias

To define aliases (shorthand versions) of commands, use the **set alias** command.

set alias *name command* [*parameter*] [*parameter*]

Syntax Description

name	Alias being created.
command	Command for which the alias is being created.
parameter	(Optional) Parameters that apply to the command for which an alias is being created.

Defaults

The default is no aliases are configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The name **all** cannot be defined as an alias. Reserved words cannot be defined as aliases.

You can set a maximum of 100 aliases on the switch.

For additional information about the *parameter* value, see the specific command for information about applicable parameters.

Examples

This example shows how to set the alias for the **clear arp** command as arpdel:

```
Console> (enable) set alias arpdel clear arp
Command alias added.
Console> (enable)
```

Related Commands

clear alias
show alias

set arp

To add IP address-to-MAC address mapping entries to the ARP table and to set the ARP aging time for the table, use the **set arp** command.

set arp [**dynamic** | **permanent** | **static**] {*ip_addr hw_addr*}

set arp agingtime *agingtime*

Syntax Description

dynamic	(Optional) Specifies that entries are subject to ARP aging updates.
permanent	(Optional) Specifies that permanent entries are stored in NVRAM until they are removed by the **clear arp** or **clear config** command.
static	(Optional) Specifies that entries are not subject to ARP aging updates.
ip_addr	IP address or IP alias to map to the specified MAC address.
hw_addr	MAC address to map to the specified IP address or IP alias.
agingtime	Sets the period of time after which an ARP entry is removed from the ARP table.
agingtime	Number of seconds that entries will remain in the ARP table before being deleted; valid values are from 0 to 1,000,000 seconds. Setting this value to **0** disables aging.

Defaults

The default is no ARP table entries exist; ARP aging is set to 1200 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When entering the *hw_addr* value, use a 6-hexadecimal byte MAC address in canonical (00-11-22-33-44-55) or noncanonical (00:11:22:33:44:55) format.

Static (nonpermanent) entries remain in the ARP table until you reset the active supervisor engine.

Examples

This example shows how to configure a dynamic ARP entry mapping that will age out after the configured ARP aging time:

```
Console> (enable) set arp dynamic 198.133.219.232 00-00-0c-40-0f-bc
ARP entry added.
Console> (enable)
```

This example shows how to set the aging time for the ARP table to 1800 seconds:

```
Console> (enable) set arp agingtime 1800
ARP aging time set to 1800 seconds.
Console> (enable)
```

This example shows how to configure a permanent ARP entry, which will remain in the ARP cache after a system reset:

```
Console> (enable) set arp permanent 198.146.232.23 00-00-0c-30-0f-bc
Permanent ARP entry added as
198.146.232.23 at 00-00-0c-30-0f-bc on vlan 5
Console> (enable)
```

This example shows how to configure a static ARP entry, which will be removed from the ARP cache after a system reset:

```
Console> (enable) set arp static 198.144.239.22 00-00-0c-50-0f-bc
Static ARP entry added as
198.144.239.22 at 00-00-0c-50-0f-bc on vlan 5
Console> (enable)
```

Related Commands

clear arp
show arp

set authentication enable

To enable authentication using the TACACS+, RADIUS, or Kerberos server to determine if you have privileged access permission, use the **set authentication enable** command.

set authentication enable {**radius** | **tacacs** | **kerberos**} **enable** [**console** | **telnet** | **http** | **all**] [**primary**]

set authentication enable {**enable** | **disable**} [**console** | **telnet** | **http** | **all**] [**primary**]

set authentication enable local {**enable** | **disable**} [**console** | **telnet** | **http** | **all**] [**primary**]

set authentication enable attempt *count* [**console** | **telnet**]

set authentication enable lockout *time* [**console** | **telnet**]

Syntax Description

radius	Specifies RADIUS authentication for login.
tacacs	Specifies TACACS+ authentication for login.
kerberos	Specifies Kerberos authentication for login.
enable	Enables the specified authentication method for login.
console	(Optional) Specifies the authentication method for console sessions.
telnet	(Optional) Specifies the authentication method for Telnet sessions.
http	(Optional) Specifies the specified authentication method for HTTP sessions.
all	(Optional) Applies the authentication method to all session types.
primary	(Optional) Specifies the specified authentication method be tried first.
disable	Disables the specified authentication method for login.
local	Specifies local authentication for login.
attempt *count*	Specifies the number of connection attempts before initiating an error; valid values are 0, from 3 to 10, and 0 to disable.
lockout *time*	Specifies the lockout timeout; valid values are from 30 to 600 seconds, and 0 to disable.

Defaults

Local authentication is enabled for console and Telnet sessions. RADIUS, TACACS+, and Kerberos are disabled for all session types. If authentication is enabled, the default **attempt** *count* is 3.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use authentication configuration for both console and Telnet connection attempts unless you use the **console** or **telnet** keywords to specify the authentication methods for each connection type individually.

Examples

This example shows how to use the TACACS+ server to determine if a user has privileged access permission:

```
Console> (enable) set authentication enable tacacs enable
tacacs enable authentication set to enable for console, telnet and http session.
Console> (enable)
```

This example shows how to use the local password to determine if the user has privileged access permission:

```
Console> (enable) set authentication enable local enable
local enable authentication set to enable for console, telnet and http session.
Console> (enable)
```

This example shows how to use the RADIUS server to determine if a user has privileged access permission for all session types:

```
Console> (enable) set authentication enable radius enable
radius enable authentication set to enable for console, telnet and http session.
Console> (enable)
```

This example shows how to use the TACACS+ server to determine if a user has privileged access permission for all session types:

```
Console> (enable) set authentication enable tacacs enable console
tacacs enable authentication set to enable for console session.
Console> (enable)
```

This example shows how to set the Kerberos server to be used first:

```
Console> (enable) set authentication enable kerberos enable primary
kerberos enable authentication set to enable for console, telnet and http session as
primary authentication method.
Console> (enable)
```

This example shows how to limit enable mode login attempts:

```
Console> (enable) set authentication enable attempt 5
Enable mode authentication attempts for console and telnet logins set to 5.
Console> (enable)
```

This example shows how to set the enable mode lockout time for both console and Telnet connections:

```
Console> (enable) set authentication enable lockout 50
Enable mode lockout time for console and telnet logins set to 50.
Console> (enable)
```

Related Commands

set authentication login
show authentication

set authentication login

To enable TACACS+, RADIUS, or Kerberos as the authentication method for login, use the **set authentication login** command.

set authentication login {**radius** | **tacacs** | **kerberos**} **enable** [**console** | **telnet** | **http** | **all**] [**primary**]

set authentication login {**radius** | **tacacs** | **kerberos**} **disable** [**console** | **telnet** | **http** | **all**]

set authentication login {**enable** | **disable**} [**console** | **telnet** | **http** | **all**]

set authentication login local {**enable** | **disable**} [**console** | **telnet** | **http** | **all**]

set authentication login attempt *count* [**console** | **telnet**]

set authentication login lockout *time* [**console** | **telnet**]

Syntax Description

radius	Specifies the use of the RADIUS server password to determine if you have access permission to the switch.
tacacs	Specifies the use of the TACACS+ server password to determine if you have access permission to the switch.
kerberos	Specifies the Kerberos server password to determine if you have access permission to the switch.
enable	Enables the specified authentication method for login.
console	(Optional) Specifies the authentication method for console sessions.
telnet	(Optional) Specifies the authentication method for Telnet sessions.
http	(Optional) Specifies the authentication method for HTTP sessions.
all	(Optional) Specifies the authentication method for all session types.
primary	(Optional) Specifies that the method specified is the primary authentication method for login.
disable	Disables the specified authentication method for login.
local	Specifies a local password to determine if you have access permission to the switch.
attempt *count*	Specifies the number of login attempts before initiating an error; valid values are 0, from 3 to 10, and 0 to disable.
lockout *time*	Specifies the lockout timeout; valid values are from 30 to 43200 seconds, and 0 to disable.

Defaults

Local authentication is the primary authentication method for login.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command allows you to choose the authentication method for the web interface. If you configure the authentication method for the HTTP session as RADIUS, then the username or password is validated using the RADIUS protocol, and TACACS+ and Kerberos authentication is set to disable for the HTTP sessions. By default, the HTTP login is validated using the local login password.

You can specify the authentication method for **console**, **telnet**, **http**, or **all** by entering the **console**, **telnet**, **http**, or **all** keywords. If you do not specify **console**, **telnet**, **http**, or **all**, the authentication method default is for **all** sessions.

Examples

This example shows how to disable TACACS+ authentication access for Telnet sessions:

```
Console> (enable) set authentication login tacacs disable telnet
tacacs login authentication set to disable for the telnet sessions.
Console> (enable)
```

This example shows how to disable RADIUS authentication access for console sessions:

```
Console> (enable) set authentication login radius disable console
radius login authentication set to disable for the console sessions.
Console> (enable)
```

This example shows how to disable Kerberos authentication access for Telnet sessions:

```
Console> (enable) set authentication login kerberos disable telnet
kerberos login authentication set to disable for the telnet sessions.
Console> (enable)
```

This example shows how to set TACACS+ authentication access as the primary method for HTTP sessions:

```
Console> (enable) set authentication login tacacs enable http primary
tacacs login authentication set to enable for HTTP sessions as primary authentification
method.
Console> (enable)
```

This example shows how to limit login attempts:

```
Console> (enable) set authentication login attempt 5
Login authentication attempts for console and telnet logins set to 5.
Console> (enable)
```

This example shows how to set the lockout time for both console and Telnet connections:

```
Console> (enable) set authentication login lockout 50
Login lockout time for console and telnet logins set to 50.
Console> (enable)
```

Related Commands

set authentication enable
show authentication

set authorization commands

To enable authorization of command events on the switch, use the **set authorization commands** command.

set authorization commands enable {**config** | **enable** | **all**} {*option*} {*fallbackoption*} [**console** | **telnet** | **both**]

set authorization commands disable [**console** | **telnet** | **both**]

Syntax Description

enable	Enables the specified authorization method for commands.
config	Permits authorization for configuration commands only.
enable	Permits authorization for enable mode commands only.
all	Permits authorization for all commands.
option	Switch response to an authorization request; valid values are **tacacs+**, **if-authenticated**, and **none**. See the “Usage Guidelines” section for valid value definitions.
fallbackoption	Switch fallback response to an authorization request if the TACACS+ server is down or not responding; valid values are **tacacs+**, **deny**, **if-authenticated**, and **none**. See the “Usage Guidelines” section for valid value definitions.
disable	Disables authorization of command events.
console	(Optional) Specifies the authorization method for console sessions.
telnet	(Optional) Specifies the authorization method for Telnet sessions.
both	(Optional) Specifies the authorization method for both console and Telnet sessions.

Defaults

The default is authorization is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you define the *option* and *fallbackoption* values, the following occurs:

- **tacacs+** specifies the TACACS+ authorization method.
- **deny** does not let you proceed.
- **if-authenticated** allows you to proceed with your action if you have been authenticated.
- **none** allows you to proceed without further authorization in case the TACACS+ server does not respond.

Examples

This example shows how to enable authorization for all commands with the **if-authenticated** *option* and **none** *fallbackoption*:

```
Console> (enable) set authorization commands enable all if-authenticated none
Successfully enabled commands authorization.
Console> (enable)
```

This example shows how to disable command authorization:

```
Console> (enable) set authorization commands disable
Successfully disabled commands authorization.
Console> (enable)
```

Related Commands

set authorization enable
set authorization exec
show authorization

set authorization enable

To enable authorization of privileged mode sessions on the switch, use the **set authorization enable** command.

set authorization enable enable {*option*} {*fallbackoption*} [**console** | **telnet** | **both**]

set authorization enable disable [**console** | **telnet** | **both**]

Syntax Description

enable	Enables the specified authorization method.
option	Switch response to an authorization request; valid values are **tacacs+**, **if-authenticated**, and **none**. See the "Usage Guidelines" section for valid value definitions.
fallbackoption	Switch fallback response to an authorization request if the TACACS+ server is down or not responding; valid values are **tacacs+**, **deny**, **if-authenticated**, and **none**. See the "Usage Guidelines" section for valid value definitions.
disable	Disables the authorization method.
console	(Optional) Specifies the authorization method for console sessions.
telnet	(Optional) Specifies the authorization method for Telnet sessions.
both	(Optional) Specifies the authorization method for both console and Telnet sessions.

Defaults

The default is authorization is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you define the *option* and *fallbackoption* values, the following occurs:

- **tacacs+** specifies the TACACS+ authorization method.
- **deny** does not let you proceed.
- **if-authenticated** allows you to proceed with your action if you have authentication.
- **none** allows you to proceed without further authorization in case the TACACS+ server does not respond.

Examples

This example shows how to enable authorization of configuration commands in enable, privileged login mode, sessions:

```
Console> (enable) set authorization enable enable if-authenticated none
Successfully enabled enable authorization.
Console> (enable)
```

This example shows how to disable enable mode authorization:

```
Console> (enable) set authorization enable disable
Successfully disabled enable authorization.
Console> (enable)
```

Related Commands

set authorization commands
set authorization exec
show authorization

set authorization exec

To enable authorization of exec (normal mode) session events on the switch, use the **set authorization exec** command.

set authorization exec enable {*option*} {*fallbackoption*} [**console** | **telnet** | **both**]

set authorization exec disable [**console** | **telnet** | **both**]

Syntax Description

enable	Enables the specified authorization method.
option	Switch response to an authorization request; valid values are **tacacs+**, **if-authenticated**, and **none**. See the "Usage Guidelines" section for valid value definitions.
fallbackoption	Switch fallback response to an authorization request if the TACACS+ server is down or not responding; valid values are **tacacs+**, **deny**, **if-authenticated**, and **none**. See the "Usage Guidelines" section for valid value definitions.
disable	Disables authorization method.
console	(Optional) Specifies the authorization method for console sessions.
telnet	(Optional) Specifies the authorization method for Telnet sessions.
both	(Optional) Specifies the authorization method for both console and Telnet sessions.

Defaults

The default is authorization is denied.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you define the *option* and *fallbackoption* values, the following occurs:

- **tacacs+** specifies the TACACS+ authorization method.
- **deny** fails authorization if the TACACS+ server does not respond.
- **if-authenticated** allows you to proceed with your action if the TACACS+ server does not respond and you have authentication.
- **none** allows you to proceed without further authorization if the TACACS+ server does not respond.

Examples

This example shows how to enable authorization of configuration commands in exec (normal mode) session events:

```
Console> (enable) set authorization exec enable if-authenticated none
Successfully enabled exec authorization.
Console> (enable)
```

This example shows how to disable exec mode authorization:

```
Console> (enable) set authorization exec disable
Successfully disabled exec authorization.
Console> (enable)
```

Related Commands

set authorization commands
set authorization enable
show authorization

set autoshut

To enable or disable automatic module shutdown, use the **set autoshut** command.

set autoshut {**frequency** *num*}

set autoshut {**period** *minutes*}

Syntax Description

frequency *num*	Sets the number of times that the module can reset itself before shutting down; valid values are from 1 to 255 times.
period *minutes*	Sets the time period in which the number of resets must occur; valid values are from 0 to 255 minutes. See the "Usage Guidelines" section for more information.

Defaults

The defaults are as follows:

- *num* is three times.
- *minutes* is two minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can shut down a module manually using the **set module disable** or the **set module power down** commands.

After the module shuts down, you must reenable the module manually.

You must configure these two parameters before an automatic shutdown can occur:

- Frequency—Allows you to specify the threshold value for an automatic module shutdown. When the number of resets reaches the value that is assigned to this option, the Ethernet module can perform an automatic shutdown.
- Period—Allows you to specify the time period in which the number of resets must occur (as configured with the **frequency** keyword). The period is measured from one these conditions:
  - When the switch first comes up
  - When the supervisor engine performs a switchover
  - When the Ethernet module is powered up
  - When the autoshut counters are cleared on the module

Note If you set the **period** argument to **0**, the module shuts down when it crosses the frequency threshold, regardless of the period of time it took to reach that threshold.

8.6 EFT Copy

When the frequency threshold is reached and occurs within the defined period, the Ethernet module automatically shuts down. The following is an example of the syslog message that displays:

```
%SYS-5-MOD_AUTOSHUT: Module 2 shutdown automatically, reset 4 times in last 5 minutes due
to inband failure
```

When the frequency threshold is reached and occurs outside the defined period, the module does not automatically shut down. The following is an example of the syslog message that displays:

```
%SYS-4-MOD_AUTOSHUT_SLOW:Module 1 reset frequency exceeded threshold but over 46 mins.
Hence NOT powering down module
```

The run-time variable states for Ethernet modules do not synchronize with the standby supervisor engine. The output of the **show autoshut** command on a standby supervisor engine does not track with the number of resets or the reasons for the resets. If the module is powered down by the **set autoshut** command, the output stays the same.

You do not have to enable automatic module shutdown in order to track the number of resets. Resets are tracked even if you do not enable automatic module shutdown.

The runtime counters are cleared only for these conditions:

- When you enter the **clear autoshut** command
- When the switch resets
- At module power up
- At supervisor engine switchover

Examples

This example shows how to set the threshold number of times that the specified module can reset itself:

```
Console> (enable) set autoshut frequency 4
Console> (enable)
```

This example shows how to set the period (in minutes) over which the frequency is valid:

```
Console> (enable) set autoshut period 3
Console> (enable)
```

Related Commands

clear autoshut
set module autoshut
show autoshut

set banner lcd

To configure the Catalyst 6500 series Switch Fabric Module LCD user banner, use the **set banner lcd** command.

set banner lcd *c* [*text*] *c*

Syntax Description

c	Delimiting character used to begin and end the message.
text	(Optional) Message of the day.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The user banner cannot contain more than 801 characters, including delimiting characters and tabs. Tabs display as eight characters but use only one character of memory.

After you configure the user banner, it is sent to all Catalyst 6500 series Switch Fabric Modules in the switch.

The Switch Fabric Module front panel has a 2 line by 20 character LCD display. To see the LCD user banner, push the SELECT button on the front panel and scroll to the USER CONFIGURATION option. Push the NEXT button to see the user banner.

To clear the LCD user banner, use the **set banner lcd** *cc* command.

Examples

This example shows how to set the Catalyst 6500 series Switch Fabric Module LCD user banner:

```
Console> (enable) set banner lcd &HelloWorld!&
LCD banner set
Console> (enable)
```

Related Commands

set banner motd
set banner telnet
show banner

set banner motd

To program an MOTD banner to appear before session login, use the **set banner motd** command.

set banner motd *c* [*text*] *c*

Syntax Description

c	Delimiting character used to begin and end the message.
text	(Optional) Message of the day.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The MOTD banner cannot contain more than 3,070 characters, including tabs. Tabs display as eight characters but take only one character of memory.

You can use either the **clear banner motd** command or the **set banner motd** *cc* command to clear the message-of-the-day banner.

Examples

This example shows how to set the message of the day using the pound sign (#) as the delimiting character:

```
Console> (enable) set banner motd #
** System upgrade at 6:00am Tuesday.
** Please log out before leaving on Monday. #
MOTD banner set.
Console> (enable)
```

This example shows how to clear the message of the day:

```
Console> (enable) set banner motd ##
MOTD banner cleared.
Console> (enable)
```

Related Commands

clear banner motd
set banner lcd
set banner telnet
show banner

set banner telnet

To display or suppress the “Cisco Systems Console” Telnet banner message, use the **set banner telnet** command.

set banner telnet {**enable** | **disable**}

Syntax Description

enable	Displays the Telnet banner.
disable	Suppresses the Telnet banner.

Defaults

The “Cisco Systems Console” Telnet banner message is enabled.

Command Types

Switch.

Command Modes

Privileged.

Examples

This example shows how to display the Telnet banner message:

```
Console> (enable) set banner telnet enable
Cisco Systems Console banner will be printed at telnet.
Console> (enable)
```

This example shows how to suppress the Telnet banner message:

```
Console> (enable) set banner telnet disable
Cisco Systems Console banner will not be printed at telnet.
Console> (enable)
```

Related Commands

set banner lcd
set banner motd
show banner

set boot auto-config

To specify one or more configuration files to use to configure the switch at bootup, use the **set boot auto-config** command. The list of configuration files is stored in the CONFIG_FILE environment variable.

set boot auto-config *device:filename* [**;***device:filename*...] [*mod*]

Syntax Description

*device***:**	Device where the startup configuration file resides.
filename	Name of the startup configuration file.
mod	(Optional) Module number of the supervisor engine containing the Flash device.

Defaults

The default CONFIG_FILE is slot0:switch.cfg.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set boot auto-config** command always overwrites the existing CONFIG_FILE environment variable settings. (You cannot prepend or append a file to the variable contents.)

If you specify multiple configuration files, you must separate the files with a semicolon (;).

To set the recurrence on other supervisor engines and switches, use the **set boot config-register auto-config** command.

Examples

This example shows how to specify a single configuration file environment variable:

```
Console> (enable) set boot auto-config slot0:cfgfile2
CONFIG_FILE variable = slot0:cfgfile2
WARNING: nvram configuration may be lost during next bootup,
         and re-configured using the file(s) specified.
Console> (enable)
```

This example shows how to specify multiple configuration file environment variables:

```
Console> (enable) set boot auto-config slot0:cfgfile;slot0:cfgfile2
CONFIG_FILE variable = slot0:cfgfile1;slot0:cfgfile2
WARNING: nvram configuration may be lost during next bootup,
         and re-configured using the file(s) specified.
Console> (enable)
```

Related Commands

set boot config-register
set boot system flash
show boot

set boot config-register

To configure the boot configuration register value, use the **set boot config-register** command.

set boot config-register 0x*value* [*mod*]

set boot config-register baud {**1200** | **2400** | **4800** | **9600** | **19200** | **38400**} [*mod*]

set boot config-register ignore-config {**enable** | **disable**} [*mod*]

set boot config-register boot {**rommon** | **bootflash** | **system**} [*mod*]

Syntax Description

0x*value*	Sets the 16-bit configuration register value.
mod	(Optional) Module number of the supervisor engine containing the Flash device.
baud 1200 | 2400 | 4800 | 9600 | 19200 | 38400	Specifies the console baud rate.
ignore-config	Sets the ignore-config feature.
enable	Enables the specified feature.
disable	Disables the specified feature.
boot	Specifies the boot image to use on the next restart.
rommon	Specifies booting from the ROM monitor.
bootflash	Specifies booting from the bootflash.
system	Specifies booting from the system.

Defaults

The defaults are as follows:

- Configuration register value is 0x10F, which causes the switch to boot from what is specified by the BOOT environment variable.
- Baud rate is set to 9600.
- **ignore-config** parameter is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

We recommend that you use only the **rommon** and **system** options with the **set boot config-register boot** command.

Each time you enter one of the **set boot config-register** commands, the system displays all current configuration-register information (the equivalent of entering the **show boot** command).

8.6 EFT Copy

The baud rate specified in the configuration register is used by the ROM monitor only and is different from the baud rate specified by the **set system baud** command.

When you enable the **ignore-config** feature, the system software ignores the configuration. Enabling the **ignore-config** parameter is the same as entering the **clear config all** command; that is, it clears the entire configuration stored in NVRAM the next time the switch is restarted.

Examples

This example shows how to specify booting from the ROM monitor:

```
Console> (enable) set boot config-register boot rommon
Configuration register is 0x100
ignore-config: disabled
console baud: 9600
boot: the ROM monitor
Console> (enable)
```

This example shows how to specify the default 16-bit configuration register value:

```
Console> (enable) set boot config-register 0x12f
Configuration register is 0x12f
break: disabled
ignore-config: disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to change the ROM monitor baud rate to 4800:

```
Console> (enable) set boot config-register baud 4800
Configuration register is 0x90f
ignore-config: disabled
console baud: 4800
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to ignore the configuration information stored in NVRAM the next time the switch is restarted:

```
Console> (enable) set boot config-register ignore-config enable
Configuration register is 0x94f
ignore-config: enabled
console baud: 4800
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to specify rommon as the boot image to use on the next restart:

```
Console> (enable) set boot config-register boot rommon
Configuration register is 0x100
ignore-config: disabled
console baud: 9600
boot: the ROM monitor
Console> (enable)
```

Related Commands

copy
set boot auto-config
set boot system flash
set config acl nvram
show boot
show config

set boot config-register auto-config

To configure auto-config file dispensation, use the **set boot config-register auto-config** command.

set boot config-register auto-config {**recurring** | **non-recurring**} [*mod*]

set boot config-register auto-config {**overwrite** | **append**}

set boot config-register auto-config sync {**enable** | **disable**}

Syntax Description

recurring	Sets auto-config to recurring and specify the switch retains the contents of the CONFIG_FILE environment variable after the switch is reset or power cycled and configured.
non-recurring	Sets auto-config to nonrecurring and cause the switch to clear the contents of the CONFIG_FILE environment variable after the switch is reset or power cycled and before the switch is configured.
mod	(Optional) Module number of the supervisor engine containing the Flash device.
overwrite	Causes the auto-config file to overwrite the NVRAM configuration.
append	Causes the auto-config file to append to the file currently in the NVRAM configuration.
sync enable | disable	Enables or disables synchronization of the auto-config file.

Defaults

The defaults are as follows:

- **overwrite**
- **non-recurring**
- **sync is disable**

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **auto-config overwrite** command clears the NVRAM configuration before executing the Flash configuration file. The **auto-config append** command executes the Flash configuration file before clearing the NVRAM configuration.

If you delete the auto-config Flash files on the supervisor engine, the files will also be deleted on the standby supervisor engine.

If you enter the **sync enable** keywords, this enables synchronization to force the configuration files to synchronize automatically to the redundant supervisor engine. The files are kept consistent with what is on the active supervisor engine.

8.6 EFT Copy

If you use the **set boot auto-config bootflash:switch.cfg** with the overwrite option, you must use the **copy config bootflash:switch.cfg** command to save the switch configuration to the auto-config file.

If you use the **set boot auto-config bootflash:switchapp.cfg** with the append option, you can use the **copy acl config bootflash:switchapp.cfg** command to save the switch configuration to the auto-config file.

If the ACL configuration location is set to Flash memory, the following message is displayed after every commit operation for either security or QoS. Use the **copy** command to save your ACL configuration to Flash memory. If you reset the system and you made one or more commits but did not copy commands to one of the files specified in the CONFIG_FILE variable, the following message displays:

```
Warning: System ACL configuration has been modified but not saved to Flash.
```

The files used with the **recurring** and **non-recurring** options are those specified by the CONFIG_FILE environment variable.

Examples

This example shows how to specify the ACL configuration Flash file at system startup:

```
Console> (enable) set boot auto-config bootflash:switchapp.cfg
Console> (enable) set boot config-register auto-config recurring
Console> (enable)
```

This example shows how to ignore the configuration information stored in NVRAM the next time the switch is restarted:

```
Console> (enable) set boot config-register auto-config non-recurring
Configuration register is 0x2102
ignore-config: disabled
auto-config: non-recurring, overwrite, auto-sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to append the auto-config file to the file currently in the NVRAM configuration:

```
Console> (enable) set boot config-register auto-config append
Configuration register is 0x2102
ignore-config: disabled
auto-config: non-recurring, append, auto-sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to use the auto-config overwrite option to save the ACL configuration to a bootflash file:

```
Console> (enable) copy config bootflash: switch.cfg
Console> (enable) set boot auto-config bootflash:switch.cfg
Console> (enable) set boot config-register auto-config overwrite
Console> (enable)
```

Caution The following two examples assume that you have saved the ACL configuration to the bootflash:switchapp.cfg file.

This example shows how to enable synchronization of the auto-config file:

```
Console> (enable) set boot config-register auto-config sync enable
Configuration register is 0x2102
ignore-config: disabled
auto-config: non-recurring, append, auto-sync enabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

This example shows how to disable synchronization of the auto-config file:

```
Console> (enable) set boot config-register auto-config sync disable
Configuration register is 0x2102
ignore-config: disabled
auto-config: non-recurring, append, auto-sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

Related Commands

set boot config-register
set boot system flash
show boot

set boot device

To set the Network Analysis Module (NAM) or Intrusion Detection System (IDS) boot environment, use the **set boot device** command.

set boot device *bootseq*[**,***bootseq*] *mod* [**mem-test-full**]

Syntax Description

bootseq	Device where the startup configuration file resides; see the "Usage Guidelines" section for format guidelines. The second *bootseq* is optional. Separate multiple *bootseq* arguments with a comma.
mod	Number of the module containing the Flash device.
mem-test-full	(Optional) Specifies a full memory test.

Defaults

The default is a partial memory test.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enter the **set boot device** command, the existing boot string in the supervisor engine NVRAM is always overwritten.

When entering the *bootseq*, use the format *bootdevice*[**:***bootdevice-qualifier*] where:

- *bootdevice* is the device where the startup configuration file resides; valid values are **pcmcia**, **hdd**, or **network**.
- *bootdevice-qualifier* is the name of the startup configuration file; valid values for **hdd** are from 1 to 99, and valid values for **pcmcia** are slot0 or slot1.

The colon between *bootdevice* and *bootdevice-qualifier* is required.

You can enter multiple *bootseqs* by separating each entry with a comma; 15 is the maximum number of boot sequences you can enter.

The supervisor engine does not validate the boot device you specify, but stores the boot device list in NVRAM.

This command is supported by the NAM or IDS only.

Examples

This example shows how to specify the boot environment to boot to the maintenance partition of the NAM on module 2:

```
Console> (enable) set boot device hdd:2 2
Device BOOT variable = hdd:2
Warning: Device list is not verified but still set in the boot string.
Console> (enable)
```

This example shows how to specify multiple boot environments on module 5:

```
Console> (enable) set boot device hdd,hdd:5,pcmcia:slot0,network,hdd:6 5
Device BOOT variable = hdd,hdd:5,pcmcia:slot0,network,hdd:6
Warning:Device list is not verified but still set in the boot string.
Console> (enable)
```

Related Commands

clear boot device
show boot device

set boot sync now

To immediately initiate synchronization of the system image between the active and redundant supervisor engine, use the **set boot sync now** command.

set boot sync now

Syntax Description

This command has no arguments or keywords.

Defaults

The default is synchronization is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set boot sync now** command is similar to the **set boot config-register auto-config** command with the **sync** keyword added. The **set boot sync now** command initiates synchronization to force the configuration files to synchronize automatically to the redundant supervisor engine. The files are kept consistent with what is on the active supervisor engine.

Examples

This example shows how to initiate synchronization of the auto-config file:

```
Console> (enable) set boot sync now
Console> (enable)
```

Related Commands

set boot auto-config
show boot

set boot sync timer

To specify an amount of time for the image synchronization timer, use the **set boot sync timer** command.

set boot sync timer *nsec*

Syntax Description

nsec	Timer amount in seconds; valid values are from 10 to 7200 seconds.

Defaults

The default is 120 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set boot sync timer** command is used to specify an image synchronization timer amount. After the specified amount of time has passed, a process begins to synchronize the image on the redundant supervisor engine with the image on the active supervisor engine if the images are not identical.

If you enter the **set boot sync now** command, the timer is bypassed, and the synchronization process begins immediately.

Examples

This example shows how to set the image synchronization timer to 300 seconds:

```
Console> (enable) set boot sync timer 300
Image auto sync timer set to 300 seconds.
Console> (enable)
```

Related Commands

set boot sync now
show boot

set boot system flash

To set the BOOT environment variable that specifies a list of images the switch loads at startup, use the **set boot system flash** command.

set boot system flash *device*:[*filename*] [**prepend**] [*mod*]

Syntax Description

device:	Device where the Flash resides.
filename	(Optional) Name of the configuration file.
prepend	(Optional) Places the device first in the list of boot devices.
mod	(Optional) Module number of the supervisor engine containing the Flash device.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

You can enter several **boot system** commands to provide a problem-free method for booting the switch. The system stores and executes the **boot system** commands in the order in which you enter them. Remember to clear the old entry when building a new image with a different filename in order to use the new image.

If the file does not exist (for example, if you entered the wrong filename), then the filename is appended to the bootstring, and this message displays, “Warning: File not found but still added in the bootstring.” If the file does exist, but is not a supervisor engine image, the file is not added to the bootstring, and this message displays, “Warning: file found but it is not a valid boot image.”

Examples

This example shows how to append the filename cat6000-sup.5-5-1.bin on device bootflash to the BOOT environment variable:

```
Console> (enable) set boot system flash bootflash:cat6000-sup.5-5-1.bin
BOOT variable = bootflash:cat6000-sup.5-4-1.bin,1;bootflash:cat6000-sup.5-5-1.bin,1;
Console> (enable)
```

This example shows how to prepend cat6000-sup.5-5-1.bin to the beginning of the boot string:

```
Console> (enable) set boot system flash bootflash:cat6000-sup.5-5-1.bin prepend
BOOT variable = bootflash:cat6000-sup.5-5-1.bin,1;bootflash:cat6000-sup.5-4-1.bin,1;
Console> (enable)
```

Related Commands

clear boot system
show boot

set cam

To add entries into the CAM table, set the aging time for the CAM table, and configure traffic filtering from and to a specific host, use the **set cam** command.

set cam {**dynamic** | **static** | **permanent**} {*unicast_mac* | *route_descr*} *mod/port* [*vlan*]

set cam {**static** | **permanent**} {*multicast_mac*} *mod/ports..* [*vlan*]

set cam {**static** | **permanent**} **filter** {*unicast_mac*} *vlan*

set cam agingtime *vlan agingtime*

Syntax Description

dynamic	Specifies entries are subject to aging.
static	Specifies entries are not subject to aging.
permanent	Specifies permanent entries are stored in NVRAM until they are removed by the **clear cam** or **clear config** command.
unicast_mac	MAC address of the destination host used for a unicast.
route_descr	Route descriptor of the "next hop" relative to this switch; valid values are from 0 to 0xffff.
mod/port	Number of the module and the port on the module.
vlan	(Optional) Number of the VLAN; valid values are from 1 to 4094.
multicast_mac	MAC address of the destination host used for a multicast.
mod/ports..	Number of the module and the ports on the module.
filter	Specifies a traffic filter entry.
agingtime	Sets the period of time after which an entry is removed from the table.
agingtime	Number of seconds (0 to 1,000,000) dynamic entries remain in the table before being deleted.

Defaults

The default configuration has a local MAC address, spanning tree address (01-80-c2-00-00-00), and CDP multicast address for destination port 1/3 (the supervisor engine). The default aging time for all configured VLANs is 300 seconds.

The *vlan* variable is required when you configure the traffic filter entry.

Setting the aging time to 0 disables aging.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If the given MAC address is a multicast address (the least significant bit of the most significant byte is set to 1) or broadcast address (ff-ff-ff-ff-ff-ff) and you specify multiple ports, the ports must all be in the same VLAN. If the given address is a unicast address and you specify multiple ports, the ports must be in different VLANs.

The MSM does not support the **set cam** command.

If you enter a route descriptor with no VLAN parameter specified, the default is the VLAN already associated with the port. If you enter a route descriptor, you may only use a single port number (of the associated port).

The MAC address and VLAN for a host can be stored in the NVRAM and are maintained even after a reset.

The *vlan* value is optional unless you are setting CAM entries to dynamic, static, or permanent for a trunk port, or if you are using the **agingtime** keyword.

If a port or ports are trunk ports, you must specify the VLAN.

Static (nonpermanent) entries remain in the table until you reset the active supervisor engine.

You can specify 256 permanent CAM entries.

Enter the *route_descr* variable as two hexadecimal bytes in the following format: 004F. Do not use a "-" to separate the bytes.

Note Static CAM entries that are configured on the active supervisor engine are lost after fast switchover. You must reconfigure CAM entries after fast switchover.

Examples

This example shows how to set the CAM table aging time to 300 seconds:

```
Console> (enable) set cam agingtime 1 300
Vlan 1 CAM aging time set to 300 seconds.
Console> (enable)
```

This example shows how to add a unicast entry to the table for module 2, port 9:

```
Console> (enable) set cam static 00-00-0c-a0-03-fa 2/9
Static unicast entry added to CAM table.
Console> (enable)
```

This example shows how to add a permanent multicast entry to the table for module 1, port 1, and module 2, ports 1, 3, and 8 through 12:

```
Console> (enable) set cam permanent 01-40-0b-a0-03-fa 1/1,2/1,2/3,2/8-12
Permanent multicast entry added to CAM table.
Console> (enable)
```

This example shows how to add a traffic filter entry to the table:

```
Console> (enable) set cam static filter 00-02-03-04-05-06 1
Filter entry added to CAM table.
Console> (enable)
```

Related Commands

clear cam
show cam

set cam monitor

To monitor the MAC addresses that are learned and stored in the CAM table, to specify the polling interval for the CAM table, or to specify the upper and lower limits for the learning of MAC addresses, use the **set cam monitor** command.

set cam monitor {**enable** | **disable**} [*mod/port* | *vlan*]

set cam monitor interval *time_s*

set cam monitor high-threshold *value* [**action** {**no-learn** | **shutdown** | **warning**}] {*mod/port* | *vlan*}

set cam monitor low-threshold *value* [**action** {**no-learn** | **warning**}] {*mod/port* | *vlan*}

Syntax Description

enable	Enables CAM monitoring.
disable	Disables CAM monitoring.
mod/port	(Optional) Number of the module and the ports on the module.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
interval *time_s*	Specifies the polling interval in seconds for monitoring the CAM table; valid values are from 5 to 3600 seconds.
high-threshold *value*	Specifies the upper limit for MAC address learning; valid values are from 5 to 32000.
action	(Optional) Specifies the action to be taken when the system exceeds the threshold limits.
no-learn	(Optional) Specifies that the system stop learning MAC addresses when the low threshold is exceeded.
shutdown	(Optional) Specifies that the system shut down the port or suspend the VLAN if the low threshold is exceeded.
warning	(Optional) Specifies that the system display a system message when the low threshold is exceeded.
mod/port	Number of the module and the ports on the module.
vlan	VLAN number; valid values are from 1 to 4094.
low-threshold *value*	Specifies the lower limit for MAC address learning; valid values are from 5 to 32000.

Defaults

CAM monitoring is enabled globally.

The polling interval is 5 seconds.

When only an interface is enabled, the low threshold is 500, and the high threshold is 32000. The violation action is a system message at the warning level (level 4).

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **no-learn** violation action prevents MAC address learning on an interface, but it does not delete any extra MAC addresses on the interface.

Examples

This example shows how to monitor the MAC addresses that are learned on a specific port and entered into the CAM table:

```
Console> (enable) set cam monitor enable 3/1
Successfully enabled cam monitor on 3/1
Console> (enable)
```

This example shows how to disable monitoring of the MAC addresses that are learned on a specific port:

```
Console> (enable) set cam monitor disable 3/1
Successfully disabled cam monitor on 3/1
Console> (enable)
```

This example shows how to specify the polling interval for the CAM table:

```
Console> (enable) set cam monitor interval 20
Cam monitor interval set to 20 sec
Console> (enable)
```

This example shows how to specify the low threshold for a port and the action to be taken when this threshold is exceeded:

```
Console> (enable) set cam monitor low-threshold 500 action warning 3/1
Successfully configured cam monitor on 3/1
Console> (enable)
```

This example shows how to specify the high threshold for a port and the action to be taken when this threshold is exceeded:

```
Console> (enable) set cam monitor high-threshold 28000 action shutdown 3/1
Successfully configured cam monitor on 3/1
Console> (enable)
```

Related Commands

clear cam monitor
show cam monitor

8.6 EFT Copy

set cam notification

To set CAM notification parameters, use the **set cam notification** command.

set cam notification {**enable** | **disable**}

set cam notification {**added** | **removed**} {**enable** | **disable**} {*mod/port*}

set cam notification historysize *log_size*

set cam notification interval *time*

set cam notification move {**enable** | **disable**}

set cam notification threshold {**enable** | **disable**}

set cam notification threshold limit *percentage*

set cam notification theshold interval *time*

set cam notification move counters {**enable** | **disable**}

Syntax Description

enable	Enables notification that a change has occurred.
disable	Disables notification that a change has occurred.
added	Specifies notification when a MAC address is learned.
removed	Specifies notification when a MAC address is deleted.
mod/port	Number of the module and the port.
historysize	Creates a notification history log.
log_size	Number of entries in the notification history log; valid sizes are between 0 and 500 entries.
interval	Sets the maximum wait time between notifications.
time	Time between notification; valid values are greater than or equal to 0 (specified in seconds).
move	Specifies MAC move notifications.
threshold	Sets parameters for CAM usage monitoring
limit	Sets CAM usage monitoring percentage.
percentage	Percentage of usage monitoring.
move counters	Sets the MAC move counters (MMC).
enable	Enables the MAC move counter.
disable	Disables the MAC move counter.

Defaults

By default, notification is disabled.

By default, the interval time is set to 1 second.

By default, the history size is set to 1 entry.

By default, the MAC move counter is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can globally disable notifications using the **set cam notification disable** command, but the other notification configuration settings will remain configured. The notification configuration settings can be reset using the **clear config** command. The **clear cam notification** command can be used to clear the history log or reset notification counters.

If you set the interval time to 0, the switch will send notifications immediately. There is an impact on the performance of the switch when you set the interval time to zero (0).

You can configure the switch to generate MAC notification SNMP traps using the **set snmp enable macnotification** command. MAC notification SNMP traps are generated even when the history log size is set to zero (0).

The severity level of the EARL facility must be set at or higher 4. If the severity level of the EARL facility is less than 4, the following message is displayed:

```
Please change the logging level for the Earl facility, as the current logging level is set
to 2 and Mac Move Counters requires a logging level of at least 4.
```

Use the **set logging level earl** command to change the severity level.

A MAC move counter is a counter that increments every time an existing MAC address moves from a given port to another port in the same VLAN.

In PVLANs, a MAC move counter is a counter that increments every time an existing MAC moves from a given port to another port in different secondary VLANs, but in the same PVLAN.

MAC move counter records a maximum of 1000 MAC moves per VLAN only. Once this maximum has been exceeded, no new moves are recorded on the VLAN. You can enter the **clear cam notification move counters** command to clear the counters.

Due to CPU versus ASIC processing speed differences, the number of moves reported by the MAC move counter may differ from the actual number of MAC moves.

MAC move counter notification is not supported on EARL 4 and earlier.

Examples

This example shows how to enable notification when a MAC address change occurs to the CAM table:

```
Console> (enable) set cam notification enable
MAC address change detection globally enabled
Be sure to specify which ports are to detect MAC address changes
with the 'set cam notification [added|removed] enable <m/p> command.
SNMP traps will be sent if 'set snmp trap enable macnotification' has been set.
Console> (enable)
```

This example shows how to enable notification when a new MAC address is added to ports 1-4 on module 3 in the CAM table:

```
Console> (enable) set cam notification added enable 3/1-4
MAC address change notifications for added addresses are
enabled on port(s) 3/1-4
Console> (enable)
```

This example shows how to enable notification when a new MAC address is added to the CAM table on ports 1-4 on module 2:

```
Console> (enable) set cam notification added enable 2/1-4
MAC address change notifications for added addresses are
enabled on port(s) 2/1-4
Console> (enable)
```

This example shows how to enable notification when a MAC address is deleted from the CAM table of ports 3-6 on module 3:

```
Console> (enable) set cam notification removed enable 3/3-6
MAC address change notifications for removed addresses are
enabled on port(s) 3/3-6
```

This example shows how to set the history log size to 300 entries:

```
Console> (enable) set cam notification historysize 300
MAC address change history log size set to 300 entries
Console> (enable)
```

This example shows how to set the interval time to 10 seconds between notifications:

```
Console> (enable) set cam notification interval 10
MAC address change notification interval set to 10 seconds
Console> (enable)
```

This example shows how to enable MAC move notification:

```
Console> (enable) set cam notification move counters enable
MAC move counters are enabled
Console> (enable)
```

Related Commands

clear cam
clear cam notification
set cam
set snmp trap
show cam
show cam notification

set cdp

To enable, disable, or configure Cisco Discovery Protocol (CDP) features globally on all ports or on specified ports, use the **set cdp** command.

set cdp {**enable** | **disable**} {*mod/ports...*}

set cdp interval *interval*

set cdp holdtime *holdtime*

set cdp version v1 | **v2**

set cdp format device-id {**mac-address** | **other**}

Syntax Description

enable	Enables the CDP feature.
disable	Disables the CDP feature.
mod/ports..	Number of the module and the ports on the module.
interval	Specifies the CDP message interval value.
interval	Number of seconds the system waits before sending a message; valid values are from 5 to 900 seconds.
holdtime	Specifies the global Time-To-Live (TTL) value.
holdtime	Number of seconds for the global TTL value; valid values are from 10 to 255 seconds.
version v1 | **v2**	Specifies the CDP version number.
format device-id	Sets the format of the device ID type-length value (TLV).
mac-address	Specifies that the device ID TLV carry the MAC address of the sending device in ASCII, in canonical format.
other	Specifies that the device's hardware serial number concatenated with the device name between parenthesis.

Defaults

The default system configuration has CDP enabled. The message interval is set to 60 seconds for every port; the default TTL value has the message interval globally set to 180 seconds. The default CDP version is version 2.

Command Types

Switch command.

Command Modes

Privileged.

8.6 EFT Copy

Usage Guidelines

The **set cdp version** command allows you to globally set the highest version number of CDP packets to send.

If you enter the global **set cdp enable** or **disable** command, CDP is globally configured. If CDP is globally disabled, CDP is automatically disabled on all interfaces, but the per-port **enable** (or **disable**) configuration is not changed. If you globally enable CDP, whether CDP is running on an interface or not depends on its per-port configuration.

If you configure CDP on a per-port basis, you can enter the *mod/ports...* value as a single module and port or a range of ports; for example, 2/1-12,3/5-12.

Examples

This example shows how to enable the CDP message display for port 1 on module 2:

```
Console> (enable) set cdp enable 2/1
CDP enabled on port 2/1.
Console> (enable)
```

This example shows how to disable the CDP message display for port 1 on module 2:

```
Console> (enable) set cdp disable 2/1
CDP disabled on port 2/1.
Console> (enable)
```

This example shows how to specify the CDP message interval value:

```
Console> (enable) set cdp interval 400
CDP interval set to 400 seconds.
Console> (enable)
```

This example shows how to specify the global TTL value:

```
Console> (enable) set cdp holdtime 200
CDP holdtime set to 200 seconds.
Console> (enable)
```

This example shows how to set the device ID format to MAC address:

```
Console> (enable) set cdp format device-id mac-address
Device Id format changed to MAC-address
Console> (enable)
```

Related Commands

show cdp
show port cdp

set channelprotocol

To set the protocol that manages channeling on a module, use the **set channelprotocol** command.

set channelprotocol {**pagp** | **lacp**} *mod*

Syntax Description

pagp	Specifies PAgP.
lacp	Specifies LACP.
mod	Number of the module.

Defaults

The default for the channel protocol is PAgP.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

LACP is supported on all Ethernet interfaces.

PAgP and LACP manage channels differently. When all the ports in a channel get disabled, PAgP removes them from its internal channels list; **show** commands do not display the channel. With LACP, when all the ports in a channel get disabled, LACP does not remove the channel; **show** commands continue to display the channel even though all its ports are down. To determine if a channel is actively sending and receiving traffic with LACP, use the **show port** command to see if the link is up or down.

LACP does not support half-duplex links. If a port is in active/passive mode and becomes half duplex, the port is suspended (and a syslog message is generated). The port is shown as “connected” using the **show port** command and as “not connected” using the **show spantree** command. This discrepancy is because the port is physically connected but never joined spanning tree. To get the port to join spanning tree, either set the duplex to full or set the channel mode to off for that port.

For more information about PAgP and LACP, refer to the “Configuring EtherChannel” chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example shows how to set PAgP for module 3:

```
Console> (enable) set channelprotocol pagp 3
Channeling protocol set to PAGP for module(s) 3.
Console> (enable)
```

This example shows how to set LACP for modules 2, 4, 5, and 6:

```
Console> (enable) set channelprotocol lacp 2,4-6
Channeling protocol set to LACP for module(s) 2,4,5,6.
Console> (enable)
```

Related Commands

clear lacp-channel statistics
set lacp-channel system-priority
set port lacp-channel
set spantree channelcost
set spantree channelvlancost
show channelprotocol
show lacp-channel

set channel vlancost

To set the channel VLAN cost, use the **set channel vlancost** command.

set channel vlancost *channel_id cost*

Syntax Description

channel_id	Number of the channel identification; valid values are from 769 to 896.
cost	Port costs of the ports in the channel.

Defaults

The default is the VLAN cost is updated automatically based on the current port VLAN costs of the channeling ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you do not enter the *cost*, the cost is updated based on the current port VLAN costs of the channeling ports.

You can configure only one channel at a time.

Note The **set channel vlancost** command creates a "set spantree portvlancost" entry for each port in the channel. You must then manually reenter the **set spantree portvlancost** command for at least one port in the channel, specifying the VLAN or VLANs that you want associated with the port. When you associate the desired VLAN or VLANs with one port, all ports in the channel are automatically updated. Refer to Chapter 6, "Configuring EtherChannel," in the *Catalyst 6500 Series Switch Software Configuration Guide* for more information.

Note With software releases 6.2(1) and earlier, the 6- and 9-slot Catalyst 6500 series switches support a maximum of 128 EtherChannels.

With software releases 6.2(2) and later, due to the port ID handling by the spanning tree feature, the maximum supported number of EtherChannels is 126 for a 6- or 9-slot chassis and 63 for a 13-slot chassis. Note that the 13-slot chassis was first supported in software release 6.2(2).

Examples

This example shows how to set the channel 769 path cost to 10:

```
Console> (enable) set channel vlancost 769 10
Port(s) 1/1-2 vlan cost are updated to 24.
Channel 769 vlancost is set to 10.
Console> (enable)
```

After you enter this command, you must reenter the **set spantree portvlancost** command so that the desired VLAN or VLANs are associated with all the channel ports.

This example shows how to associate the channel 769 path cost to 10 for VLAN 1 through VLAN 1005:

```
Console> (enable) set spantree portvlancost 1/1 cost 24 1-1005
Port 1/1 VLANs 1025-4094 have path cost 19.
Port 1/1 VLANs 1-1005 have path cost 24.
Port 1/2 VLANs 1-1005 have path cost 24.
Console> (enable)
```

Related Commands

set spantree portvlancost
show channel

set config acl nvram

To copy the current committed ACL configuration from DRAM back into NVRAM, use the **set config acl nvram** command.

set config acl nvram

Syntax Description

This command has no arguments or keywords.

Defaults

The default is NVRAM.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command fails if there is not enough space in NVRAM.

This command copies the current committed configuration to NVRAM; this configuration might be different from the configuration in the auto-config file. After the ACL configuration is copied into NVRAM, you must turn off the auto-config options using the **clear boot auto-config** command.

Examples

This example shows how to copy the ACL configuration to NVRAM:

```
Console> (enable) set config acl nvram
ACL configuration copied to NVRAM.
Console> (enable)
```

Related Commands

clear config
copy
set boot config-register
set boot system flash
show boot

set config checkpoint

To create a checkpoint configuration file, use the **set config checkpoint** command.

set config checkpoint [**name** *name*] [**device** *device*]

Syntax Description

name *name*	(Optional) Names the checkpoint configuration file.
device *device*	(Optional) Specifies device on which the checkpoint configuration file is saved.

Defaults

The default name that the switch automatically generates is in the format CKPi_MMDDYYHHMM, where "i" represents a checkpoint number.

The file is stored on the currently specified default device.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A configuration checkpoint file is identified by a name that you specify when you create the file. The configuration checkpoint filename can be no more than 15 characters. If you do not specify a name, the system generates one. The system-generated name is in the format CKPi_MMDDYYHHMM, where "i" represents a checkpoint number.

The checkpoint file is stored either on the bootflash or on slotX/diskX. If you do not specify a device, the file is stored on the current default device.

The configuration checkpoint file is stored as a text file that can be read and edited. We strongly advise that you do not edit the file.

You can create a maximum of five configuration checkpoint files on a system.

The checkpoint configuration is stored in the NVRAM. The configuration is not cleared when you enter the **clear config all** command. To clear all checkpoint configuration files or a particular configuration checkpoint file, use the **clear config checkpoint** command.

This feature is supported on systems with redundant supervisor engines. The checkpoint configuration and its associated files are synchronized to the redundant supervisor engine.

Use the **set config rollback** command to roll back the current switch configuration file to a configuration checkpoint file.

Examples

This example shows how to create a system-generated configuration checkpoint file:

```
Console> (enable) set config checkpoint
Configuration checkpoint CKP0_0722040712 creation successful.
Console> (enable)
```

This example shows how to specify a name and device for a configuration checkpoint file:

```
Console> (enable) set config checkpoint name SARAH_07122002 device bootflash:
Configuration checkpoint SARAH_07122002 creation successful.
Console> (enable)
```

Related Commands

clear config checkpoint
set config rollback
show config checkpoints

set config mode

To change the configuration mode from a binary model to a text model or to automatically save the system configuration in text mode in NVRAM, use the **set config mode** command.

set config mode binary

set config mode text {**nvram** | *device:file-id*}

set config mode text auto-save {**enable** | **disable**}

set config mode text auto-save interval *mins*

Syntax Description

binary	Sets the system configuration mode to a binary model.
text	Sets the system configuration mode to a text model.
nvram	Specifies the saved configuration be stored in NVRAM.
device:file-id	Name of the device and filename where the saved configuration will be stored.
auto-save	Specifies saving the text configuration in NVRAM automatically.
enable	Enables saving the text configuration in NVRAM automatically.
disable	Disables saving the text configuration in NVRAM automatically.
interval	Sets the time interval between occurrences of saving the text configuration in NVRAM; see the "Usage Guidelines" section for more information.
mins	(Optional) Number of minutes between occurrences of saving the text configuration in NVRAM; valid values are from 1 minute to 35000 minutes (approximately 25 days).

Defaults

The default setting of this command is binary. The configuration is saved in NVRAM.

The number of minutes between occurrences of saving the text configuration in NVRAM is 30 minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can specify the time interval between occurrences of saving the text configuration in NVRAM even if the system is in binary mode. If you do not specify the number of minutes after entering the **interval** keyword, the interval is set to the default of 30 minutes.

The text configuration is not saved automatically in NVRAM unless the auto-save feature is enabled. To enable the auto-save feature, you must first set the system configuration mode to text and configure the system to save the text configuration in NVRAM. If the system configuration mode is set to a binary model, you cannot enable the auto-save feature.

Examples

This example shows how to set the configuration mode to binary:

```
Console> (enable) set config mode binary
System configuration copied to NVRAM. Configuration mode set to binary.
Console> (enable)
```

This example shows how to set the configuration mode to text and designate the location and filename for saving the text configuration file:

```
Console> (enable) set config mode text bootflash:switch.cfg
Binary system configuration has been deleted from NVRAM. Configuration mode set to text.
Use the write memory command to save configuration changes. System configuration file set
to: bootflash:switch.cfg
The file specified will be used for configuration during the next bootup.
Console> (enable)
```

This example shows how to enable the auto-save feature when the configuration is set to text mode and the system is configured to save the text configuration in NVRAM:

```
Console> (enable) set config mode text auto-save enable
auto-save feature has been enabled
auto-save feature has started
Please do a write mem manually if you plan to reboot the switch or any card before first
expiry of the timer
Console> (enable)
```

This example shows the message that is displayed if you attempt to enable the auto-save feature when the configuration is not set to text mode and the system is not configured to save the text configuration in NVRAM:

```
Console> (enable) set config mode text auto-save enable
auto-save cannot be enabled unless config mode is set to text and config file is stored in
nvram.
Use the 'set config mode text nvram' command to enable automatic saving of the system
configuration to nvram
Console> (enable)
```

This example shows how to set the interval between saves to 2880 minutes:

```
Console> (enable) set config mode text auto-save interval 2880
auto-save interval set to 2880 minutes
Console> (enable)
```

This example shows how to set the interval between saves to the default setting of 30 minutes:

```
Console> (enable) set config mode text auto-save interval
auto-save interval set to 30 minutes
Console> (enable)
```

Related Commands

show config mode
write

8.6 EFT Copy

set config rollback

To roll the current configuration file back to a checkpoint configuration file, use the **set config rollback** command.

set config rollback *name*

Syntax Description

name	Configuration checkpoint filename.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can roll back the current switch configuration file to a previously saved configuration file in the event that the current file produces undesirable system results. You can roll back to any of the saved configuration checkpoint files in any order. Because they are generated using a complete configuration, they are independent of each other.

Use the **set config checkpoint** command to create configuration checkpoint files. Use the **show config checkpoints** command to display configuration checkpoint filenames.

Related Commands

clear config checkpoint
set config checkpoint
show config checkpoints

8.6 EFT Copy

set cops

To configure COPS functionality, use the **set cops** command.

set cops server *ipaddress* [*port*] [**primary**] [**diff-serv** | **rsvp**]

set cops domain-name *domain_name*

set cops retry-interval *initial incr max*

Syntax Description

server	Sets the name of the COPS server.
ipaddress	IP address or IP alias of the server.
port	(Optional) Number of the TCP port the switch connects to on the server.
primary	(Optional) Specifies the primary server.
diff-serv	(Optional) Sets the COPS server for differentiated services.
rsvp	(Optional) Sets the COPS server for RSVP+.
domain-name *domain_name*	Specifies the domain name of the switch.
retry-interval	Specifies the retry interval in seconds.
initial	Initial timeout value; valid values are from 0 to 65535 seconds.
incr	Incremental value; valid values are from 0 to 65535 seconds.
max	Maximum timeout value; valid values are from 0 to 65535 seconds.

Defaults

The defaults are as follows:

- The retry interval default values are initial = 30 seconds, incr = 30 seconds, max = 5 minutes.
- The default domain-name is a string of length zero.
- No policy decision point (PDP) servers are configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure the names or addresses of up to two PDP servers. One must be the primary, and the optional second server is a secondary, or backup, PDP server.

The COPS domain name can be set globally only; there is no option to set it for each COPS client.

Names such as the server, domain-name, and roles can contain a maximum of 31 characters; longer names are truncated to 31 characters. Valid letters are a-z, A-Z, 0-9, ., - and _. Names cannot start with an underscore (_). The names are not case sensitive for matching, but are case sensitive for display.

When specifying the **retry-interval**, the total of the initial timeout value and the incremental value (increment on each subsequent failure) may not exceed the maximum timeout value.

Examples

This example shows how to configure a server as a primary server:

```
Console> (enable) set cops server 171.21.34.56 primary
171.21.34.56 added to COPS server table as primary server.
Console> (enable)
```

This example shows how to configure a server as a primary RSVP+ server:

```
Console> (enable) set cops server 171.21.34.56 primary rsvp
171.21.34.56 added to COPS server table as primary server for RSVP.
Console> (enable)
```

This example shows how to configure a server as a secondary (or backup) server:

```
Console> (enable) set cops server my_server2
my_server2 added to the COPS server table as backup server.
Console> (enable)
```

This example shows how to set the domain name:

```
Console> (enable) set cops domain-name my_domain
Domain name set to my_domain.
Console> (enable)
```

This example shows how to set the retry interval:

```
Console> (enable) set cops retry-interval 15 1 30
Connection retry intervals set.
Console> (enable)
```

This example shows the display output if the total of the initial timeout value and the incremental value you entered exceeds the maximum timeout value:

```
Console> (enable) set cops retry-interval 15 1 10
The initial timeout plus the increment value may not exceed the max value.
Console> (enable)
```

Related Commands

clear cops
show cops

set crypto key rsa

To generate and configure an RSA key pair, use the **set crypto key rsa** command.

set crypto key rsa *nbits* [**force**]

Syntax Description

nbits	Size of the key; valid values are 512 to 2048 bits.
force	(Optional) Regenerates the keys and suppress the warning prompt of overwriting existing keys.

Defaults

The command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **crypto** commands are supported on systems that run these image types only:

- supk9 image—for example, cat6000-supk9.6-1-3.bin
- supcvk9 image—for example, cat6000-supcvk9.6-1-3.bin

If you do not enter the **force** keyword, the **set crypto key** command is saved into the configuration file and you will have to use the **clear config all** command to clear the RSA keys.

The *nbits* value is required.

To support SSH login, you first must generate an RSA key pair.

Examples

This example shows how to create an RSA key:

```
Console> (enable) set crypto key rsa 1024
Generating RSA keys.... [OK]
Console> (enable)
```

Related Commands

clear crypto key rsa
show crypto key

set default portstatus

To set the default port status, use the **set default portstatus** command.

set default portstatus {**enable** | **disable**}

Syntax Description

enable	Activates default port status.
disable	Deactivates default port status.

Defaults

The default is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enter the **clear config all** command, or if a configuration loss occurs, all ports collapse into VLAN 1. This situation might cause a security and network instability problem. During a configuration loss, when you enter the **set default portstatus** command, all ports are put into a disable state, and the traffic flowing through the ports is blocked. You can then manually configure the ports back to the enable state.

This command is not saved in the configuration file.

After you set the default port status, the default port status does not clear when you enter the **clear config all** command.

Examples

This example shows how to disable the default port status:

```
Console> (enable) set default portstatus disable
 port status set to disable.
Console> (enable)
```

Related Commands

show default

set dhcp-snooping

To enable DHCP snooping information-option host tracking or the MAC address matching feature, use the **set dhcp-snooping** command.

set dhcp-snooping information-option host-tracking {**enable** | **disable**}

set dhcp-snooping match-mac {**enable** | **disable**}

set dhcp-snooping bindings-database auto-save *interval*

set dhcp-snooping bindings-database *device*:[*filename*]

Syntax Description

information-option	Specifies the DHCP information option feature.
host-tracking	Specifies host tracking.
enable	Enables the DHCP snooping feature.
disable	Disables the DHCP snooping feature.
match-mac	Specifies the DHCP snooping MAC address matching feature.
bindings-database	Configures storage of the DHCP snooping bindings database.
auto-save	Specifies the bindings database automatic save interval.
interval	Time interval in minutes; valid values are from 0 to 35000.
device:[*filename*]	Flash device where the bindings are saved and optionally, the file name that contains the bindings.

Defaults

Host tracking is disabled.

MAC address matching is enabled.

The *interval* is 0, which means that the **auto-save** feature is disabled.

The flash device is bootflash and the default filename is “dhcp-snooping-bindings-database.”

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set dhcp-snooping information-option host-tracking** {**enable** | **disable**} command enables or disables host tracking. Enabling host tracking causes the DHCP snooping process to insert the relay information agent option (option 82) with remote ID and circuit ID suboptions in all client-to-server DHCP packets on VLANs for which DHCP snooping is enabled. Enabling host tracking also activates the processing of option 82 in received server-to-client packets.

The **set dhcp-snooping match-mac** {**enable** | **disable**} command enables or disables the MAC address matching feature. When this option is enabled, the source MAC address in the Ethernet header is matched with the “chaddr” field in the DHCP payload for DHCP packets that come from untrusted ports. If the MAC address and “chaddr” field do not match, packets are dropped, and the counter for dropped packets on untrusted ports is incremented.

If DHCP snooping is disabled on a VLAN, the bindings for that VLAN are deleted.

The DHCP-snooping binding entries can be stored to a flash device so that the bindings can be restored immediately after the switch is reset.

To configure the auto-save interval for DHCP-snooping bindings, use the **auto-save** *interval* option. Valid ranges for the interval are 1 through 35000 minutes. Specifying a 0 disables the periodic saving of bindings on the flash device and deletes the bindings file stored in flash. Specifying a 0 does not clear a user-specified filename. The user-specified filename is cleared and returned to the default filename after you enter the **clear config all** command.

To specify the flash device and filename for storing the bindings, use the *device:filename* option. By default, the flash device is bootflash and the default filename is “dhcp-snooping-bindings-database.” If you have not configured a filename, the bindings are automatically saved with the default filename on the flash device.

Examples

This example shows how to enable DHCP snooping information-option host tracking:

```
Console> (enable) set dhcp-snooping information-option host-tracking enable
DHCP Snooping Information Option Enabled.
Console> (enable)
```

This command shows how to disable DHCP snooping MAC address matching:

```
Console> (enable) set dhcp-snooping match-mac disable
DHCP Snooping MAC address matching disabled.
Console> (enable)
```

This example shows how to enable the **auto-save** option for DHCP-snooping binding entries and specify an interval of 600 minutes for the periodic saving of the bindings:

```
Console> (enable) set dhcp-snooping bindings-database auto-save 600
DHCP Snooping auto-save interval set to 600 minutes.
Console> (enable)
```

This example shows how to specify the flash device and filename for storing the bindings:

```
Console> (enable) set dhcp-snooping bindings-database disk1:dhcp-bindings
DHCP Snooping bindings storage file set to disk1:dhcp-bindings.
Console> (enable)
```

Related Commands

show dhcp-snooping config

set diagnostic bootup level

To specify the bootup generic online diagnostics level, use the **set diagnostic bootup level**.

set diagnostic bootup level {**bypass** | **complete** | **minimal**}

Syntax Description

bypass	Skips all online diagnostic tests.
complete	Runs all online diagnostic tests.
minimal	Runs only PFC tests for the supervisor engine and loopback tests fro all ports.

Defaults

The bootup level is **minimal**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Although the default bootup level for generic online diagnostics is **minimal**, we recommend that you set the level to **complete**. We strongly recommend that you do not bypass diagnostics.

The bootup diagnostics level applies to the entire switch. The bootup diagnostics level cannot be configured on a per-module basis.

Note GOLD is supported on the Supervisor Engine 720 and the Supervisor Engine 32 only. Earlier diagnostic commands are still supported on the Supervisor Engine 1 and the Supervisor Engine 2.

Examples

This example shows how to specify **complete** as the bootup diagnostics level:

```
Console> (enable) set diagnostic bootup level complete
Diagnostic level set to complete
Console> (enable)
```

Related Commands

clear diagnostic
diagnostic start
diagnostic stop
set diagnostic diagfail-action
set diagnostic event-log size
set diagnostic monitor
set diagnostic ondemand
set diagnostic schedule
show diagnostic

set diagnostic diagfail-action

To specify the generic online diagnostics failure response for the system, use the **set diagnostic diagfail-action** command.

set diagnostic diagfail-action {**ignore** | **system**}

Syntax Description

ignore	Specifies that test failures are ignored and the system still boots up.
system	Specifies that the test failures trigger error recovery.

Defaults

The **system** keyword is the default.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Note GOLD is supported on the Supervisor Engine 720 and the Supervisor Engine 32 only. Earlier diagnostic commands are still supported on the Supervisor Engine 1 and the Supervisor Engine 2.

Examples

This example shows how to configure the system to ignore test failures and still boot up:

```
Console> (enable) set diagnostic diagfail-action ignore
Diagnostic failure action set to ignore.
Console> (enable)
```

This example shows how to trigger an error recovery in the event of test failures:

```
Console> (enable) set diagnostic diagfail-action system
Diagnostic failure action set to system.
Console> (enable)
```

Related Commands

clear diagnostic
diagnostic start
diagnostic stop
set diagnostic bootup level
set diagnostic event-log size
set diagnostic monitor
set diagnostic ondemand
set diagnostic schedule
show diagnostic

set diagnostic event-log size

To specify the size of event log for generic online diagnostics, use the **set diagnostic event-log size** command.

set diagnostic event-log size *number_of_entries*

Syntax Description

number_of_entries	Number of online diagnostics events in the event log; valid values are 1 to 10000.

Defaults

500 entries.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Note GOLD is supported on the Supervisor Engine 720 and the Supervisor Engine 32 only. Earlier diagnostic commands are still supported on the Supervisor Engine 1 and the Supervisor Engine 2.

Examples

This example shows how to specify 1000 entries for the online diagnostics event log size:

```
Console> (enable) set diagnostic event-log size 1000
Diagnostic event-log size set to 1000
Console> (enable)
```

Related Commands

clear diagnostic
diagnostic start
diagnostic stop
set diagnostic bootup level
set diagnostic diagfail-action
set diagnostic monitor
set diagnostic ondemand
set diagnostic schedule
show diagnostic

set diagnostic monitor

To configure generic online diagnostic health monitoring, use the **set diagnostic monitor** command.

set diagnostic monitor interval module *mod_num* **test** {**all** | *test_ID_num* | *test_list*} *hh:mm:ss*

set diagnostic monitor module *mod_num* **test** {**all** | *test_ID_num* | *test_list*}

set diagnostic monitor syslog

Syntax Description

interval module	Configures online diagnostic monitoring test intervals.
mod_num	Number of the module.
test	Specifies particular online diagnostic tests.
all	Specifies all online diagnostic tests.
test_ID_num	Number of a specific online diagnostic test.
test_list	List of online diagnostic tests.
hh:mm:ss	Time in 24-hour format.
module	Enables health-monitoring diagnostic tests.
syslog	Enables syslog generation when a test fails.

Defaults

Disruptive tests are disabled by default. Some non-disruptive tests are enabled by default. Use the **show diagnostic content module** command to determine which tests are disruptive (D) and non-disruptive (N) by looking the "Attributes" column of the command output. We recommend that only the non-disruptive tests be used for health monitoring.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure health-monitoring diagnostic testing on specified modules while the switch is connected to a live network. You can specify the execution interval for each health-monitoring test, whether or not to generate a system message upon test failure, or whether an individual test should be enabled or disabled.

Note GOLD is supported on the Supervisor Engine 720 and the Supervisor Engine 32 only. Earlier diagnostic commands are still supported on the Supervisor Engine 1 and the Supervisor Engine 2.

Examples

This example shows how to specify that the online diagnostic health-monitoring tests (test 18) be run on module 7 at 12:12:12 and 100 milliseconds every 10 days:

```
Console> (enable) set diagnostic monitor interval module 7 test 18 12:12:12 100 10
Diagnostic monitor interval set at 12:12:12 100 10 for module 7 test 18
Console> (enable)
```

This example shows how to enable test 18 on module 7:

```
Console> (enable) set diagnostic monitor module 7 test 18
Module 7 test 18 diagnostic monitor enable.
Console> (enable)
```

This example shows how to enable syslog generation when a test fails:

```
Console> (enable) set diagnostic monitor syslog
Diagnostic monitor syslog enable.
Console> (enable)
```

Usage Guidelines

clear diagnostic
diagnostic start
diagnostic stop
set diagnostic bootup level
set diagnostic diagfail-action
set diagnostic event-log size
set diagnostic ondemand
set diagnostic schedule
show diagnostic

set diagnostic ondemand

To configure on-demand generic online diagnostics, use the **set diagnostic ondemand** command.

set diagnostic ondemand action-on-failure {**continue** *failure_limit* | **stop**}

set diagnostic ondemand iterations *number_of_iterations*

Syntax Description

action-on-failure	Sets action that the switch should take in the event of online diagnostic test failures.
continue *failure_limit*	Continues on-demand tests until the test failure limit is reached; valid values are from 0 to 65534 failures.
stop	Specifies that online diagnostic tests stop when a single failure occurs.
interations	Specifies the number of times to repeat online diagnostic tests.
number_of_iterations	Number of times to repeat online diagnostic tests; valid values are from 1 to 999.

Defaults

The *failure_limit* argument is 0.

The *number_of_iterations* argument is 1.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

For a complete list of on-demand generic online diagnostic tests for supervisor engines, fabric-enabled modules, and non-fabric-enabled modules, see the "Configuring GOLD" chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Note GOLD is supported on the Supervisor Engine 720 and the Supervisor Engine 32 only. Earlier diagnostic commands are still supported on the Supervisor Engine 1 and the Supervisor Engine 2.

Examples

This example shows how to specify that the online diagnostics stop running after experiencing 100 failures:

```
Console> (enable) set diagnostic ondemand action-on-failure continue 100
Diagnostic ondemand action-on-failure set to continue 100
Console> (enable)
```

This example shows how to specify that the online diagnostics run 50 times:

```
Console> (enable) set diagnostic ondemand iterations 50
Diagnostic ondemand iterations set to 50
Console> (enable)
```

8.6 EFT Copy

Related Commands

clear diagnostic
diagnostic start
diagnostic stop
set diagnostic bootup level
set diagnostic diagfail-action
set diagnostic event-log size
set diagnostic monitor
set diagnostic schedule
show diagnostic

set diagnostic schedule

To schedule generic online diagnostics, use the **set diagnostic schedule** command.

set diagnotic schedule module *mod_num* **test** {**all** | *test_ID_num* | *test_list*} {**port** {*port_num* | *port_range* | **all**} | **daily** *hh:mm* | **on month** *days_of_month range_of_years hh:mm* | **weekly day** *hh:mm*}

Syntax Description

module *mod_num*	Specifies the module for which to schedule online diagnostics.
test	Specifies particular online diagnostic tests.
all	Species all online diagnostic tests.
test_ID_num	Number of a specific online diagnostic test.
test_list	List of online diagnostic tests.
port	Specifies the port on which the online diagnostic tests are run.
port_num	Number of the port.
port_range	Range of ports.
all	Specifies all ports on the module.
daily	Specifies a daily schedule
hh:mm	Hour and minute.
on	Specifies an absolute schedule.
month	Specifies the month.
days_of_month	Days of the month; valid values are from 1 to 31.
range_of_years	Range of years; valid values are from 1993-2035.
weekly	Specifies a weekly schedule.
day	Specifies a day of the week.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can schedule online diagnostics to run at a designated time of day or on a daily, weekly, or monthly basis for a specific module. You can specify that all tests be run or that individual tests be run. The tests can be scheduled to run only once or be repeated at specified intervals.

Note GOLD is supported on the Supervisor Engine 720 and the Supervisor Engine 32 only. Earlier diagnostic commands are still supported on the Supervisor Engine 1 and the Supervisor Engine 2.

Examples

This example shows how to schedule diagnostic testing (tests 1 and 2 specified) to occur on a specific date and time for a specific module:

```
Console> (enable) set diagnostic schedule module 7 test 1 daily 12:12
Diagnostic schedule set at daily 12:12 for module 7 test 1
Console> (enable)
```

This example shows how to schedule diagnostic testing (test 1 specified) to occur daily at a certain time for a specific port and module:

```
Console> (enable) set diagnostic schedule module 7 test 3 port 1 daily 16:16
Diagnostic schedule set at daily 16:16 for module 7 test 3
Console> (enable)
```

Related Commands

clear diagnostic
diagnostic start
diagnostic stop
set diagnostic bootup level
set diagnostic diagfail-action
set diagnostic event-log size
set diagnostic monitor
set diagnostic ondemand
show diagnostic

set dot1q-all-tagged

To change all existing and new dot1q trunks to the dot1q-only mode, use the **set dot1q-all-tagged** command.

set dot1q-all-tagged {**enable** | **disable**}

Syntax Description

enable	Enables dot1q-tagged-only mode.
disable	Disables dot1q-tagged-only mode.

Defaults

The 802.1Q tagging feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enable dot1q-tagged-only, all data packets are sent out tagged and all received untagged data packets are dropped on all 802.1Q trunks.

You cannot enable the dot1q tunneling feature on a port until dot1q-tagged-only mode is enabled.

You cannot disable dot1q-tagged-only mode on the switch until dot1q tunneling is disabled on all the ports on the switch.

The optional **all** keyword is not supported.

Note Policy-based forwarding (PBF) does not work with 802.1Q tunnel traffic. PBF is supported on Layer 3 IP unicast traffic, but it is not applicable to Layer 2 traffic. At the intermediate (PBF) switch, all 802.1Q tunnel traffic appears as Layer 2 traffic.

If you enable dot1q-tagged globally, the dot1q-tagged per-port setting controls whether or not frames are tagged. If you disable dot-1q-tagged globally, the default group is never tagged and the per-port setting has no effect.

Examples

This example shows how to enable dot1q tagging:

```
Console> (enable) set dot1q-all-tagged enable
Dot1q tagging is enabled
Console> (enable)
```

Related Commands

set port dot1qtunnel
show dot1q-all-tagged

8.6 EFT Copy

set dot1x

To configure 802.1X on a system, use the **set dot1x** command.

set dot1x system-auth-control {**enable** | **disable**}

set dot1x {**quiet-period** | **tx-period** | **re-authperiod**} *seconds*

set dot1x {**supp-timeout** | **server-timeout**} *seconds*

set dot1x max-req *count*

set dot1x shutdown-timeout *seconds*

set dot1x vlan-group *vlan_group_name vlan*

set dot1x radius-accounting {**enable** | **disable**}

set dot1x radius-vlan-assignment {**enable** | **disable**}

set dot1x radius-keepalive {**enable** | **disable**}

Syntax Description

system-auth-control	Specifies authentication for the system.
enable	Enables the specified 802.1X function.
disable	Disables the specified 802.1X function.
quiet-period *seconds*	Specifies the idle time between authentication attempts; valid values are from 0 to 65535 seconds.
tx-period *seconds*	Specifies the time for the retransmission of EAP-Request/Identity frame; valid values are from 0 to 65535 seconds. See the "Usage Guidelines" section for additional information.
re-authperiod *seconds*	Specifies the time constant for the retransmission reauthentication time; valid values are from 1 to 65535 seconds.
supp-timeout *seconds*	Specifies the time constant for the retransmission of EAP-Request packets; valid values are from 0 to 65535 seconds. See the "Usage Guidelines" section for additional information.
server-timeout *seconds*	Specifies the time constant for the retransmission of packets by the backend authenticator to the authentication server; valid values are from 1 to 65535 seconds. See the "Usage Guidelines" section for additional information.
max-req *count*	Specifies the maximum number of times that the state machine retransmits an EAP-Request frame to the supplicant before it times out the authentication session; valid values are from 1 to 10.
shutdown-timeout *seconds*	Specifies the amount time that a port is shut down after a security violation; valid values are from 1 to 65535 seconds. See the "Usage Guidelines" section for additional information.
vlan-group	Specifies the VLAN group name.
vlan_group_name	Name of the VLAN group.
vlan	VLAN number; valid values are from 1 to 4094.
radius-accounting	Specifies 802.1X RADIUS accounting and tracking.

radius-vlan-assignment	Specifies 802.1X RADIUS VLAN assignment.
radius-keepalive	Specifies 802.1X RADIUS keepalive state.

Defaults

The default settings are as follows:

- **system-auth-control** is enabled.
- **quiet-period** is 60 seconds.
- **tx-period** is 30 seconds.
- **re-authperiod** is 3600 seconds.
- **supp-timeout** is 30 seconds.
- **server-timeout** is 30 seconds.
- **max-req** count is 2.
- **shutdown-timeout** is 300 seconds.
- **radius-accounting** is disabled.
- **radius-vlan-assignment** is disabled.
- **radius-keepalive** is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you set the **system-auth-control**, the following applies:

- The **enable** keyword allows you to control each port's authorization status per the port-control parameter set using the **set port dot1x** command.
- The **disable** keyword allows you to make all ports behave as though the port-control parameter is set to **force-authorized**.

If you do not enable reauthentication, reauthentication does not automatically occur after authentication has occurred.

Private VLANs and 802.1X configurations are mutually exclusive of one another.

When the supplicant does not notify the authenticator that it received the EAP-request/identity packet, the authenticator waits a period of time (set by entering the **tx-period** *seconds* parameter), and then retransmits the packet.

When the supplicant does not notify the backend authenticator that it received the EAP-request packet, the backend authenticator waits a period of time (set by entering the **supp-timeout** *seconds* parameter), and then retransmits the packet.

When the authentication server does not notify the backend authenticator that it received specific packets, the backend authenticator waits a period of time (set by entering the **server-timeout** *seconds* parameter), and then retransmits the packets.

When you enter the **set dot1x dhcp-relay-agent** command, you can enter more than one VLAN.

To activate the shutdown-timeout timer on a port, enter the **set port dot1x** *mod/port* **shutdown-timeout** command.

To configure the 802.1X user distribution feature, follow these guidelines:

- Ensure that at least one VLAN is mapped to the VLAN group.
- You can map more than one VLAN to a VLAN group.
- The VLAN group can be modified by adding or deleting a VLAN.
- When an existing VLAN is cleared from the VLAN group name, none of the ports authenticated in the VLAN are cleared, but the mappings are removed from the existing VLAN group.
- If you clear the last VLAN from the VLAN group name, the VLAN group is deleted.
- You can clear a VLAN group, even when active VLANs are mapped to the group. When a VLAN group is cleared, none of the ports or users that are in the authenticated state in any VLAN within the group are cleared, but the VLAN mappings to the VLAN group are cleared.
- If you enter the **set dot1x radius-vlan-assignment disable** command, the VLAN information that is sent from the RADIUS server is ignored, and the port stays in the NVRAM-configured VLAN. This command is used to enable or disable the VLAN assignment feature globally. When the command is enabled, the switch uses the tunnel attributes to extract the VLAN name in the RADIUS Access-Accept message. The command is enabled by default.

To check whether or not configured RADIUS servers are alive, the switch can send out a dummy username for authentication. In reply to the dummy username, the RADIUS servers send an access rejection. To turn off authentication attempts that test the RADIUS servers, enter the **set dot1x radius-keepalive disable** command. If you disable this feature, the switch does not check the status of the servers, and the RADIUS server logs do not fill with dummy attempts.

Note In software releases 7.5 through 8.2, the command to enable or disable the RADIUS keepalive feature is **set feature dot1x-radius-keepalive**. In software release 8.3 and later releases, the command is **set dot1x radius-keepalive**.

Examples

This example shows how to set the system authentication control:

```
Console> (enable) set dot1x system-auth-control enable
dot1x authorization enabled.
Console> (enable)
```

This example shows how to set the idle time between authentication attempts:

```
Console> (enable) set dot1x quiet-period 45
dot1x quiet-period set to 45 seconds.
Console> (enable)
```

This example shows how to set the retransmission time:

```
Console> (enable) set dot1x tx-period 15
dot1x tx-period set to 15 seconds.
Console> (enable)
```

This example shows you how to specify the reauthentication time:

```
Console> (enable) set dot1x re-authperiod 7200
dot1x re-authperiod set to 7200 seconds
Console> (enable)
```

This example shows you how to specify the retransmission of EAP-Request packets by the authenticator to the supplicant:

```
Console> (enable) set dot1x supp-timeout 15
dot1x supp-timeout set to 15 seconds.
Console> (enable)
```

This example shows how to specify the retransmission of packets by the backend authenticator to the authentication server:

```
Console> (enable) set dot1x server-timeout 15
dot1x server-timeout set to 15 seconds.
Console> (enable)
```

This example shows how to specify the maximum number of packet retransmissions:

```
Console> (enable) set dot1x max-req 5
dot1x max-req set to 5.
Console> (enable)
```

This example shows how to enable authentication for the DHCP Relay Agent on VLANs 1 through 5 and 24:

```
Console> (enable) set dot1x dhcp-relay-agent enable 1-5,24
dot1x dhcp-relay-agent enabled for vlans 1-5, 24.
Console> (enable)
```

This example shows how to disable authentication for the DHCP Relay Agent on VLAN 1:

```
Console> (enable) set dot1x dhcp-relay-agent disable 1
dotx dhcp-relay-agent disable for vlan 1
Console> (enable)
```

This example shows how to create a new VLAN group in the system:

```
Console> (enable) set dot1x vlan-group engg-dept 3
Vlan group engg-dept is successfully configured and mapped to vlan 3.
Console> (enable)
```

This example shows how to map another VLAN to an existing VLAN group name:

```
Console> (enable) set dot1x vlan-group engg-dept 4
Vlan 4 is successfully mapped to vlan group engg-group.
Console> (enable)
```

This example shows how to globally enable RADIUS accounting and tracking:

```
Console> (enable) set dot1x radius-accounting enable
dot1x radius-accounting enabled.
Console> (enable)
```

This example shows how to globally enable the RADIUS VLAN assignment feature:

```
Console> (enable) set dot1x radius-vlan-assignment enable
dot1x radius-vlan-assignment enabled.
Console> (enable)
```

This example shows how to globally enable the RADIUS keepalive state feature:

```
Console> (enable) set dot1x radius-keepalive enable
dot1x radius-keepalive state enabled.
Console> (enable)
```

Related Commands	
	clear dot1x config clear dot1x vlan-group set port dot1x set radius deadtime show dot1x show port dot1x

set enablepass

To change the password for the privileged level of the CLI, use the **set enablepass** command.

set enablepass

Syntax Description

This command has no arguments or keywords.

Defaults

The default configuration has no enable password configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Passwords are case sensitive and may be 0 to 19 characters in length, including spaces.

The command prompts you for the old password. If the password you enter is valid, you are prompted to enter a new password and to verify the new password.

Examples

This example shows how to establish a new password:

```
Console> (enable) set enablepass
Enter old password: <old_password>
Enter new password: <new_password>
Retype new password: <new_password>
Password changed.
Console> (enable)
```

Related Commands

enable
set password

8.6 EFT Copy

set eou

To globally enable or disable Extensible Authentication Protocol over User Datagram Protocol (EoU), use the **set eou** command.

set eou {enable | disable}

Syntax Description

enable	Enables EoU globally.
disable	Disables EoU globally.

Defaults

Global EoU is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

For configuration guidelines and restrictions, see the "Configuring Network Access Control" chapter of the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to enable LAN port IP (LPIP) on the switch:

```
Console> (enable) set eou enable
EoU LPIP Enabled globally
Console> (enable)
```

Related Commands

clear eou
set eou allow clientless
set eou authorize
set eou initialize
set eou logging
set eou max-retry
set eou radius-accounting
set eou rate-limit
set eou revalidate
set eou timeout
set port eou
set security acl ip
show eou
show port eou

set eou allow clientless

To enable or disable bypassing of the LAN port IP (LPIP) posture validation for a clientless host, use the **set eou allow clientless** command.

set eou allow clientless {enable | disable}

Syntax Description

enable	Allows clientless hosts.
disable	Does not allow clientless hosts.

Command Default

The clientless mechanism is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

For configuration guidelines and restrictions, see the “Configuring Network Access Control” chapter of the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to enable bypassing of the LPIP posture validation for a clientless host:

```
Console> (enable) set eou allow clientless enable
EoU Clientless hosts will be allowed
Console> (enable)
```

Related Commands

clear eou
set eou
set eou authorize
set eou initialize
set eou logging
set eou max-retry
set eou radius-accounting
set eou rate-limit
set eou revalidate
set eou timeout
set port eou
set security acl ip
show eou
show port eou

set eou authorize

To statically authorize a device by IP address or by MAC address and to apply an associated policy to the device, use the **set eou authorize** command.

set eou authorize ip *ip_addr* [*ip_mask*] **policy** *policy_name*

set eou authorize mac-address *mac_addr* [*mac_mask*] **policy** *policy_name*

Syntax Description

ip *ip_addr*	Sets an IP address-based exception list.
ip_mask	(Optional) IP mask.
policy *policy_name*	Specifies a policy name.
mac-address *mac_addr*	Sets a MAC address-based exception list.
mac_mask	(Optional) MAC address mask.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set eou authorize** command allows a device with specific IP address or MAC address to be treated as an exception host. When that host is detected, it dynamically installs the specified policy.

If the policy template does not exist, when you enter this command, the policy template is created.

For other configuration guidelines and restrictions, see the “Configuring Network Access Control” chapter of the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to statically authorize a device with a specific IP address and to apply an associated policy to the device:

```
Console> (enable) set eou authorize ip 172.20.52.19 255.255.255.224 policy poll
Mapped IP address 172.20.52.0 IP mask 255.255.255.224 to policy name poll
Console> (enable)
```

This example shows how to statically authorize a device using the device MAC address and apply an associated policy to the device:

```
Console> (enable) set eou authorize mac-address 03-56-B7-45-65-56 policy poll
Mapped MAC 03-56-b7-45-65-56 to policy name poll.
Console> (enable)
```

Related Commands

clear eou
set eou
set eou allow clientless
set eou initialize
set eou logging
set eou max-retry
set eou radius-accounting
set eou rate-limit
set eou revalidate
set eou timeout
set port eou
set security acl ip
show eou
show port eou

set eou initialize

To restart the state machine for a host, use the **set eou initialize** command.

set eou initialize {**all** | **ip** *ip_addr* | **mac** *mac_addr* | **posture-token** *posture_token*}

set eou initialize authentication {**clientless** | **eap** | **static**}

Syntax Description

all	Initializes all EoU interfaces.
ip *ip_addr*	Initializes port with the specified IP address.
mac *mac_addr*	Initializes port with the specified MAC address.
posture-token *posture_token*	Initializes all EoU ports with the specified posture token.
authentication	Initializes all EoU ports of a specific authentication type.
clientless	Initializes all clientless ports.
eap	Initializes all ports with EAP authentication.
static	Initializes all hosts in an exception list.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

For configuration guidelines and restrictions, see the "Configuring Network Access Control" chapter of the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to restart a host's state machine using the IP address:

```
Console> (enable) set eou initialize ip 172.20.52.19
Initializing Eou for ipAddress 172.20.52.19
Console> (enable)
```

Related Commands

clear eou
set eou
set eou allow clientless
set eou authorize
set eou logging
set eou max-retry
set eou radius-accounting
set eou rate-limit
set eou revalidate
set eou timeout
set port eou
set security acl ip
show eou
show port eou

set eou logging

To enable or disable EoU logging for LAN port IP events, use the **set eou logging** command.

set eou logging {**enable** | **disable**}

Syntax Description

enable	Enables logging.
disable	Disables logging.

Defaults

Logging is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable logging:

```
Console> (enable) set eou logging enable
Logging enabled for LPIP events.
Console> (enable)
```

Related Commands

clear eou
set eou
set eou allow clientless
set eou authorize
set eou initialize
set eou max-retry
set eou radius-accounting
set eou rate-limit
set eou revalidate
set eou timeout
set port eou
set security acl ip
show eou
show port eou

set eou max-retry

To specify the number of times a packet is retransmitted to the Cisco Trust Agent (CTA) before declaring the CTA nonresponsive, use the **set eou max-retry** command.

set eou max-retry *max_retries*

Syntax Description

max_retries	Maximum number of reattempts; valid values are from 1 to 10.

Defaults

Packets are retransmitted 3 times.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

For configuration guidelines and restrictions, see the "Configuring Network Access Control" chapter of the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to set the number of times that a packet is retransmitted to the CTA before declaring the CTA nonresponsive:

```
Console> (enable) set eou max-retry 6
eou max-retry set to 6.
Console> (enable)
```

Related Commands

clear eou
set eou
set eou allow clientless
set eou authorize
set eou initialize
set eou logging
set eou radius-accounting
set eou rate-limit
set eou revalidate
set eou timeout
set port eou
set security acl ip
show eou
show port eou

set eou radius-accounting

To globally enable or disable EoU RADIUS accounting, use the **set eou radius-accounting** command.

set eou radius-accounting {**enable** | **disable**}

Syntax Description

enable	Enables EoU RADIUS accounting.
disable	Disables EoU RADIUS accounting.

Defaults

EoU RADIUS accounting is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable EOU RADIUS accounting:

```
Console> (enable) set eou radius-accounting enable
Radius Accounting for Eou Enabled.
Console> (enable)
```

Related Commands

clear eou
set eou
set eou allow clientless
set eou authorize
set eou initialize
set eou logging
set eou max-retry
set eou rate-limit
set eou revalidate
set eou timeout
set port eou
set security acl ip
show eou
show port eou

set eou rate-limit

To set the maximum number of simultaneous EoU sessions that are allowed on the switch, use the **set eou rate-limit** command.

set eou rate-limit *rate*

Syntax Description

rate	Number of simultaneous sessions; valid values are 0 and from 10 to 200.

Defaults

The number of simultaneous sessions is 0.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the number of simultaneous EoU sessions to 100:

```
Console> (enable) set eou rate-limit 100
eou ratelimit set to 100.
Console> (enable)
```

Related Commands

clear eou
set eou
set eou allow clientless
set eou authorize
set eou initialize
set eou logging
set eou max-retry
set eou radius-accounting
set eou revalidate
set eou timeout
set port eou
set security acl ip
show eou
show port eou

8.6 EFT Copy

set eou revalidate

To revalidate a host, use the **set eou revalidate** command.

set eou revalidate {**all** | **ip** *ip_addr* | **mac** *mac_addr* | **posture-token** *posture_token*}

set eou revalidate authentication {**clientless** | **eap** | **static**}

Syntax Description

all	Revalidates all EoU ports.
ip *ip_addr*	Revalidates a port with the specified IP address.
mac *mac_addr*	Revalidates a port with the specified MAC address.
posture-token *posture_token*	Revalidates all ports with the specified posture token.
authentication	Revalidates all ports of a specific authentication type.
clientless	Revalidates all clientless ports.
eap	Revalidates all ports with EAP authentication.
static	Revalidates all hosts in an exception list.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to revalidate all hosts:

```
Console> (enable) set eou revalidate all
EoU LPIP revalidation started for all hosts
Console> (enable)
```

This example shows how to revalidate all clientless hosts:

```
Console> (enable) set eou revalidate authentication clientless
Revalidate all clientless hosts
Console> (enable)
```

Related Commands

clear eou
set eou
set eou allow clientless
set eou authorize
set eou initialize
set eou logging
set eou max-retry
set eou radius-accounting
set eou rate-limit
set eou timeout
set port eou
set security acl ip
show eou
show port eou

8.6 EFT Copy

set eou timeout

To set EoU-related timers, use the **set eou timeout** command.

set eou timeout {**aaa** | **hold-period** | **retransmit** | **revalidation** | **status-query**} *seconds*

Syntax Description

aaa	Sets EoU AAA timeout.
hold-period	Sets EoU hold timeout.
retransmit	Sets EoU retransmit timeout.
revalidation	Sets EoU revalidation timeout.
status-query	Sets EoU status-query timeout.
seconds	Timeout in seconds; see the “Usage Guidelines” section for valid values.

Defaults

The following are the EoU timer defaults:

- **aaa**—60 seconds.
- **hold-period**—180 seconds.
- **retransmit**—30 seconds.
- **revalidation**—3600 seconds.
- **status-query**—300 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The following are ranges for EoU timeout periods:

- The **aaa** value is from 1 to 60 seconds.
- The **hold-period** value is from 60 to 86400 seconds.
- The **retransmit** value is from 1 to 60 seconds.
- The **revalidation** value is from 5 to 86400 seconds.
- The **status-query** value is from 30 to 1800 seconds.

Examples

This example shows how to set the status-query timeout to 30 seconds:

```
Console> (enable) set eou timeout status-query 30
LPIP Status Query timeout set to 30 seconds.
Console> (enable)
```

Related Commands

clear eou
set eou
set eou allow clientless
set eou authorize
set eou initialize
set eou logging
set eou max-retry
set eou radius-accounting
set eou rate-limit
set eou revalidate
set port eou
set security acl ip
show eou
show port eou

set errdisable-timeout

To configure a timeout to automatically reenable ports that are in the errdisable state, use the **set errdisable-timeout** command.

set errdisable-timeout {**enable** | **disable**} {*reason*}

set errdisable-timeout interval {*interval*}

Syntax Description

enable	Enables errdisable timeout.
disable	Disables errdisable timeout.
reason	Reason for the port being in errdisable state; valid values are **arp-inspection, bcast-suppression**, **bpdu-guard**, **channel-misconfig**, **cross-fallback, duplex-mismatch**, **gl2pt-ingress-loop**, **gl2pt-threshold-exceed**, **gl2pt-cdp-threshold-exceed**, **gl2pt-stp-threshold-exceed**, **gl2pt-vtp-threshold-exceed**, **link-rxcrc**, **link-txcrc**, **udld**, **other**, **all**.
interval *interval*	Specifies the timeout interval; valid values are from 30 to 86400 seconds (30 seconds to 24 hours).

Defaults

By default, all the errdisable state reasons are disabled globally; whenever there are no reasons enabled, the timer is stopped.

By default, the timeout is set to **disable**, and the *interval* value is set at 300 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A port enters errdisable state for the following reasons (these reasons appear as configuration options within the **set errdisable-timeout enable** command):

- **rp-inspection**—ARP inspection
- **bcast-suppression** —Broadcast suppression
- **bpdu-guard**—BPDU port-guard
- **cam-monitor**—CAM monitoring
- **channel-misconfig**—Channel misconfiguration
- **crossbar-fallback**—Crossbar failure
- **duplex-mismatch**—Duplex mismatch
- **gl2pt-ingress-loop**—Layer 2 protocol tunnel misconfiguration
- **gl2pt-threshold-exceed**—When Layer 2 protocol tunnel threshold is exceeded
- **gl2pt-cdp-threshold-exceed**—When Layer 2 protocol tunnel CDP threshold is exceeded

- **gl2pt-stp-threshold-exceed**—When Layer 2 protocol tunnel STP threshold is exceeded
- **gl2pt-vtp-threshold-exceed**—When Layer 2 protocol tunnel VTP threshold is exceeded
- **link-rxcrc**—When link-errors RX threshold is exceeded
- **link-txcrc**—When link-errors TX threshold is exceeded
- **udld**—UDLD
- **other**—Reasons other than the above
- **all**—Applies errdisable timeout for all of the above reasons

You can enable or disable errdisable timeout for each of the reasons that are listed. If you specify "other," all ports errdisabled by causes other than the reasons listed are enabled for errdisable timeout. If you specify "all," all ports errdisabled for any reason are enabled for errdisable timeout.

You can manually prevent a port from being reenabled by setting the errdisable timeout for that port to disable using the **set port errdisable-timeout** *mod/port* **disable** command.

Examples

This example shows how to enable an errdisable timeout due to a BPDU port-guard event:

```
Console> (enable) set errdisable-timeout enable bpdu-guard
Successfully enabled errdisable-timeout for bpdu-guard.
Console> (enable)
```

This example shows how to set an errdisable timeout interval to 450 seconds:

```
Console> (enable) set errdisable-timeout interval 450
Successfully set errdisable timeout to 450 seconds.
Console> (enable)
```

This example shows how to set an errdisable timeout for broadcast suppression events:

```
Console> (enable) set errdisable-timeout enable bcast-suppression
Successfully enabled errdisable timeout for bcast-suppression.
Console> (enable)
```

This example shows how to set an errdisable timeout for ARP inspection events:

```
Console> (enable) set errdisable-timeout enable arp-inspection
Successfully enabled errdisable-timeout for arp-inspection.
Console> (enable)
```

Related Commands

set port errdisable-timeout
show errdisable-timeout

8.6 EFT Copy

set errordetection

To enable or disable various error detections, use the **set errordetection** command.

set errordetection inband {**enable** | **disable**}

set errordetection memory {**enable** | **disable**}

set errordetection portcounters {**enable** | **disable**}

set errordetection packet-buffer {**errdisable** | **powercycle** |
supervisor {**errdisable** | **shutdown**}}

set errordetection link-errors {**enable** | **disable**}

set errordetection link-errors action {**errordisable** | **port-failover**}

set errordetection link-errors interval *value*

set errordetection link-errors threshold {**inerrors** | **rxcrc** | **txcrc**} [**high** *value*] [**low** *value*]

set errordetection link-errors sampling *value*

Syntax Description

inband	Detects errors in the inband (sc0) interface.
enable	Enables the specified error detection.
disable	Disables the specified error detection.
memory	Detects memory corruption.
portcounters	Monitors and polls port counters.
packet-buffer	Specifies how to handle packet-buffer errors.
errdisable	Errdisables ports with packet-buffer errors.
powercycle	Power cycles modules with packet-buffer errors.
supervisor	Specifies handling packer-buffer errors on the supervisor engine.
errdisable	Errdisables supervisor engine ports with packet-buffer errors.
shutdown	Shuts down supervisor engine ports with packet-buffer errors.
link-errors	Detects link errors.
action	Specifies how link errors are handled.
errordisable	Errdisables the port when the high threshold is reached.
port-failover	Errdisables the port if the port is in a channel but is not the last operational port in the channel. The port also goes into errdisable state if it is a single port.
interval *value*	Specifies a timer constraint for reading the error counters on ports; valid values are 30 to 1800 seconds.
threshold	Specifies the threshold for link errors.
inerrors	Specifies the inerrors threshold.
rxcrc	Specifies the RXCRC (CRCAlignErrors) error counter threshold.
txcrc	Specifies the TXCRC error counter threshold.
high *value*	(Optional) Sets the high threshold value; valid values are 2 to 65535 packets.

low *value*	(Optional) Sets the low threshold value; valid values are 1 to 65534 packets.
sampling *value*	Specifies the number of consecutive times that a port must reach the high or low threshold value before the port is placed in the errdisable state; valid values are 1 to 255 times.

Defaults

The following are the default settings for **set errordetection**:

- Inband error detection is enabled.
- Memory error detection is enabled.
- Portcounters error detection is enabled.
- Packet-buffer error detection is **errdisable**.
- Packet-buffer error detection for the supervisor engine is **shutdown**.
- Link-error error detection is **port-failover**.
- The link-error interval is 30 seconds.
- The high value for the inerrors threshold is 1001 packets.
- The low value for the inerrors threshold is 1000 packets.
- The high value for the rxcrc threshold is 1001 packets.
- The low value for the rxcrc threshold is 1000 packets.
- The high value for the txcrc threshold is 1001 packets.
- The low value for the rxcrc threshold is 1000 packets.
- The link-error sampling is 3 times.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set errordetection** command is useful for monitoring the switch. If an error is detected, a syslog message informs you that a problem exists before noticeable performance degradation occurs. For example, entering these commands displays the following information:

- **set errordetection inband**—Displays the type of inband failure occurrence, such as inband stuck, resource errors, and inband fail when you start the switch.
- **set errordetection memory**—Displays the address where the memory corruption occurred.
- **set errordetection portcounters**—Displays the module and port number and the counter that had the problem between two consecutive polls.

The rapid boot feature minimizes the amount of downtime a module experiences if the module encounters a packet-buffer error. You can enter one of the following commands to handle the error condition:

- **set errordetection packet-buffer errdisable**—If you enter the **errdisable** keyword, only ports that experience the packet-buffer error are put in errdisable state.
- **set errordetection packet-buffer powercycle**—If you enter the **powercycle** keyword, the module is power cycled. When you choose this option, a ROMMON image is downloaded on the module, and the normal bootup sequence is bypassed to reduce module downtime.
- **supervisor**—If you enter the **supervisor errdisable** keywords, the supervisor engine ports that experience the packet-buffer errors are put in the errdisable state. If you enter the **supervisor shutdown** keywords, the supervisor engine ports that experience the packet-buffer errors are shut down.

Caution Do not power cycle the module when the ROMMON image is downloading. Doing so might damage the module.

The rapid boot feature is available on the following modules:

- WS-X6248-RJ45
- WS-X6248-TELCO
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6148-RJ45
- WS-X6148-RJ21

The **set errordetection link-errors** global commands allow you to configure link error handling. When entering the **set errordetection link-errors** commands, follow these guidelines:

- **set errordetection link-errors action** {**errordisable** | **port-failover**}

  If the error count for a port reaches the high value for the configurable threshold (within the sampling count period specified), the **action** is either **errordisable** or **port-failover**. If you select **errordisable**, the port goes into the errdisable state when the high threshold is reached. If you select **port-failover**, the channel status of the port is considered. The port goes into the errdisable state if the port is in a channel and is not the last operational port in the channel. The port also goes into errdisable state if it is a single port.

- **set errordetection link-errors interval** *value*

  The **interval** *value* that you specify determines how often the error counter for a port is read.

- **set errordetection link-errors threshold** {**inerrors** | **rxcrc** | **txcrc**} [**high** *value*] [**low** *value*]

  The threshold values that you specify determine how many link errors are allowed during the interval that you specify by entering the **set errordetection interval** *value* command. If the low threshold is reached (within the sampling count period specified), a syslog message is displayed. If the high threshold is reached (within the sampling count period specified), in addition to displaying a syslog message, the port is either errdisabled or the port failover mechanism takes effect.

  When you enter the **inerrors** keyword, the ifInErrors counter is checked. For packet-oriented interfaces, the ifInErrors counter includes the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the ifInErrors counter includes the number of inbound transmission units that contained errors that prevented them from being delivered to a higher-layer protocol.

After the **inerrors** keyword, **rx-threshold** keyword, or the **tx-threshold** keyword, enter one of the following options:

– The **low** keyword and a value

– The **high** keyword and a value

– Both keywords and a value for each

- **set errordetection link-errors sampling** *value*

  To minimize the possibility of accidentally putting a port into the errdisable state because of a one-time event that is not a true system error condition, you can specify a sampling value. This value determines the number of times a port must reach the high or low threshold value before the port is placed in the errdisable state. For example, if the high threshold value for a port is 1000 and the sampling count is 3, the port is errdisabled only after it has reached the 1000 threshold 3 consecutive times.

Examples

This example shows how to enable memory error detection:

```
Console> (enable) set errordetection memory enable
Memory error detection enabled.
Console> (enable)
```

This example shows how to enable power cycling for a module that encounters packet-buffer errors:

```
Console> (enable) set errordetection packet-buffer powercycle
Warning: Boot ROM upgrade is required on module(s) 8 for rapid boot.
This will require a reset of the module(s). Do you want to continue (y/n) [n]? y
2004 May 11 16:24:01 EST +00:00 %SYS-6-CFG_CHG:Global block changed by Console//
Failed to download boot code on module 8.
Packet buffer error detection set to powercycle.
Console (enable)
```

This example shows how to put ports that encounter packet-buffer errors into errdisable state:

```
Console (enable) set errordetection packet-buffer errdisable
Packet buffer error detection set to errdisable.
Console (enable)
```

This example shows how to specify how link errors are handled:

```
Console> (enable) set errordetection link-errors action errordisable
Console> (enable)
```

This example shows how to set the timer constraint for reading error counters on ports to 60 seconds:

```
Console> (enable) set errordetection link-errors interval 60
Console> (enable)
```

This example shows how to set the rx-threshold for ports to 2000 packets:

```
Console> (enable) set errordetection link-errors rx-threshold high 2000
Console> (enable)
```

This example shows how to set the link-error sampling value to 10 times:

```
Console> (enable) set errordetection link-errors sampling 10
Console> (enable)
```

Related Commands

set errdisable-timeout
set port errordetection
show errdisable-timeout
show errordetection
show port errordetection

set ethernet-cfm

To enable or disable Connectivity Fault Management (CFM) globally on a switch, use the **set ethernet-cfm** command.

set ethernet-cfm {**disable** | **enable**}

Syntax Description

disable	Disables CFM globally on a switch.
enable	Enables CFM globally on a switch.

Defaults

CFM is disabled.

Command Types

Switch command.‘

Command Modes

Privileged.

Usage Guidelines

This command stores the **enable** or **disable** setting in NVRAM.

Examples

This example shows how to enable CFM globally on a switch:

```
Console> (enable) set ethernet-cfm enable
Ethernet CFM enabled.
Console> (enable)
```

Related Commands

set ethernet-cfm continuity-check

To initiate or terminate the transmission of continuity-check messages for a specific level, use the **set ethernet-cfm continuity-check** command.

set ethernet-cfm continuity-check {**disable** | **enable**} **level** *level* [**vlan** *vlans*]

Syntax Description

disable	Disables continuity check.
enable	Enables continuity check.
level *level*	Maintenance level of the local MEPs; valid values are from 0 to 7.
vlan *vlans*	(Optional) Specifies the VLAN or range of VLANs on which to do the check; valid values are from 1 to 4094.

Defaults

Continuity check messages are disabled for all levels.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a VLAN, this command initializes or terminates continuity-check messages for all VLANs at the maintenance level that you specify.

Examples

This example shows how to initialize the transmission of continuity-check messages for level 7 and applies to all VLANs in that level:

```
Console> (enable) set ethernet-cfm continuity-check enable level 7
Continuity Check for ME level 7  is enabled.
Console> (enable)
```

This example shows how to initialize the transmission of continuity-check messages for level 4 and applies to the VLAN range of 10-199:

```
Console> (enable) set ethernet-cfm continuity-check enable level 4 vlan 10-199
Continuity Check for ME level 4 in vlans 10-199 is enabled.
Console> (enable)
```

set ethernet-cfm continuity-check level

To configure continuity-check message attributes for a specific level of the local MEPs, use the **set ethernet-cfm continuity-check level** command.

set ethernet-cfm continuity-check level *level* **vlan** *vlans* **interval** *interval-value* [**loss-threshold** *threshold*]

Syntax Description

level	Maintenance level of the local MEPs; valid values are from 0 to 7.
vlan *vlans*	VLAN or a range of VLANs on which to do the check; valid values are from 1 to 4094.
internal *interval-value*	Interval between continuity check messages; valid values are 0 to 2000 seconds.
loss-threshold *threshold*	(Optional) Specifies the number of continuity-check messages that can be lost before cleaning up the corresponding entry in the continuity-check database; valid values are from 0 to 10.

Defaults

The default settings are as follows:

interval-value: 10 seconds

threshold: 2 messages.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set ethernet-cfm continuity-check level** command sets the broadcast attribute of local MEPs.

Use the *interval-value* argument to configure how often continuity-check messages are sent. If you configure the *interval-value* too small, and there are multiple small interval configurations, a warning message is issued. [what does this mean?]

You can enter the *threshold* argument to specify the message loss threshold. Whenever a continuity-check entry is aged out, a syslog message is generated indicating that the connection to the MPID may have issues. [what does this mean?]

Examples

This example shows how to configure continuity check message attributes for a level of 100, VLAN range of 10-100, and interval of 800 seconds and a loss-threshold of 2 messages:

```
Console> (enable) set ethernet-cfm continuity-check level 100 vlan 10-100 interval 800
loss-threshold 4
Continuity Check for ME level 100 in vlan 10-100 interval set to 800.
Console> (enable)
```

8.6 EFT Copy

set ethernet-cfm domain

To create a maintenance domain and configure the maintenance level, use the **set ethernet-cfm domain** command.

set ethernet-cfm domain *domain-name* **level** *level*

Syntax Description

domain-name	Maintenance domain name.
level	Maintenance level; valid values are from 0 to 7.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Is the maintenance level created by this command or just specified?

Examples

This example shows how to a configure a maintenance domain ‘customerXYDomain’ with level 100:

```
Console> (enable) set ethernet-cfm enable domain customerXYDomain level 6
CFM Domain ‘customerXYDomain’ (level 6) created.
Console> (enable)
```

set ethernet-cfm ping-reply

To enable or disable the service support for CFM loop-back, use the **set ethernet-cfm ping-reply** command. [This command not in 8.6(0.234)TAL.]

set ethernet-cfm ping-reply {**disable** | **enable** | **mp-only**}

Syntax Description

disable	Enables a response to a CFM loop-back ping.
enable	Disables a response to a CFM loop-back ping.
mp-only	Enables a response to a CFM loop-back ping addressed to a local MEP or MIP only.

Defaults

The ping-reply is mp-only.

Command Modes

Privileged.

Command Types

Switch command.

Usage Guidelines

This command is under evaluation and might not be implemented in phase 1.

Examples

This example shows how to initialize CFM loop-back ping-reply:

```
Console> (enable) set ethernet-cfm ping-reply enable
CFM loop-back ping-reply is enabled.
Console> (enable)
```

set ethernet-cfm vlan

To associate a VLAN in a specific maintenance domain with a customer service instance identifer (CSID), use the **set ethernet-cfm vlan** command.

set ethernet-cfm vlan *vlans* **domain** *domain-name* **service** *csi-id*

Syntax Description

vlans	VLAN or a range of VLANs in the specified maintenance domain. Valid values: any integer or range of integers (examples, 10, 10-120).
domain *domain-name*	Domain where VLAN is located. Valid values: any string representing the domain name (example, 'customerYZDomain')
service *csi-id*	Customer service instance identifer to associate with VLAN. Valid value: any string.

Defaults

No CSID is assigned to any VLAN.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use this command to associate the VLAN and the CSID.

Ensure that the maintenance domain and the CSID exist prior to entering this command.

Examples

This example shows how to associate VLAN 120 in the domain customerYZDomain with the CSID of custZ:

```
Console> (enable) set ethernet-cfm vlan 120 domain customerYZDomain service custZ
Vlan 120 is mapped to csid custZ..
Console> (enable)
```

8.6 EFT Copy

set fan-tray-version

To set the version for the fan tray in the chassis, use the **set fan-tray-version** command.

set fan-tray-version {**1** | **2**}

Syntax Description

1	Specifies version 1 for a lower-powered fan tray.
2	Specifies version 2 for a higher-powered fan tray.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set fan-tray-version** command informs the software of the fan tray type so that the software can make the right cooling and power consumption adjustments for the chassis. The fan tray version is stored in the backplane IDPROM.

You must enter **set fan-tray-version 2** before installing a higher-powered fan tray. You must enter **set fan-tray-version 1** before downgrading to a lower-powered fan tray.

Use a higher-powered fan tray with a Supervisor Engine 720 with the 2500 W or 4000 W power supply.

Enter the **show environment cooling** command to display the fan tray version for the chassis.

Examples

This example shows how to set the fan tray version:

```
Console> (enable) set fan-tray-version 2
Programming successful for Chassis Serial EEPROM.
Fan tray version set to 2
Console> (enable)
```

Related Commands

show environment

set feature agg-link-partner

To enable or disable the aggressive link partner feature, use the **set feature agg-link-partner** command.

set feature agg-link-partner {**enable** | **disable**}

Syntax Description

enable	Enables the aggressive link partner feature.
disable	Disables the aggressive link partner feature.

Defaults

The aggressive link partner feature is disabled globally.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enable this feature, you reduce the possibility of aggressive link partners causing excessive collisions. Excessive collisions can lead to excessive alignment errors and runts.

The aggressive link partner feature works only on half duplex 10/100 ports.

The **set feature agg-link-partner** command is a global command so when you enable or disable this feature, all related modules in the chassis are enabled or disabled.

Examples

This example shows how to enable the aggressive link partner feature:

```
Console> (enable) set feature agg-link-partner enable
Aggressive link partner feature enabled.
Console> (enable)
```

This example shows how to disable the aggressive link partner feature:

```
Console> (enable) set feature agg-link-partner disable
Aggressive link partner feature disabled.
Console> (enable)
```

set feature mdg

To enable or disable the multiple default gateway feature, use the **set feature mdg** command.

set feature mdg {**enable** | **disable**}

Syntax Description

enable	Enables the multiple default gateway.
disable	Disables the multiple default gateway.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enable the multiple default gateway feature, the Catalyst 6500 series switch pings the default gateways every 10 seconds to verify that the gateways are still available.

Examples

This example shows how to enable the multiple default gateway feature:

```
Console> (enable) set feature mdg enable
Multiple  Gateway feature enabled.
Console> (enable)
```

This example shows how to disable the multiple default gateway feature:

```
Console> (enable) set feature mdg disable
Multiple  Gateway feature disabled.
Console> (enable)
```

8.6 EFT Copy

set firewall

To configure the parameters for a Firewall Services Module (FWSM), use the **set firewall** command.

set firewall multiple-vlan-interfaces {**enable** | **disable**}

Syntax Description

multiple-vlan-interfaces	Sets the multiple VLAN interface feature for an FWSM.
enable	Enables multiple VLAN interfaces for an FWSM.
disable	Disables multiple VLAN interfaces for an FWSM.

Defaults

The multiple VLAN interface feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Disabling the multiple VLAN interface feature sets the FWSM to single VLAN interface mode.

Examples

This example shows how to enable the multiple VLAN feature on a firewall module:

```
Console> (enable) set firewall multiple-vlan-interfaces enable
This command will enable multiple vlan feature for all firewall modules in the
chassis .Can result in traffic bypassing the firewall module
Do you want to continue (y/n) [n]?y
Multiple vlan feature enabled for firewall
Console> (enable)
```

This example shows how to disable the multiple VLAN feature on a firewall module:

```
Console> (enable) set firewall multiple-vlan-interfaces disable
This command will disable multiple vlan feature for all firewall modules in the chassis.
Do you want to continue (y/n) [n]?y
Multiple vlan feature disabled for firewalls. All layer 3 firewall vlan interfaces have
been brought down on MSFC
Please remove all the layer 3 firewall vlan interfaces from MSFC using no interface
command on MSFC.
Console> (enable)
```

Related Commands

show firewall

set ftp

To configure File Transfer Protocol (FTP) parameters, use the **set ftp** command.

set ftp username *new_ftp_username*

set ftp password *new_ftp_password*

set ftp mode passive {**enable** | **disable**}

Syntax Description

username	Specifies a username for FTP connections.
new_ftp_username	Username for FTP.
password	Specifies a password for FTP connections.
new_ftp_password	Password for FTP.
mode	Specifies the FTP mode.
passive	Specifies passive mode for FTP connections.
enable	Enables passive mode.
disable	Disables passive mode.

Defaults

The FTP mode is set to passive.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

For security reasons, the *new_ftp_password* argument is not stored in NVRAM. The password is encrypted by using a proprietary encryption algorithm.

The FTP mode is passive. To clear the FTP passive mode, use the **clear ftp passive** command.

Examples

This example shows how to specify a username for FTP connections:

```
Console> (enable) set ftp username dkoya
Ftp username set to dkoya.
Console> (enable)
```

This example shows how to specify a password for FTP connections:

```
Console> (enable) set ftp password mypassword
Ftp password set.
Console> (enable)
```

This example shows how to disable FTP passive mode:

```
Console> (enable) set ftp mode passive disable
FTP Passive mode disabled.
Console> (enable)
```

Related Commands

clear ftp
show ftp

set garp timer

To adjust the values of the join, leave, and leaveall timers, use the **set garp timer** command.

set garp timer {*timer_type*} {*timer_value*}

Syntax Description

timer_type	Type of timer; valid values are **join**, **leave,** and **leaveall**.
timer_value	Timer values in milliseconds; valid values are from 1 to 2147483647 milliseconds.

Defaults

The defaults are the join timer is 200 milliseconds, the leave timer is 600 milliseconds, and the leaveall timer is 10000 milliseconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The modified timer values are applied to all General Attribute Registration Protocol (GARP) applications (for example, GMRP and GVRP) timer values.

You must maintain the following relationship for the various timer values:

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.

Caution Set the same GARP application (for example, GMRP and GVRP) timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP applications will not operate successfully.

Examples

This example shows how to set the join timer value for all the ports on all the VLANs:

```
Console> (enable) set garp timer join 100
GMRP/GARP Join timer value is set to 100 milliseconds.
Console> (enable)
```

This example shows how to set the leave timer value for all the ports on all the VLANs:

```
Console> (enable) set garp timer leave 300
GMRP/GARP Leave timer value is set to 300 milliseconds.
Console> (enable)
```

Related Commands

set gmrp timer
set gvrp timer
show garp timer

set gmrp

To enable or disable GARP Multicast Registration Protocol (GMRP) on the switch in all VLANs on all ports, use the **set gmrp** command.

set gmrp {**enable** | **disable**}

Syntax Description

enable	Enables GMRP on the switch.
disable	Disables GMRP on the switch.

Defaults

The default is GMRP is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You cannot enable GMRP if IGMP snooping is already enabled.

Examples

This example shows how to enable GMRP on the switch:

```
Console> (enable) set gmrp enable
GMRP is enabled.
Console> (enable)
```

This example shows how to disable GMRP on the switch:

```
Console> (enable) set gmrp disable
GMRP is disabled.
Console> (enable)
```

This example shows the display if you try to enable GMRP on the switch with IGMP enabled:

```
Console> (enable) set gmrp enable
Disable IGMP to enable GMRP snooping feature.
Console> (enable)
```

Related Commands

show gmrp configuration

set gmrp fwdall

To enable or disable the Forward All feature on a specified port or module and port list, use the **set gmrp fwdall** command.

set gmrp fwdall {**enable** | **disable**} *mod/port...*

Syntax Description

enable	Enables GMRP Forward All on a specified port.
disable	Disables GMRP Forward All on a specified port.
mod/port...	Number of the module and the ports on the module.

Defaults

The default is the Forward All feature is disabled for all ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Forward All indicates that a port is interested in receiving all the traffic for all the multicast groups.

If the port is trunking, then this feature is applied to all the VLANs on that port.

Examples

This example shows how to enable GMRP Forward All on module 5, port 5:

```
Console> (enable) set gmrp fwdall enable 5/5
GMRP Forward All groups option enabled on port(s) 5/5.
Console> (enable)
```

This example shows how to disable the GMRP Forward All on module 3, port 2:

```
Console> (enable) set gmrp service fwdall disable 3/2
GMRP Forward All groups option disabled on port(s) 3/2.
Console> (enable)
```

Related Commands

show gmrp configuration

set gmrp registration

To specify the GMRP registration type, use the **set gmrp registration** command.

set gmrp registration {**normal** | **fixed** | **forbidden**} *mod/port...*

Syntax Description

normal	Specifies dynamic GMRP multicast registration and deregistration on the port.
fixed	Specifies the multicast groups currently registered on the switch are applied to the port, but any subsequent registrations or deregistrations do not affect the port. Any registered multicast groups on the port are not deregistered based on the GARP timers.
forbidden	Specifies that all GMRP multicasts are deregistered and prevent any further GMRP multicast registration on the port.
mod/port...	Number of the module and the ports on the module.

Defaults

The default is administrative control is normal.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must return the port to **normal** registration mode to deregister multicast groups on the port.

GMRP supports a total of 3072 multicast addresses for the whole switch.

Examples

This example shows how to set the registration type to **fixed** on module 3, port 3:

```
Console> (enable) set gmrp registration fixed 3/3
GMRP Registration is set to Fixed for port(s) 3/3.
Console> (enable)
```

This example shows how to set the registration type to **forbidden** on module 1, port 1:

```
Console> (enable) set gmrp registration forbidden 1/1
GMRP Registration is set to Forbidden for port(s) 1/1.
Console> (enable)
```

Related Commands

show gmrp configuration

set gmrp timer

To adjust the values of the join, leave, and leaveall timers, use the **set gmrp timer** command.

set gmrp timer {*timer_type*} {*timer_value*}

Syntax Description

timer_type	Type of timer; valid values are **join**, **leave,** and **leaveall**.
timer_value	Timer values in milliseconds; valid values are from 1 to 2147483647 milliseconds.

Defaults

The default is the join timer is 200 milliseconds, the leave timer is 600 milliseconds, and the leaveall timer is 10000 milliseconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must maintain the following relationship for the various timer values:

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.

Caution Set the same GARP application (for example, GMRP and GVRP) timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP applications will not operate successfully.

Note The modified timer values are applied to all GARP application (for example, GMRP and GVRP) timer values.

Examples

This example shows how to set the join timer value to 100 milliseconds for all the ports on all the VLANs:

```
Console> (enable) set gmrp timer join 100
GARP Join timer value is set to 100 milliseconds.
Console> (enable)
```

This example shows how to set the leave timer value to 300 milliseconds for all the ports on all the VLANs:

```
Console> (enable) set gmrp timer leave 300
GARP Leave timer value is set to 300 milliseconds.
Console> (enable)
```

This example shows how to set the leaveall timer value to 20000 milliseconds for all the ports on all the VLANs:

```
Console> (enable) set gmrp timer leaveall 20000
GARP LeaveAll timer value is set to 20000 milliseconds.
Console> (enable)
```

Related Commands

set garp timer
set gvrp timer
show gmrp timer

set gvrp

To enable or disable GARP VLAN Registration Protocol (GVRP) globally in the switch or on a per-port basis, use the **set gvrp** command.

set gvrp {**enable** | **disable**} [*mod/port*]

Syntax Description

enable	Enables GVRP on the switch.
disable	Disables GVRP on the switch.
mod/port	(Optional) Number of the module and port on the module.

Defaults

The default is GVRP is globally set to disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enable VTP pruning, VTP pruning runs on all the GVRP-disabled trunks.

To run GVRP on a trunk, you need to enable GVRP both globally on the switch and individually on the trunk.

Examples

This example shows how to enable GVRP globally on the switch:

```
Console> (enable) set gvrp enable
GVRP enabled.
Console> (enable)
```

This example shows how to disable GVRP:

```
Console> (enable) set gvrp disable
GVRP disabled.
Console> (enable)
```

This example shows how to enable GVRP on module 2, port 1:

```
Console> (enable) set gvrp enable 2/1
GVRP enabled on port 2/1.
Console> (enable)
```

Related Commands

set garp timer
set gvrp timer
show gmrp timer
show gvrp configuration

8.6 EFT Copy

set gvrp applicant

To specify whether or not a VLAN is declared out of blocking ports, use the **set gvrp applicant** command.

set gvrp applicant {**normal** | **active**} {*mod/port...*}

Syntax Description

normal	Disallows the declaration of any VLAN out of blocking ports.
active	Enforces the declaration of all active VLANs out of blocking ports.
mod/port..	Number of the module and the ports on the module.

Defaults

The default is GVRP applicant set to normal.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To run GVRP on a trunk, you need to enable GVRP both globally on the switch and individually on the trunk.

On a port connected to a device that does not support the per-VLAN mode of STP, the port state may continuously cycle from blocking to listening to learning, and back to blocking. To prevent this, you must enter the **set gvrp applicant active** *mod/port...* command on the port to send GVRP VLAN declarations when the port is in the STP blocking state.

Examples

This example shows how to enforce the declaration of all active VLANs out of specified blocking ports:

```
Console> (enable) set gvrp applicant active 4/2-3,4/9-10,4/12-24
Applicant was set to active on port(s) 4/2-3,4/9-10,4/12-24.
Console> (enable)
```

This example shows how to disallow the declaration of any VLAN out of specified blocking ports:

```
Console> (enable) set gvrp applicant normal 4/2-3,4/9-10,4/12-24
Applicant was set to normal on port(s) 4/2-3,4/9-10,4/12-24.
Console> (enable)
```

Related Commands

show gvrp configuration

set gvrp dynamic-vlan-creation

To enable or disable dynamic VLAN creation, use the **set gvrp dynamic-vlan-creation** command.

set gvrp dynamic-vlan-creation {**enable** | **disable**}

Syntax Description

enable	Enables dynamic VLAN creation.
disable	Disables dynamic VLAN creation.

Defaults

The default is dynamic VLAN creation is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can enable dynamic VLAN creation only when VTP is in transparent mode and no ISL trunks exist in the switch.

This feature is not allowed when there are 802.1Q trunks that are not configured with GVRP.

Examples

This example shows how to enable dynamic VLAN creation:

```
Console> (enable) set gvrp dynamic-vlan-creation enable
Dynamic VLAN creation enabled.
Console> (enable)
```

This example shows what happens if you try to enable dynamic VLAN creation and VTP is not in transparent mode:

```
Console> (enable) set gvrp dynamic-vlan-creation enable
VTP has to be in TRANSPARENT mode to enable this feature.
Console> (enable)
```

This example shows how to disable dynamic VLAN creation:

```
Console> (enable) set gvrp dynamic-vlan-creation disable
Dynamic VLAN creation disabled.
Console> (enable)
```

Related Commands

set vtp
show gvrp configuration

set gvrp registration

To set the administrative control of an outbound port and apply to all VLANs on the trunk, use the **set gvrp registration** command. GVRP registration commands are entered on a per-port basis.

set gvrp registration {**normal** | **fixed** | **forbidden**} *mod/port...*

Syntax Description

normal	Allows dynamic registering and deregistering each VLAN (except VLAN 1) on the port.
fixed	Supports manual VLAN creation and registration, prevent VLAN deregistration, and register all VLANs known to other ports.
forbidden	Specifies that all the VLANs (except VLAN 1) are statically deregistered from the port.
mod/port...	Number of the module and the ports on the module.

Defaults

The default administrative control is normal.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you set VLAN registration, you are communicating to the switch that the VLAN is interested in the users that are connecting to this port and that the VLAN's broadcast and multicast traffic is allowed to be sent to the port.

For static VLAN configuration, you should set the *mod/port...* control to **fixed** or **forbidden** if the *mod/port...* will not receive or process any GVRP message.

For each dynamically configured VLAN on a port, you should set the *mod/port...* control to **normal** (default), except for VLAN 1; GVRP registration mode for VLAN 1 is always fixed and is not configurable. VLAN 1 is always carried by 802.1Q trunks on which GVRP is enabled.

When GVRP is running, you can create a VLAN through a GVRP trunk port only if you enter the **set gvrp dynamic-vlan-creation enable** and the **set gvrp registration normal** commands.

Examples

This example shows how to set the administrative control to **normal** on module 3, port 7:

```
Console> (enable) set gvrp registration normal 3/7
Registrar Administrative Control set to normal on port 3/7.
Console> (enable)
```

This example shows how to set the administrative control to **fixed** on module 5, port 10:

```
Console> (enable) set gvrp registration fixed 5/10
Registrar Administrative Control set to fixed on Port 5/10.
Console> (enable)
```

This example shows how to set the administrative control to **forbidden** on module 5, port 2:

```
Console> (enable) set gvrp registration forbidden 5/2
Registrar Administrative Control set to forbidden on port 5/2.
Console> (enable)
```

Related Commands

show gvrp configuration

set gvrp timer

To adjust the values of the join, leave, and leaveall timers, use the **set gvrp timer** command.

set gvrp timer {*timer_type*} {*timer_value*}

Syntax Description

timer_type	Type of timer; valid values are **join**, **leave,** and **leaveall**.
timer_value	Timer values in milliseconds; valid values are from 1 to 2147483647 milliseconds.

Defaults

The default is the join timer is 200 milliseconds, the leave timer is 600 milliseconds, and the leaveall timer is 10000 milliseconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must maintain the following relationship for the various timer values:

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.

Caution Set the same GARP application (for example, GMRP and GVRP) timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP applications will not operate successfully.

Note The modified timer values are applied to all GARP application (for example, GMRP and GVRP) timer values.

Examples

This example shows how to set the join timer value to 100 milliseconds for all the ports on all the VLANs:

```
Console> (enable) set gvrp timer join 100
GVRP/GARP Join timer value is set to 100 milliseconds.
Console> (enable)
```

This example shows how to set the leave timer value to 300 milliseconds for all the ports on all the VLANs:

```
Console> (enable) set gvrp timer leave 300
GVRP/GARP Leave timer value is set to 300 milliseconds.
Console> (enable)
```

This example shows how to set the leaveall timer value to 20000 milliseconds for all the ports on all the VLANs:

```
Console> (enable) set gvrp timer leaveall 20000
GVRP/GARP LeaveAll timer value is set to 20000 milliseconds.
Console> (enable)
```

Related Commands

set garp timer
show gvrp configuration

set igmp

To enable or disable Internet Group Management Protocol (IGMP) snooping on the switch, use the **set igmp** command.

set igmp {**enable** | **disable**}

Syntax Description

enable	Enables IGMP snooping on the switch.
disable	Disables IGMP snooping on the switch.

Defaults

The default is IGMP snooping is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

IGMP must be disabled to run GMRP.

If your system is configured with a Supervisor Engine 1, you must enable one of the multicast services (IGMP snooping or GMRP) on the switch in order to use IP MMLS.

Examples

This example shows how to enable IGMP snooping on the switch:

```
Console> (enable) set igmp enable
IGMP feature for IP multicast enabled
Console> (enable)
```

This example shows how to disable IGMP snooping on the switch:

```
Console> (enable) set igmp disable
IGMP Snooping is disabled.
Console> (enable)
```

This example shows the display if you try to enable GMRP on the switch with IGMP enabled:

```
Console> (enable) set igmp enable
Disable GMRP to enable IGMP snooping feature.
Console> (enable)
```

Related Commands

clear igmp statistics
set rgmp
show igmp statistics

set igmp fastblock

To enable or disable the IGMP version 3 fast-block mechanism on the switch, use the **set igmp fastblock** command.

set igmp fastblock {**enable** | **disable**}

Syntax Description

enable	Enables the IGMP version 3 fast-block mechanism.
disable	Disables the IGMP version 3 fast-block mechanism.

Defaults

By default, the IGMP version 3 fast-block mechanism is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable the fast-block mechanism on the switch:

```
Console> (enable) set igmp fastblock enable
IGMP V3 fastblock enabled
Console> (enable)
```

This example shows how to disable the fast-block mechanism on the switch:

```
Console> (enable) set igmp fastblock disable
IGMP V3 fastblock disabled
Console> (enable)
```

Related Commands

set igmp v3-processing
show multicast v3-group

set igmp fastleave

To enable or disable Internet Group Management Protocol (IGMP) fastleave processing, use the **set igmp fastleave** command.

set igmp fastleave {**enable** | **disable**}

Syntax Description

enable	Enables IGMP fastleave processing.
disable	Disables IGMP fastleave processing.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This command shows how to enable IGMP fastleave processing:

```
Console> (enable) set igmp fastleave enable
IGMP fastleave set to enable.
Warning: Can cause disconnectivity if there are more than one host joining the same group
per access port.
Console> (enable)
```

This command shows how to disable IGMP fastleave processing:

```
Console> (enable) set igmp fastleave disable
IGMP fastleave set to disable.
Console> (enable)
```

Related Commands

clear igmp statistics
set igmp
show multicast protocols status

set igmp flooding

To activate or to prevent flooding of multicast traffic after the last host leaves a multicast group, enter the **set igmp flooding** command.

set igmp flooding {**enable** | **disable**}

Syntax Description

enable	Activates multicast flooding.
disable	Prevents multicast flooding.

Defaults

IGMP flooding is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

For more information about IGMP flooding, refer to the "Understanding How IGMP Snooping Works" section of the "Configuring Multicast Services" chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example shows how to prevent the flooding of multicast traffic after the last host leaves a multicast group:

```
Console> (enable) set igmp flooding disable
IGMP Flooding disabled
Console> (enable)
```

This example shows how to enable the flooding of multicast traffic after the last host leaves a multicast group:

```
Console> (enable) set igmp flooding enable
IGMP Flooding enabled (default)
Console> (enable)
```

8.6 EFT Copy

set igmp leave-query-type

To set the type of query to be sent when a port receives a leave message, use the **set igmp leave-query-type** command.

set igmp leave-query-type {**mac-gen-query** | **general-query** | **auto-mode**}

Syntax Description

mac-gen-query	Specifies sending a MAC-based general query on receiving a leave message.
general-query	Specifies sending a general query on receiving a leave message.
auto-mode	Specifies sending a group-specific query if no version 1 hosts are detected.

Defaults

By default, a MAC-based general query is sent when a port receives a leave message.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to send a MAC-based general query:

```
Console> (enable) set igmp leave-query-type mac-gen-query
Console> (enable)
```

This example shows how to send a general query:

```
Console> (enable) set igmp leave-query-type general-query
Console> (enable)
```

This example shows how to send a group-specific query if no version 1 hosts are detected:

```
Console> (enable) set igmp leave-query-type auto-mode
IGMP Leave Query Type set to Auto-Type
Console> (enable)
```

Related Commands

show igmp leave-query-type

set igmp mode

To set the IGMP snooping mode, use the **set igmp mode** command.

set igmp mode {**igmp-only** | **igmp-cgmp** | **auto**}

Syntax Description

igmp-only	Specifies IGMP snooping only.
igmp-cgmp	Specifies IGMP and CGMP modes.
auto	Overrides the dynamic switching of IGMP snooping modes.

Defaults

The default is IGMP mode is **auto**.

Command Types

Switch.

Command Modes

Privileged.

Usage Guidelines

The switch dynamically chooses either IGMP-only or IGMP-CGMP mode, depending on the traffic present on the network. IGMP-only mode is used in networks with no CGMP devices. IGMP-CGMP mode is used in networks with both IGMP and CGMP devices. Auto mode overrides the dynamic switching of the modes.

Examples

This example shows how to set the IGMP mode to IGMP-only:

```
Console> (enable) set igmp mode igmp-only
IGMP mode set to igmp-only
Console> (enable)
```

This example shows how to set the IGMP mode to auto:

```
Console> (enable) set igmp mode auto
IGMP mode set to auto
Console> (enable)
```

Related Commands

show igmp mode

set igmp querier

To configure the IGMP querier for a specific VLAN, use the **set igmp querier** command.

set igmp querier {**enable** | **disable**} *vlan*

set igmp querier *vlan* {**qi** | **oqi**} *seconds*

set igmp querier address *vlan ip_addr*

Syntax Description

enable	Enables the IGMP querier for a VLAN.
disable	Disables the IGMP querier for a VLAN.
vlan	Number of the VLAN.
qi	Sets the querier interval for the VLAN.
oqi	Sets the other querier interval for the VLAN.
seconds	Range of the querier interval or the other querier interval in seconds; valid values are from 1 to 65535 seconds.
address	Sets the querier IP address for the VLAN.
ip_addr	IP address for the VLAN.

Defaults

IGMP querier is disabled.

The default value for **qi** is 125 seconds.

The default value for **oqi** is 300 seconds.

The default value for *ip_addr* is 0.0.0.0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must enable IGMP querier on every VLAN for which switch querier functionality is required. In the absence of general queries, the **oqi** value is the amount of time a switch waits before electing itself as the querier.

Examples

This example shows how to enable the IGMP querier for VLAN 4001:

```
Console> (enable) set igmp querier enable 4001
IGMP switch querier enabled for VLAN 4001
Console> (enable)
```

This example shows how to set the querier interval to 130 seconds for VLAN 4001:

```
Console> (enable) set igmp querier 4001 qi 130
QI for VLAN 4001 set to 130 second(s)
Console> (enable)
```

Related Commands

show igmp querier information

8.6 EFT Copy

set igmp v3-processing

To explicitly enable or disable IGMP version 3 snooping, use the **set igmp v3-processing** command.

set igmp v3-processing {**enable** | **disable**}

Syntax Description

enable	Enables IGMP version 3 snooping.
disable	Disables IGMP version 3 snooping.

Defaults

By default, IGMP version 3 snooping is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

IGMP version 3 is supported on Supervisor Engine 2 and Supervisor Engine 720. Supervisor Engine 1 and Supervisor Engine 1A do not support this feature.

If IGMP version 3 processing is disabled, any previous IGMP version 3 snooping entries are cleared. These IGMP version 3 entries are relearned as IGMP version 2 (GDA-based) entries after the switch receives an IGMP version 3 report. Any subsequent IGMP version 3 reports for other multicast sources or groups are also processed as IGMP version 2 reports.

When MMLS is enabled, IGMP version 3 processing works only in PIM SSM mode. If MMLS is disabled, IGMP version 3 reports are processed as IGMP version 2 reports. IGMP version 3 processing works independent of PIM mode when MMLS is enabled.

Examples

This example shows how to enable IGMP version 3 processing:

```
Console> (enable) set igmp v3-processing enable
IGMP V3 processing enabled
Console> (enable)
```

This example shows how to disable IGMP version 3 processing:

```
Console> (enable) set igmp v3-processing disable
IGMP V3 processing disabled
Console> (enable)
```

Related Commands

set igmp fastblock
show multicast v3-group

8.6 EFT Copy

set image-verification

To ensure the integrity of a downloaded image, use the **set image-verification** command.

set image-verification [**boot** | **copy** | **reset**] {**enable** | **disable**}

Syntax Description

boot	(Optional) Specifies image verification at boot time.
copy	(Optional) Specifies image verification at copy time.
reset	(Optional) Specifies image verification at reset time.
enable	Enables image verification.
disable	Disables image verification.

Defaults

The image verification feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure the image verification feature to work when the system is booting, after the image has been copied, or before a system resets. If you enable or disable the image verification feature without specifying the **boot** keyword, the **copy** keyword, or the **reset** keyword, all three are enabled or disabled.

Examples

This example shows how to enable the image verification feature at reset time:

```
Console> (enable) set image-verification reset enable
Console> (enable)
```

This example shows how to disable the image verification feature at copy time:

```
Console> (enable) set image-verification copy disable
Console> (enable)
```

Related Commands

show image-verification

8.6 EFT Copy

set inlinepower

To set inline power parameters, use the **set inlinepower** command.

set inlinepower defaultallocation *value*

set inlinepower notify-threshold *value* **module** *mod*

Syntax Description

defaultallocation	Sets the default power allocation per port
value	Default power allocation; valid values are from 4000 to 15400 milliwatts.
notify-threshold	Sets the inline power usage notification threshold.
value	Percentage of power usage that sets off the threshold notification; valid values are from 1 to 99 percent.
module *mod*	Specifies the module.

Defaults

The default allocation value is 15400 milliwatts.

The notification threshold is 99 percent.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set inlinepower defaultallocation** command is global and only affects Cisco IP phones.

Caution The **set inlinepower defaultallocation** command can be harmful when there is not enough power in the system to bring up all connected inline power devices. If you set a small *value* for the power allocation, all connected inline power devices initially will be powered up. However, after receiving CDP messages, the system will learn that devices are consuming more power and deny power to some of the ports. Setting a small value might also result in the overdrawing of power for some time with unanticipated results, such as hardware failures and unexpected resets.

7000 milliwatts is the maximum power supported for these modules: WS-X6148-RJ21V, WS-X6148-RJ45V, WS-X6348-RJ21V, and WS-X6348-RJ45V.

The inline power threshold notification generates a syslog message when inline power usage exceeds the specified threshold.

Examples

This example shows how to set the default power allocation to 9500 milliwatts:

```
Console> (enable) set inlinepower defaultallocation 9500
Default inline power allocation set to 9500 mWatt per applicable port.
Console> (enable)
```

This example shows how to set the threshold for the inline power usage notification:

```
Console> (enable) set inlinepower notify-threshold 40 module 4
Module 4 inlinepower notify-threshold is set to 40%.
Console> (enable)
```

Related Commands

set port inlinepower
show environment
show inlinepower
show port inlinepower

set interface

To configure the in-band and Serial Line Internet Protocol (SLIP) interfaces on the switch, use the **set interface** command.

set interface {**sc0** | **sl0** | **sc1**} {**up** | **down**}

set interface sl0 *slip_addr dest_addr*

set interface sc0 [*vlan*] [*ip_addr*[*netmask* [*broadcast*]]]

set interface sc0 [*vlan*] [*ip_addr/netmask* [*broadcast*]]

set interface sc0 dhcp {**renew** | **release**}

set interface sc1 [*vlan*] [*ip_addr*[*netmask* [*broadcast*]]]

set interface sc1 [*vlan*] [*ip_addr/netmask* [*broadcast*]]

Syntax Description

sc0	Specifies the sc0 in-band interface.
sl0	Specifies the SLIP interface.
sc1	Specifies the sc1 in-band interface.
up	Brings the interface into operation.
down	Brings the interface out of operation.
slip_addr	IP address of the console port.
dest_addr	IP address of the host to which the console port will be connected.
vlan	(Optional) Number of the VLAN to be assigned to the interface; valid values are from 1 to 4094.
ip_addr	(Optional) IP address.
/netmask	(Optional) Subnet mask.
broadcast	(Optional) Broadcast address.
dhcp	Performs Dynamic Host Configuration Protocol (DHCP) operations on the sc0 interface.
renew	Renews the lease on a DHCP-learned IP address.
release	Releases a DHCP-learned IP address back to the DHCP IP address pool.

Defaults

The default configuration is the in-band interface (sc0) in VLAN 1 with the IP address, subnet mask, and broadcast address set to 0.0.0.0. The default configuration for the SLIP interface (sl0) is that the IP address and broadcast address are set to 0.0.0.0.0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set interface sc0 dchp** command is valid only when the address is learned from the DHCP server and available in privileged mode only.

Two configurable network interfaces are on a Catalyst 6500 series switch: in-band (sc0) and SLIP (sl0). Configuring the sc0 interface with an IP address and subnet mask allows you to access the switch CLI using Telnet from a remote host. You should assign the sc0 interface to an active VLAN configured on the switch (the default is VLAN 1). Make sure the IP address you assign is in the same subnet as other stations in that VLAN.

Configuring the sl0 interface with an IP address and destination address allows you to make a point-to-point connection to a host through the console port. Use the **slip attach** command to activate SLIP on the console port (you will not be able to access the CLI using a terminal connected to the console port until you use the **slip detach** command to deactivate SLIP on the console port).

When you specify the *netmask* value, this indicates the number of bits allocated to subnetting in the host ID section of the given Class A, B, or C address. For example, if you enter an IP address for the sc0 interface as 172.22.20.7, the host ID bits for this Class B address is 16.

If you enter the *netmask* value in length of bits, for example, 204.20.22.7/24, the range for length is from 0 to 31 bits. If you do not enter the *netmask* value, the number of bits is assumed to be the natural netmask.

Examples

This example shows how to use **set interface sc0** and **set interface sl0** from the console port. It also shows how to bring down **interface sc0** using a terminal connected to the console port:

```
Console> (enable) set interface sc0 192.20.11.44/255.255.255.0
Interface sc0 IP address and netmask set.
Console> (enable) set interface sl0 192.200.10.45 192.200.10.103
Interface sl0 SLIP and destination address set.
Console> (enable) set interface sc0 down
Interface sc0 administratively down.
Console> (enable)
```

This example shows how to set the IP address for sc0 through a Telnet session. Note that the default netmask for that IP address class is used (for example, a Class C address uses 255.255.255.0, and a Class B uses 255.255.0.0):

```
Console> (enable) set interface sc0 192.200.11.40
This command may disconnect active telnet sessions.
Do you want to continue (y/n) [n]? y
Interface sc0 IP address set.
```

This example shows how to take the interface out of operation through a Telnet session:

```
Console> (enable) set interface sc0 down
This command will inactivate telnet sessions.
Do you want to continue (y/n) [n]? y
Interface sc0 administratively down.
```

This example shows how to assign the sc0 interface to a particular VLAN:

```
Console> (enable) set interface sc0 5
Interface sc0 vlan set.
Console> (enable)
```

This example shows what happens when you assign the sc0 interface to a nonactive VLAN:

```
Console> (enable) set interface sc0 200
Vlan is not active, user needs to set vlan 200 active
Interface sc0 vlan set.
Console> (enable)
```

This example shows how to release a DHCP-learned IP address back to the DHCP IP address pool:

```
Console> (enable) set interface sc0 dhcp release
Releasing IP address...Done
Console> (enable)
```

This example shows how to renew a lease on a DHCP-learned IP address:

```
Console> (enable) set interface sc0 dhcp renew
Renewing IP address...Done
Console> (enable)
```

This example shows how to set the IP address for sc1 from the console port:

```
Console> (enable) set interface sc1 10.6.33.15 255.255.255.0
set interface sc1 10.6.33.15 255.255.255.0
Interface sc1 IP address and netmask set.
Console> (enable)
```

Related Commands

show interface
slip

set ip alias

To add aliases of IP addresses, use the **set ip alias** command.

set ip alias *name ip_addr*

Syntax Description

name	Name of the alias being defined.
ip_addr	IP address of the alias being defined.

Defaults

The default configuration is one IP alias (0.0.0.0) configured as the default.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to define an IP alias of mercury for IP address 192.122.174.234:

```
Console> (enable) set ip alias mercury 192.122.174.234
IP alias added.
Console> (enable)
```

Related Commands

clear ip alias
show ip alias

set ip dns

To enable or disable DNS, use the **set ip dns** command.

set ip dns {**enable** | **disable**}

Syntax Description

enable	Enables DNS.
disable	Disables DNS.

Defaults

The default is DNS is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable DNS:

```
Console> (enable) set ip dns enable
DNS is enabled.
Console> (enable)
```

This example shows how to disable DNS:

```
Console> (enable) set ip dns disable
DNS is disabled.
Console> (enable)
```

Related Commands

show ip dns

8.6 EFT Copy

set ip dns domain

To set the default DNS domain name, use the **set ip dns domain** command.

set ip dns domain *name*

Syntax Description

name	DNS domain name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you specify a domain name on the command line, the system attempts to resolve the host name as entered. If the system cannot resolve the host name as entered, it appends the default DNS domain name as defined with the **set ip dns domain** command. If you specify a domain name with a trailing dot, the program considers this to be an *absolute* domain name.

Examples

This example shows how to set the default DNS domain name:

```
Console> (enable) set ip dns domain yow.com
 DNS domain name set to yow.com.
Console> (enable)
```

Related Commands

clear ip dns domain
show ip dns

set ip dns server

To set the IP address of a Domain Name System (DNS) server, use the **set ip dns server** command.

set ip dns server *ip_addr* [**primary**]

Syntax Description

ip_addr	IP address of the DNS server.
primary	(Optional) Configures a DNS server as the primary server.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure up to three DNS name servers as backup. You can also configure any DNS server as the primary server. The primary server is queried first. If the primary server fails, the backup servers are queried.

If DNS is disabled, you must use the IP address with all commands that require explicit IP addresses or manually define an alias for that address. The alias has priority over DNS.

Examples

These examples show how to set the IP address of a DNS server:

```
Console> (enable) set ip dns server 198.92.30.32
198.92.30.32 added to DNS server table as primary server.

Console> (enable) set ip dns server 171.69.2.132 primary
171.69.2.132 added to DNS server table as primary server.

Console> (enable) set ip dns server 171.69.2.143 primary
171.69.2.143 added to DNS server table as primary server.
```

This example shows what happens if you enter more than three DNS name servers as backup:

```
Console> (enable) set ip dns server 161.44.128.70
DNS server table is full. 161.44.128.70 not added to DNS server table.
```

Related Commands

clear ip dns server
show ip dns

set ip fragmentation

To enable or disable the fragmentation of IP packets bridged between FDDI and Ethernet networks, use the **set ip fragmentation** command.

set ip fragmentation {**enable** | **disable**}

Syntax Description

enable	Permits fragmentation for IP packets bridged between FDDI and Ethernet networks.
disable	Disables fragmentation for IP packets bridged between FDDI and Ethernet networks.

Defaults

The default value is IP fragmentation is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If IP fragmentation is disabled, packets are dropped.

Note that FDDI and Ethernet networks have different maximum transmission units (MTUs).

Examples

This example shows how to disable IP fragmentation:

```
Console> (enable) set ip fragmentation disable
Bridge IP fragmentation disabled.
Console> (enable)
```

Related Commands

show ip route

set ip http port

To configure the TCP port number for the HyperText Transfer Protocol (HTTP) server, use the **set ip http port** command.

set ip http port {**default** | *port-number*}

Syntax Description

default	Specifies the default HTTP server port number (80).
port-number	Number of the TCP port for the HTTP server; valid values are from 1 to 65535.

Defaults

The default TCP port number is 80.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the IP HTTP port default:

```
Console> (enable) set ip http port default
HTTP TCP port number is set to 80.
Console> (enable)
```

This example shows how to set the IP HTTP port number:

```
Console> (enable) set ip http port 2398
HTTP TCP port number is set to 2398.
Console> (enable)
```

Related Commands

set ip http server
show ip http

set ip http server

To enable or disable the HTTP server, use the **set ip http server** command.

set ip http server {**enable** | **disable**}

Syntax Description

enable	Enables the HTTP server.
disable	Disables the HTTP server.

Defaults

The default is the HTTP server is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable the HTTP server:

```
Console> (enable) set ip http server enable
HTTP server is enabled.
Console> (enable)
```

This example shows the system response when the HTTP server-enabled command is not supported:

```
Console> (enable) set ip http server enable
Feature not supported.
Console> (enable)
```

This example shows how to disable the HTTP server:

```
Console> (enable) set ip http server disable
HTTP server disabled.
Console> (enable)
```

Related Commands

set ip http port
show ip http

set ip permit

To enable or disable the IP permit list and to specify IP addresses to be added to the IP permit list, use the **set ip permit** command.

set ip permit {**enable** | **disable**}

set ip permit {**enable** | **disable**} [**telnet** | **ssh** | **snmp**]

set ip permit *addr* [*mask*] [**telnet** | **ssh** | **snmp** | **all**]

Syntax Description

enable	Enables the IP permit list.
disable	Disables the IP permit list.
telnet	(Optional) Specifies the Telnet IP permit list.
ssh	(Optional) Specifies the SSH IP permit list.
snmp	(Optional) Specifies the SNMP IP permit list.
addr	IP address to be added to the IP permit list. An IP alias or host name that can be resolved through DNS can also be used.
mask	(Optional) Subnet mask of the specified IP address.
all	(Optional) Specifies all entries in the IP permit list be removed.

Defaults

The default is IP permit list is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can achieve the same functionality of the IP permit list by using VLAN access control lists (VACLs). VACLs are handled by hardware (PFC), and the processing is considerably faster. For VACL configuration information, refer to the *Catalyst 6500 Series Switch Software Configuration Guide*.

You can configure up to 100 entries in the permit list. If you enable the IP permit list, but the permit list has no entries configured, a caution displays on the screen.

Make sure you enter the entire **disable** keyword when entering the **set ip permit disable** command. If you abbreviate the keyword, the abbreviation is interpreted as a host name to add to the IP permit list.

If you do not specify the **snmp**, **ssh**, **telnet**, or **all** keyword, the IP address is added to both the SNMP and Telnet permit lists.

You enter the mask in dotted decimal format, for example, 255.255.0.0.

Examples

This example shows how to add an IP address to the IP permit list:

```
Console> (enable) set ip permit 192.168.255.255
192.168.255.255 added to IP permit list.
Console> (enable)
```

This example shows how to add an IP address using an IP alias or host name to both the SNMP and Telnet permit lists:

```
Console> (enable) set ip permit batboy
batboy added to IP permit list.
Console> (enable)
```

This example shows how to add a subnet mask of the IP address to both the SNMP and Telnet permit lists:

```
Console> (enable) set ip permit 192.168.255.255 255.255.192.0
192.168.255.255 with mask 255.255.192.0 added to IP permit list.
Console> (enable)
```

This example shows how to add an IP address to the Telnet IP permit list:

```
Console> (enable) set ip permit 172.16.0.0 255.255.0.0 telnet
172.16.0.0 with mask 255.255.0.0 added to telnet permit list.
Console> (enable)
```

This example shows how to add an IP address to the SNMP IP permit list:

```
Console> (enable) set ip permit 172.20.52.32 255.255.255.224 snmp
172.20.52.32 with mask 255.255.255.224 added to snmp permit list.
Console> (enable)
```

This example shows how to add an IP address to all IP permit lists:

```
Console> (enable) set ip permit 172.20.52.3 all
172.20.52.3 added to IP permit list.
Console> (enable)
```

This example shows how to enable the IP permit list:

```
Console> (enable) set ip permit enable
Telnet, Snmp and Ssh permit list enabled
Console> (enable)
```

This example shows how to disable the IP permit list:

```
Console> (enable) set ip permit disable
Telnet, Snmp and Ssh permit list disabled.
Console> (enable)
```

This example shows how to enable a specific IP permit list type:

```
Console> (enable) set ip permit enable ssh
SSH permit list enabled.
Console> (enable)
```

Related Commands

clear ip permit
show ip permit

set ip redirect

To enable or disable ICMP redirect messages on the Catalyst 6500 series switches, use the **set ip redirect** command.

set ip redirect {**enable** | **disable**}

Syntax Description

enable	Permits ICMP redirect messages to be returned to the source host.
disable	Prevents ICMP redirect messages from being returned to the source host.

Defaults

The default configuration is ICMP redirect is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to deactivate ICMP redirect messages:

```
Console> (enable) set ip redirect disable
ICMP redirect messages disabled.
Console> (enable)
```

Related Commands

show ip route
show netstat

set ip route

To add IP addresses or aliases to the IP routing table, use the **set ip route** command.

set ip route {*destination*}[/*netmask*] {*gateway*} [*metric*] [**primary**]

Syntax Description

destination	IP address, IP alias of the network, or specific host to be added. Use **default** as the destination to set the new entry as the default route.
/netmask	(Optional) Number of bits in netmask or dot format (for example, 172.20.22.7/24 or 172.20.22.7/255.255.255.0).
gateway	IP address or IP alias of the router.
metric	(Optional) Value used to indicate the number of hops between the switch and the gateway.
primary	(Optional) Used with the multiple IP gateways feature to specify the default IP gateway with the highest priority.

Defaults

The default configuration routes the local network through the sc0 interface with metric 0 as soon as sc0 is configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure up to three default gateways. The **primary** is the highest priority. If you do not designate a primary gateway, priority is based on the order of input. If you enter two primary definitions, the second definition becomes the primary and the first definition becomes the secondary default IP gateway.

You can only specify the **primary** keyword for a default route.

When you enter the *destination* value or *gateway* value, enter it in dot notation, for example, a.b.c.d.

When you specify the *netmask* value, this indicates the number of bits allocated to subnetting in the host ID section of the given Class A, B, or C address. For example, if you enter an IP address for the sc0 interface as 172.22.20.7, the host ID bits for this Class B address is 16. Any number of bits in the host ID bits can be allocated to the netmask field. If you do not enter the *netmask* value, the number of bits is assumed to be the natural netmask.

When you enter the netmask, enter it as the number of bits or dot format, for example, **destination/24** or **destination/255.255.255.0**. If you enter the netmask in dot format, you must have contiguous 1s.

Examples

These examples show how to add three default routes to the IP routing table, checking after each addition using the **show ip route** command:

```
Console> (enable) set ip route default 192.122.173.42 1 primary
Route added.
Console> (enable)

Console> (enable) show ip route
Fragmentation   Redirect   Unreachable
-------------   --------   -----------
enabled         enabled    enabled
Destination     Gateway         Flags   Use         Interface
--------------- --------------- ------  ----------  ---------
default         192.122.173.42   UG            59444  sc0
192.22.74.0     192.22.74.223    U                 5  sc0
Console> (enable)
Console> (enable) set ip route default 192.122.173.43 1
Route added.
Console> (enable)

Console> (enable) show ip route
Fragmentation   Redirect   Unreachable
-------------   --------   -----------
enabled         enabled    enabled
Destination     Gateway         Flags   Use         Interface
--------------- --------------- ------  ----------  ---------
default         192.122.173.43   UG            59444  sc0
default         192.122.173.42   UG            59444  sc0
192.22.74.0     192.22.74.223    U                 5  sc0
Console> (enable)

Console> (enable) set ip route default 192.122.173.44 1
Route added.
Console> (enable)

Console> (enable) show ip route
Fragmentation   Redirect   Unreachable
-------------   --------   -----------
enabled         enabled    enabled
Destination     Gateway         Flags   Use         Interface
--------------- --------------- ------  ----------  ---------
default         192.122.173.44   UG            59444  sc0
default         192.122.173.43   UG            59444  sc0
default         192.122.173.42   UG            59444  sc0
192.22.74.0     192.22.74.223    U                 5  sc0
Console> (enable)
```

Related Commands

clear ip route
show ip route

set ip telnet server

To enable or disable the Telnet server, use the **set ip telnet server** command.

set ip telnet server {**enable** | **disable**}

Syntax Description

enable	Enables the Telnet server.
disable	Disables the Telnet server.

Defaults

The Telnet server is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable the Telnet server:

```
Console> (enable) set ip telnet server enable
Telnet server enabled
2005 Aug 23 08:12:20 %SYS-5-TELNET_STARTED:Telnet Daemon Started
Console> (enable)
```

Related Commands

show ip telnet

set ip unreachable

To enable or disable ICMP unreachable messages on the Catalyst 6500 series switch, use the **set ip unreachable** command.

set ip unreachable {**enable** | **disable**}

Syntax Description

enable	Allows IP unreachable messages to be returned to the source host.
disable	Prevents IP unreachable messages from being returned to the source host.

Defaults

The default is ICMP unreachable messages is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enable ICMP unreachable messages, the switch returns an ICMP unreachable message to the source host whenever it receives an IP datagram that it cannot deliver. When you disable ICMP unreachable messages, the switch does not notify the source host when it receives an IP datagram that it cannot deliver.

For example, a switch has the ICMP unreachable message function enabled and IP fragmentation disabled. If a FDDI frame is received and needs to transmit to an Ethernet port, the switch cannot fragment the packet. The switch drops the packet and returns an IP unreachable message to the Internet source host.

Examples

This example shows how to disable ICMP unreachable messages:

```
Console> (enable) set ip unreachable disable
ICMP Unreachable message disabled.
Console> (enable)
```

Related Commands

show ip route

set kerberos clients mandatory

To make Kerberos authentication mandatory for authenticating to services on the network, use the **set kerberos clients mandatory** command.

set kerberos clients mandatory

Syntax Description

This command has no arguments or keywords.

Defaults

The default is Kerberos clients are not set to mandatory.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

As an added layer of security, you can optionally configure the switch so that after users authenticate to it, they can authenticate to other services on the network only with Kerberos clients. If you do not make Kerberos authentication mandatory and Kerberos authentication fails, the application attempts to authenticate users using the default method of authentication for that network service. For example, Telnet prompts for a password.

Examples

This example shows how to make Kerberos authentication mandatory:

```
Console> (enable) set kerberos clients mandatory
Kerberos clients set to mandatory
Console> (enable)
```

Related Commands

clear kerberos clients mandatory
set kerberos credentials forward
show kerberos

set kerberos credentials forward

To configure clients to forward users' credentials as they connect to other hosts in the Kerberos realm, use the **set kerberos credentials forward** command.

set kerberos credentials forward

Syntax Description

This command has no arguments or keywords.

Defaults

The default is forwarding is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A user authenticated to a Kerberized switch has a ticket granting ticket (TGT) and can use it to authenticate to a host on the network. However, if forwarding is not enabled and a user tries to list credentials after authenticating to a host, the output will show no Kerberos credentials present.

You can optionally configure the switch to forward user TGTs as they authenticate from the switch to Kerberized remote hosts on the network by using Kerberized Telnet.

Examples

This example shows how to enable Kerberos credentials forwarding:

```
Console> (enable) set kerberos credentials forward
Kerberos credentials forwarding enabled
Console> (enable)
```

Related Commands

set kerberos clients mandatory
set kerberos local-realm
show kerberos

set kerberos local-realm

To configure a switch to authenticate users defined in the Kerberos database, use the **set kerberos local-realm** command.

set kerberos local-realm *kerberos_realm*

Syntax Description

kerberos_realm	IP address or name (in uppercase characters) of the Kerberos realm.

Defaults

The default value is a NULL string.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To authenticate a user defined in the Kerberos database, you must configure the switch to know the host name or IP address of the host running the KDC and the name of the Kerberos realm.

You must enter the Kerberos realm name in all uppercase characters.

Examples

This example shows how to set a default Kerberos local realm for the switch:

```
Console> (enable) set kerberos local-realm CISCO.COM
Kerberos local realm for this switch set to CISCO.COM.
Console> (enable)
```

Related Commands

clear kerberos realm
set kerberos realm
show kerberos

set kerberos realm

To map the name of a Kerberos realm to a DNS domain name or a host name, use the **set kerberos realm** command.

set kerberos realm {*dns_domain* | *host*} *kerberos_realm*

Syntax Description

dns_domain	DNS domain name to map to Kerberos realm.
host	IP address or name to map to Kerberos host realm.
kerberos_realm	IP address or name of Kerberos realm.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can map the name of the Kerberos realm to a DNS domain name or a host name by entering the **set kerberos realm** command. The information entered with this command is stored in a table with one entry for each Kerberos realm. The maximum number of entries in the table is 100.

You must enter Kerberos realms in uppercase characters.

Examples

This example shows how to map the Kerberos realm to a domain name:

```
Console> (enable) set kerberos realm CISCO CISCO.COM
Kerberos DnsDomain-Realm entry set to CISCO - CISCO.COM
Console> (enable)
```

Related Commands

clear kerberos realm
set kerberos local-realm
show kerberos

set kerberos server

To specify which Key Distribution Center (KDC) to use on the switch, use the **set kerberos server** command.

set kerberos server *kerberos_realm* {*hostname* | *ip_address*} [*port*]

Syntax Description

kerberos_realm	Name of the Kerberos realm.
hostname	Name of host running the KDC.
ip_address	IP address of host running the KDC.
port	(Optional) Number of the port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can specify to the switch which KDC to use in a Kerberos realm. Optionally, you can also specify the port number which the KDC is monitoring. The Kerberos server information you enter is maintained in a table with one entry for each Kerberos realm. The maximum number of entries in the table is 100.

The KDC is a Kerberos server and database program running on a network host that allocates the Kerberos credentials to different users or network services.

Examples

This example shows how to specify the Kerberos server:

```
Console> (enable) set kerberos server CISCO.COM 187.0.2.1 750
Kerberos Realm-Server-Port entry set to:CISCO.COM - 187.0.2.1 - 750
Console> (enable)
```

Related Commands

clear kerberos server
show kerberos

8.6 EFT Copy

set kerberos srvtab entry

To enter the SRVTAB file directly into the switch from the command line, use the **set kerberos srvtab entry** command.

set kerberos srvtab entry *kerberos_principal principal_type timestamp key_version_number key_type key_length encrypted_keytab*

Syntax Description

kerberos_principal	Service on the switch.
principal_type	Version of the Kerberos SRVTAB.
timestamp	Number representing the date and time the SRVTAB entry was created.
key_version_number	Version of the encrypted key format.
key_type	Type of encryption used.
key_length	Length, in bytes, of the encryption key.
encrypted_keytab	Secret key the switch shares with the KDC.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To make it possible for remote users to authenticate to the switch using Kerberos credentials, the switch must share a secret key with the KDC. To do this, you must give the switch a copy of the file that is stored in the KDC, which contains the secret key. These files are called SRVTAB files.

When you enter the SRVTAB directly into the switch, create an entry for each Kerberos principal (service) on the switch. The entries are maintained in the SRVTAB table. The maximum table size is 20 entries.

The KDC is a Kerberos server and database program running on a network host that allocates the Kerberos credentials to different users or network services.

The key is encrypted with the private 3DES key when you copy the configuration to a file or enter the **show config** command.

Examples

This example shows how to enter a SRVTAB file directly into the switch:

```
Console> (enable) set kerberos srvtab entry host/niners.cisco.com@CISCO.COM 0 932423923 1
1 8 03;;5>00>50;0=0=0
Kerberos SRVTAB entry set to
Principal:host/niners.cisco.com@CISCO.COM
Principal Type:0
Timestamp:932423923
Key version number:1
Key type:1
Key length:8
Encrypted key tab:03;;5>00>50;0=0=0
```

Related Commands

clear kerberos clients mandatory
show kerberos

set kerberos srvtab remote

To provide the switch with a copy of the SRVTAB file from the KDC that contains the secret key, use the **set kerberos srvtab remote** command.

set kerberos srvtab remote {*hostname* | *ip_address*} *filename*

Syntax Description

hostname	Name of host running the KDC.
ip_address	IP address of host running the KDC.
filename	Name of the SRVTAB file.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To make it possible for remote users to authenticate to the switch using Kerberos credentials, the switch must share a secret key with the KDC. To do this, you must give the switch a copy of the file that is stored in the KDC, which contains the secret key. These files are called SRVTAB files.

The KDC is a Kerberos server and database program running on a network host that allocates the Kerberos credentials to different users or network services.

The most secure method to copy SRVTAB files to the hosts in your Kerberos realm is to copy them onto physical media and go to each host in turn and manually copy the files onto the system. To copy SRVTAB files to the switch, which does not have a physical media drive, you must transfer them through the network using TFTP.

Examples

This example shows how to copy SRVTAB files to the switch remotely from the KDC:

```
Console> (enable) set kerberos srvtab remote 187.20.32.10 /users/jdoe/krb5/ninerskeytab
Console> (enable)
```

Related Commands

clear kerberos creds
set kerberos srvtab entry
show kerberos

8.6 EFT Copy

set key config-key

To define a private 3DES key, use the **set key config-key** command.

set key config-key *string*

Syntax Description

string	3DES key name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can define a private 3DES key for the switch. You can use the private 3DES key to encrypt the secret key that the switch shares with the KDC. If you set the 3DES key, the secret key is not displayed in clear text when you execute the **show kerberos** command. The key length should be eight characters or less.

Examples

This example shows how to define a 3DES key:

```
Console> (enable) set key config-key abcd
Kerberos config key set to abcd
Console> (enable)
```

Related Commands

clear key config-key

set l2protocol-tunnel cos

To apply a CoS value to all ingress tunneling ports, use the **set l2protocol-tunnel cos** command.

set l2protocol-tunnel cos *cos-value*

Syntax Description

cos-value	CoS value; valid values are 0 to 7.

Defaults

The default value for CoS is **5**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Because the CoS value applies to all ingress tunneling ports, all encapsulated PDUs sent out by the switch have the same CoS value.

Examples

This example shows how to set the CoS value to 6:

```
Console> (enable)  set l2protocol-tunnel cos 6
New CoS value is 6.
Console> (enable)
```

Related Commands

clear l2protocol-tunnel cos
clear l2protocol-tunnel statistics
set port l2protocol-tunnel
show l2protocol-tunnel statistics
show port l2protocol-tunnel

set l2protocol-tunnel trunk

To set Layer 2 protocol tunneling on trunks, use the **set l2protocol-tunnel trunk** command.

set l2protocol-tunnel trunk {**enable** | **disable**}

Syntax Description

enable	Enables Layer 2 protocol tunneling on trunks.
disable	Disables Layer 2 protocol tunneling on trunks.

Defaults

Layer 2 protocol tunneling on trunks is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Do not enable or disable Layer 2 protocol tunneling on trunks when active Layer 2 protocol tunnels are already configured. If you plan to configure Layer 2 protocol tunneling on trunks, do so before performing any other Layer 2 protocol tunneling tasks.

Examples

This example shows how to enable Layer 2 protocol tunneling on trunks:

```
Console> (enable) set l2protocol-tunnel trunk enable
Layer 2 Protocol Tunnel on trunks is allowed.
Console> (enable)
```

This example shows how to disable Layer 2 protocol tunneling on trunks:

```
Console> (enable) set l2protocol-tunnel trunk disable
Warning!! Clear any layer 2 protocol tunnel configuration on trunks
before using this command.
Layer 2 Protocol Tunnel on trunks is not allowed.
Console> (enable)
```

Related Commands

show l2protocol-tunnel statistics
show port l2protocol-tunnel

set lacp-channel system-priority

To set the priority of the system, use the **set lacp-channel system-priority** command.

set lacp-channel system-priority *value*

Syntax Description

value	Number of the priority; valid values are from 1 to 65535.

Defaults

The default system priority value is **32768**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

LACP is supported on all Ethernet interfaces.

The **set lacp-channel system-priority** command is a global command; however, the priority value is used only for the modules that are running LACP. The priority value is ignored on the modules that are running PAgP.

Higher value numbers correspond to lower priority levels.

For differences between PAgP and LACP, refer to the "Guidelines for Port Configuration" section of the "Configuring EtherChannel" chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Related Commands

clear lacp-channel statistics
set channelprotocol
set port lacp-channel
set spantree channelcost
set spantree channelvlancost
show lacp-channel
show port lacp-channel

set lcperroraction

To configure how your system handles Link Control Protocol (LCP) errors when a module reports an ASIC problem to the NMP, use the **set lcperroraction** command.

set lcperroraction *action*

Syntax Description

action	Action for handling LCP errors. See the "Usage Guidelines" section for more information about valid values for action levels.

Defaults

The default is that the action level is set to **ignore**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Valid values for action levels are as follows:

- **operator**—The system displays a recommended action for you to take. The system also logs the LCP error.
- **system**—The system automatically takes an action to handle the LCP error. The system also logs the LCP error.
- **ignore**—No action is taken. The system only logs the LCP error.

Note Be careful when using the **system** value because the switch automatically takes action, including possibly resetting or power cycling modules.

Examples

This example shows how to set the action that handles an LCP error:

```
Console> (enable) set lcperroraction ignore
Console> (enable)
```

Related Commands

show lcperroraction

set lda

To configure the ASLB information on the Catalyst 6500 series switch, use the **set lda** command.

set lda enable | disable

set lda vip {*server_virtual_ip*} {*destination_tcp_port*} [{*server_virtual_ip*} {*destination_tcp_port*}] ...

set lda mac ld {*ld_mac_address*}

set lda mac router {*mac_address*}...

set lda router {*router_vlan*} {*ld_mod/port*} [*backup_ld_mod/port*]

set lda server {*server_vlan*} {*ld_mod/port*} [*backup_ld_mod/port*]

set lda udpage {*udpagetime*}

Syntax Description

enable | disable	Enables or disables the ASLB feature.
vip *server_virtual_ip destination_tcp_port*	Specifies the virtual IP address of the server and the number of the destination TCP port that will be accelerated by the switch (up to 1024).
mac ld *ld_mac_address*	Specifies the LD MAC address.
mac router *mac_address...*	Specifies the router MAC address.
router *router_vlan*	Specifies the router VLAN.
ld_mod/port	Module and port number of the port connected to the LD on the VLAN.
backup_ld_mod/port	(Optional) Module and port number of the port connected to the backup LD.
server *server_vlan*	Specifies the server VLAN.
udpage *udpagetime*	Specifies the UDP aging time for LocalDirector acceleration.

Defaults

The default is the ASLB is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported only on switches configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card).

You can enter a zero (0) as a wildcard (don't care) digit for the *destination_tcp_port* value.

You can enter up to 1024 *server_virtual_ip destination_tcp_port* entries separated by a space.

To cancel a previously entered VIP, use the **clear lda** **vip** command.

To cancel a previously entered MAC LD or router, use the **clear lda** **mac** command.

You need to enter the **set lda** commands to provide all the necessary information before using the **commit lda** command to program the setup into hardware.

The information you enter through the **set lda** commands are immediately saved into NVRAM, but you must enter the **commit lda** command for the setting to take effect.

When you disable the ASLB feature, you can enter the **set lda** commands, but the **commit lda** command will fail.

When you enter the **set lda** **mac router** command, you can enter up to 32 MAC addresses.

You can enter the value zero (0) to disable the **udpage** option. The *udpagingtime* value is specified in milliseconds; values are from 0 milliseconds to 2024000 milliseconds.

Examples

This example shows how to enable the ASLB feature:

```
Console> (enable) set lda enable
Successfully enabled Local Director Acceleration.
Console> (enable)
```

This example shows how to disable the ASLB feature:

```
Console> (enable) set lda disable
Disabling Local Director Acceleration.....
Successfully disabled Local Director Acceleration.
Console> (enable)
```

This example shows how to specify the virtual IP address:

```
Console> (enable) set lda vip 10.0.0.8 8
Successfully set server virtual ip and port information.
Use commit lda command to save settings to hardware.
Console> (enable)
```

This example shows how to specify the MAC address for the LocalDirector:

```
Console> (enable) set lda mac ld 1-2-3-4-5-6
Successfully set mac address.
Use commit lda command to save settings to hardware.
Console> (enable)
```

This example shows how to specify multiple router MAC addresses:

```
Console> (enable) set lda mac router 1-2-3-4-5-6 3-4-56-67-4-5
Successfully set mac address.
Use commit lda command to save settings to hardware.
Console> (enable)
```

This example shows how to specify the router VLAN:

```
Console> (enable) set lda router 110 4/26
Successfully set router vlan and ld port.
Use commit lda command to save settings to hardware.
Console> (enable)
```

This example shows how to specify the udpage aging time:

```
Console> (enable) set lda udpage 20
Succesfully set LDA UDP aging time to 20ms.
Console> (enable)
```

This example shows how to specify the server VLAN:

```
Console> (enable) set lda server 105 4/40
Successfully set server vlan and LD port.
Use commit lda command to save settings to hardware.
Console> (enable)
```

Related Commands

clear lda
commit lda
show lda

set length

To configure the number of lines in the terminal display screen, use the **set length** command.

set length *number* [**default**]

Syntax Description

number	Number of lines to display on the screen; valid values are from 0 to 512.
default	(Optional) Sets the number of lines in the terminal display screen for the current administration session and all other sessions.

Defaults

The default value is 24 lines upon starting a session.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Output from a single command that overflows a single display screen is followed by the --More-- prompt. At the --More-- prompt, you can press **Ctrl-C**, **q**, or **Q** to interrupt the output and return to the prompt, press the **Spacebar** to display an additional screen of output, or press **Return** to display one more line of output.

Setting the screen length to 0 turns off the scrolling feature and causes the entire output to display at once. Unless you use the **default** keyword, a change to the terminal length value applies only to the current session.

When you change the value in a session, the value applies only to that session. When you use the **clear config** command, the number of lines in the terminal display screen is reset to the default of 100.

The **default** keyword is available in privileged mode only.

Examples

This example shows how to set the screen length to 60 lines:

```
Console> (enable) set length 60
Screen length for this session set to 60.
Console> (enable)
```

This example shows how to set the default screen length to 40 lines:

```
Console> (enable) set length 40 default
Screen length set to 40.
Console> (enable)
```

set localuser

To configure the switch to use local user authentication to authenticate access on the switch, use the **set localuser** command.

set localuser authentication {**enable** | **disable**}

set localuser user *username* [**password** *pwd*] [**privilege** *privilege_level*]

set localuser password [user *username*]

Syntax Description

authentication	Specifies local user authentication.
enable	Enables local user authentication.
disable	Disables local user authentication.
user *username*	Specifies a local user account.
password *pwd*	(Optional) Specifies a local user password.
privilege *privilege_level*	(Optional) Specifies a privilege level; valid values are 0 and 15.
password	Changes local user password.

Defaults

Local user authentication is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure a maximum of twenty-five local user accounts on each switch.

Before you can enable local user authentication, you must define at least one local user account.

A username must be fewer than sixty-five characters in length and can consist of only alphabetic and numeric characters. At least one of the characters in the username must be alphabetic.

The privilege level assigned to a username and password combination designates whether a user will be logged in to normal or privileged mode after successful authentication. A user with a privilege level of 0 is automatically logged in to normal mode, and a user with a privilege level of 15 is logged in to privileged mode. A user with a privilege level of 0 can still access privileged mode by entering the **enable** command and password combination.

Note If you are running a Cisco View image or are logging in using HTTP log in the initial authentication is done using the username and password combination. Privilege mode authentication can be done by either providing the privilege password or using the username and password combination, provided the local user has a privilege level of 15.

Examples

This example shows how to use the create a local user account, including password and privilege level:

```
Console> (enable) set localuser user picard password captain privilege 15
Added local user picard.
Console> (enable)
```

This example shows how to enable local user authentication:

```
Console> (enable) set localuser authentication enable
LocalUser authentication enabled
Console> (enable)
```

This example shows how to disable local user authentication:

```
Console> (enable) set localuser authentication disable
LocalUser authentication disabled
Console> (enable)
```

This example shows you how to reset your own password:

```
Console> (enable) set localuser password
Enter old password:*****
Enter new password:*******
Retype new password:*******
Password changed.

Console> (enable)
```

This example shows you, as an administrator, how to reset the password for a user:

```
Console> (enable) set localuser password picard
Enter new password:*******
Retype new password:*******
Password changed.
Console> (enable)
```

Related Commands

clear localuser
show localuser

set logging buffer

To limit the number of system logging messages buffered, use the **set logging buffer** command.

set logging buffer *buffer_size*

Syntax Description

buffer_size	Number of system logging messages to store in the buffer; valid values are 1 to 500.

Defaults

The default value is 500.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to limit the syslog message buffer to 400 messages:

```
Console> (enable) set logging buffer 400
System logging buffer size set to <400>.
Console> (enable)
```

Related Commands

clear logging buffer
set logging timestamp
show logging buffer

set logging callhome

To enable or disable the CallHome feature, use the **set logging callhome** command.

set logging callhome {**enable** | **disable**}

Syntax Description

enable	Enables CallHome functionality.
disable	Disables CallHome functionality.

Defaults

CallHome functionality is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you disable CallHome, only CallHome functionality is affected. To disable a specific parameter, you must clear each parameter individually.

Examples

This example shows how to enable the CallHome functionality:

```
Console> (enable) set logging callhome enable
Callhome functionality is enabled.
Callhome messages will be sent to the configured destination addresses.
Console> (enable)
```

This example shows how to disable the CallHome functionality:

```
Console> (enable) set logging callhome disable
Callhome functionality is disabled.
Callhome messages will not be sent to the configured destination addresses.
Console> (enable)
```

Related Commands

clear logging callhome
clear logging callhome from
clear logging callhome reply-to
clear logging callhome severity
clear logging callhome smtp-server
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome severity
set logging callhome smtp-server
show logging callhome
show logging callhome destination
show logging callhome from
show logging callhome reply-to
show logging callhome severity
show logging callhome smtp-server

set logging callhome destination

To set the CallHome destination address to receive the CallHome messages, fragment size, SNMP profile and SNMP index, use the **set logging callhome destination** command.

set logging callhome destination *E_addr* [**fragment** *size*] [**snmp-profile** *name*] [**snmp-index** *snmp-index*]

Syntax Description

E_addr	The e-mail or pager address to receive CallHome messages.
fragment *size*	(Optional) Sends CallHome messages as a series of fragmented messages; valid values are from 0 to 160 bytes.
snmp-profile *name*	(Optional) Specifies the SNMP profile name.
snmp-index *snmp-index*	(Optional) Specifies the SNMP profile index; valid values are from 1 to 65535.

Defaults

The default settings are as follows:

- **fragment** *size*—**0** (no fragmentation).
- **snmp-profile** *name*—_CLI_NAME0, _CLI_NAME1, _CLI_NAME2, _CLI_NAME3 for the first through the fourth **snmp-profile** *name* in the destination address table.
- **snmp-index** *snmp-index*—1, 2, 3, 4 for the first through the fourth **snmp-index** in the destination address table.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must enter this command for each destination address to receive syslog messages.

You can configure a maximum of four destination addresses.

The e-mail or pager address can be a maximum of 63 characters.

A **fragment** size of **0** specifies no fragmentation.

The SNMP profile and SNMP index are required for SNMP purposes only and do not need to be specified from the CLI.

Examples

This example shows how to set the following addresses to receive CallHome messages:

- page adminjoe@epage.cisco.com using a fragment size of 128 bytes
- e-mail adminboss@cisco.com, and adminjane@cisco.com

```
Console> (enable) set logging callhome destination adminjoe@epage.cisco fragment 128
Included adminjoe@epage.cisco in the table of callhome destination addresses.
Messages will be sent to this address in fragments of 128 bytes.
```

```
Console> (enable) set logging callhome destination adminjane@cisco.com
Included adminjane@cisco.com in the table of callhome destination addresses.
Messages will be sent to this address without fragmentation.
Console> (enable) set logging callhome destination adminboss@cisco.com
Included adminboss@cisco.com in the table of callhome destination addresses.
Messages will be sent to this address without fragmentation.
Console> (enable)
```

Related Commands

clear logging callhome
set logging callhome
set logging callhome from
set logging callhome reply-to
set logging callhome severity
set logging callhome smtp-server
show logging callhome
show logging callhome destination

set logging callhome from

To set the From e-mail address used by the CallHome feature, use the **set logging callhome from** command.

set logging callhome from *E_addr*

Syntax Description

E_addr	The e-mail or pager address from which the SMTP server sends failed syslog message delivery messages.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use the **set logging callhome from** command if you want notifications of failed delivery of syslog messages. If the SMTP server fails to deliver a syslog message for whatever reason, the address that you set here receives these notifications.

Examples

This example shows how to set the From address to adminjoe@cisco.com:

```
Console> (enable) set logging callhome from adminjoe@cisco.com
From address of callhome messages is set to adminjoe@cisco.com
Console> (enable)
```

Related Commands

clear logging callhome from
set logging callhome
set logging callhome destination
set logging callhome reply-to
set logging callhome severity
set logging callhome smtp-server
show logging callhome
show logging callhome from

set logging callhome reply-to

To set the Reply-to e-mail address, use the **set logging callhome reply-to** command.

set logging callhome reply-to *E_addr*

Syntax Description

E_addr	E-mail address sent with syslog messages that indicates the address to reply to, if different than the From address.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use the **set logging callhome reply-to** command if the recipient of the syslog message intends to reply to the received messages and if those replies must be sent to an address that is different from the address set by entering the **set logging callhome from** command. If you do not set the reply-to address, the switch uses the from address.

Examples

This example shows how to set the Reply-to address to adminjane@cisco.com:

```
Console> (enable) set logging callhome reply-to adminjane@cisco.com
Reply-To address of callhome messages is set to adminjane@cisco.com
Console> (enable)
```

Related Commands

clear logging callhome reply-to
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome smtp-server
show logging callhome
show logging callhome reply-to

set logging callhome severity

To specify the CallHome severity level of system messages to capture, use the **set logging callhome severity** command.

set logging callhome severity *level*

Syntax Description

level	Severity level of system messages to capture; severity level definitions are listed in Table 2-13.

Table 2-13 Severity Level Definitions

Severity Level	Description
0—emergencies	System unusable
1—alerts	Immediate action required
2—critical	Critical condition
3—errors	Error conditions
4—warnings	Warning conditions
5—notifications	Normal bug significant condition
6—informational	Informational messages
7—debugging	Debugging messages

Defaults

The default severity level is set to **2**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The CallHome feature is closely tied to syslog messages and their severity. When you set the CallHome severity level, carefully consider what level of severity you require for both the syslog messages and the CallHome messages.

For example, if you configure a very fine syslog severity level such as alerts (level 1), and a coarse CallHome severity level such as notifications (level 5), the destination addresses will only receive alerts and emergencies (levels 0 and 1) and not the remaining CallHome severity level notifications (levels 2, 3, and 4) you specified. To avoid this, set the CallHome severity level at the same severity level, or higher, that you set the syslog message severity.

Examples

This example shows how to set the severity to level 3:

```
Console> (enable) set logging callhome severity 3
Callhome severity level set to 3
Console> (enable)
```

Related Commands

clear logging callhome severity
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome smtp-server
show logging callhome
show logging callhome severity

set logging callhome smtp-server

To designate an IP address as an SMTP server used by the CallHome feature, use the **set logging callhome smtp-server** command.

set logging callhome smtp-server *IP_addr*

Syntax Description

IP_addr	IP address of the SMTP server.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must enter this command for each SMTP server.

You can configure a maximum of three SMTP servers.

Examples

This example shows how to SMTP server with the IP address 172.16.8.19:

```
Console> (enable) set logging callhome smtp-server 172.20.8.16
Included 172.20.8.16 in the table of callhome SMTP servers.
Console> (enable)
```

Related Commands

clear logging callhome smtp-server
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome severity
show logging callhome
show logging callhome smtp-server

set logging console

To enable and disable the sending of system logging messages to the console, use the **set logging console** command.

set logging console {**enable** | **disable**}

Syntax Description

enable	Enables system message logging to the console.
disable	Disables system message logging to the console.

Defaults

The default is system message logging to the console is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable system message logging to the console:

```
Console> (enable) set logging console enable
System logging messages will be sent to the console.
Console> (enable)
```

This example shows how to disable system message logging to the console:

```
Console> (enable) set logging console disable
System logging messages will not be sent to the console.
Console> (enable)
```

Related Commands

set logging level
set logging session
show logging
show logging buffer

set logging history

To set the number and severity level of syslog messages sent to the syslog history table, use the **set logging history** command.

set logging history *history_table_size*

set logging history severity *history_severity_level*

Syntax Description

history_table_size	Size of the syslog history table; valid values are from 0 to 500.
severity	Sets the syslog history severity level
history_severity_level	Severity level; valid values are from 0 to 7.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The Catalyst 6500 series switch holds syslog messages until the number of messages equals the defined size of the history log, after which the N messages are sent.

Examples

This example shows how to set the size of the syslog history table to 400:

```
Console> (enable) set logging history 400
System logging history table size set to <400>.
Console> (enable)
```

This example shows how to limit syslog messages that are sent to the history log based on severity level:

```
Console> (enable) set logging history severity 5
System logging history set to severity <5>
Console> (enable)
```

Related Commands

clear logging buffer
show logging

set logging level

To set the facility and severity level used when logging system messages, use the **set logging level** command.

set logging level *facility severity* [**default**]

Syntax Description

facility	Value to specify the type of system messages to capture; facility types are listed in Table 2-14.
severity	Value to specify the severity level of system messages to capture; severity level definitions are listed in Table 2-15.
default	(Optional) Causes the specified logging level to apply to all sessions.

Table 2-14 Facility Types

Facility Name	Definition
acl	access control list
all	All facilities
cdp	Cisco Discovery Protocol
cops	Common Open Policy Service Protocol
dtp	Dynamic Trunking Protocol
dvlan	Dynamic VLAN
earl	Enhanced Address Recognition Logic
filesys	file system facility
gvrp	GARP VLAN Registration Protocol
ip	Internet Protocol
kernel	Kernel
ld	ASLB facility
mcast	Multicast
mgmt	Management
mls	Multilayer Switching
pagp	Port Aggregation Protocol
privatevlan	Private VLAN facility
protfilt	Protocol Filter
pruning	VTP pruning
qos	Quality of Service
radius	Remote Access Dial-In User Service
rsvp	ReSerVation Protocol
security	Security
snmp	Simple Network Management Protocol

Table 2-14 Facility Types (continued)

Facility Name	Definition
spantree	Spanning Tree Protocol
sys	System
tac	Terminal Access Controller
tcp	Transmission Control Protocol
telnet	Terminal Emulation Protocol
tftp	Trivial File Transfer Protocol
udld	User Datagram Protocol
vmps	VLAN Membership Policy Server
vtp	Virtual Terminal Protocol

Table 2-15 Severity Level Definitions

Severity Level	Description
0—emergencies	System unusable
1—alerts	Immediate action required
2—critical	Critical condition
3—errors	Error conditions
4—warnings	Warning conditions
5—notifications	Normal bug significant condition
6—informational	Informational messages
7—debugging	Debugging messages

Defaults

The default is *facility* is set to **all**, and *level* is set to **0**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can also set the logging level by using the **set logging server** command.

If you do not use the **default** keyword, the specified logging level applies only to the current session.

Examples

This example shows how to set the default facility and severity level for system message logging:

```
Console> (enable) set logging level snmp 2 default
System logging facility <snmp> set to severity 2(critical).
Console> (enable)
```

Related Commands

clear logging level
show logging
show logging buffer

set logging server

To enable and disable system message logging to configured syslog servers and to add a syslog server to the system logging server table, use the **set logging server** command.

set logging server {**enable** | **disable**}

set logging server *ip_addr*

set logging server *facility severity*

set logging server severity *severity*

set logging server *facility*

Syntax Description

enable	Enables system message logging to configured syslog servers.
disable	Disables system message logging to configured syslog servers.
ip_addr	IP address of the syslog server to be added to the configuration.
facility	Type of system messages to capture; server facility types are listed in Table 2-16.
severity	Severity level; severity level definitions are listed in Table 2-15.
severity *severity*	Sets the syslog maximum severity control globally for all message types; severity level definitions are listed in Table 2-15.

Table 2-16 Server Facility Types

Severity Level	Description
local 0	Server facility local 0
local 1	Server facility local 1
local 2	Server facility local 2
local 3	Server facility local 3
local 4	Server facility local 4
local 5	Server facility local 5
local 6	Server facility local 6
local 7	Server facility local 7
syslog	syslog facility

Defaults

The default is no syslog servers are configured to receive system messages.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can also set the logging level by using the **set logging level** command. If you do not enter the facility or server keywords, the parameter is applied to all levels.

Severity logging to a configured syslog server depends on the configuration set by the **set logging level** command. The server severity level must be greater than or equal to the default severity level of the message facility that you expect to receive in syslog messages on the syslog server.

Examples

This example shows how to enable system message logging to the server:

```
Console> (enable) set logging server enable
System logging messages will be sent to the configured syslog servers.
Console> (enable)
```

This example shows how to disable system message logging to the server:

```
Console> (enable) set logging server disable
System logging messages will not be sent to the configured syslog servers.
Console> (enable)
```

This example shows how to add a server to the system logging server table using its IP address:

```
Console> (enable) set logging server 171.69.192.205
171.69.192.205 added to the System logging server table.
Console> (enable)
```

This example shows how to globally set the syslog maximum severity control for all message types:

```
Console> (enable) set logging server severity 4
System logging server severity set to 4(warnings).
Console> (enable)
```

Related Commands

clear logging server
show logging

set logging session

To enable or disable the sending of system logging messages to the current login session, use the **set logging session** command.

set logging session {**enable** | **disable**}

Syntax Description

enable	Enables the sending of system logging messages to the current login session.
disable	Disables the sending of system logging messages to the current login session.

Defaults

The default is system message logging to the current login session is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to prevent system logging messages from being sent to the current login session:

```
Console> (enable) set logging session disable
System logging messages will not be sent to the current login session.
Console> (enable)
```

This example shows how to cause system logging messages to be sent to the current login session:

```
Console> (enable) set logging session enable
System logging messages will be sent to the current login session.
Console> (enable)
```

Related Commands

set logging console
set logging level
show logging
show logging buffer

set logging telnet

To enable or disable logging on Telnet sessions, use the **set logging telnet** command.

set logging telnet {**enable** | **disable**}

Syntax Description

enable	Enables logging on Telnet sessions.
disable	Disables logging on Telnet sessions.

Defaults

The default is system message logging to the Telnet session is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to allow system logging messages to be sent to new Telnet sessions:

```
Console> (enable) set logging telnet enable
System logging messages will be sent to the new telnet sessions.
Console> (enable)
```

This example shows how to prevent system logging messages from being sent to new Telnet sessions:

```
Console> (enable) set logging telnet disable
System logging messages will not be sent to the new telnet sessions.
Console> (enable)
```

Related Commands

set logging console
set logging level
show logging
show logging buffer

set logging timestamp

To enable or disable the time-stamp display on system logging messages, use the **set logging timestamp** command.

set logging timestamp {**enable** | **disable**}

Syntax Description

enable	Enables the time-stamp display.
disable	Disables the time-stamp display.

Defaults

By default, system message logging time-stamp is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable the time-stamp display:

```
Console> (enable) set logging timestamp enable
System logging messages timestamp will be enabled.
Console> (enable)
```

This example shows how to disable the time-stamp display:

```
Console> (enable) set logging timestamp disable
System logging messages timestamp will be disabled.
Console> (enable)
```

Related Commands

show logging

set logout

To set the number of minutes until the system disconnects an idle session automatically, use the **set logout** command.

set logout *timeout*

Syntax Description

timeout	Number of minutes until the system disconnects an idle session automatically; valid values are from 0 to 10,000 minutes.

Defaults

The default is 20 minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Setting the value to 0 disables the automatic disconnection of idle sessions.

The **show tech-support** command may time out if the configuration file output takes longer to display than the configured session timeout time. If this happens, enter a **set logout** *timeout* value of 0 to disable automatic disconnection of idle sessions or enter a longer *timeout* value.

Examples

This example shows how to set the number of minutes until the system disconnects an idle session automatically:

```
Console> (enable) set logout 20
Sessions will be automatically logged out after 20 minutes of idle time.
Console> (enable)
```

This example shows how to disable the automatic disconnection of idle sessions:

```
Console> (enable) set logout 0
Sessions will not be automatically logged out.
Console> (enable)
```

Related Commands

show tech-support

set mac-auth-bypass

To configure the parameters for the MAC authentication bypass feature, use the **set mac-auth-bypass** command.

set mac-auth-bypass {**enable** | **disable**}

set mac-auth-bypass {**auth-fail-timeout** *seconds* | **reauth-timeout** *seconds* | **shutdown-timeout** *seconds*}

set mac-auth-bypass {**reauthentication** | **radius-accounting**} {**enable** | **disable**}

set mac-auth-bypass violation {**restrict** | **shutdown**}

Syntax Description

enable	Globally enables the MAC authentication bypass feature.
disable	Globally disables the MAC authentication bypass feature.
auth-fail-timeout *seconds*	Sets the amount of time that a port waits in authentication failure (AuthFail) state before attempting authentication again; valid values are from 5 to 65535 seconds.
reauth-timeout *seconds*	Sets the time after which reauthentication is triggered if global authentication is enabled; valid values are from 300 to 65535 seconds.
shutdown-timeout *seconds*	Sets the time after which a port is automatically enabled after it was shut down because of a security violation; valid values are from 0 to 65535.
reauthentication	Sets global reauthentication mode.
radius-accounting	Sets RADIUS accounting.
enable	Enables reauthentication or RADIUS accounting.
disable	Disables reauthentication or RADIUS accounting.
violation	Sets how the switch responds to a security violation event.
restrict	Adds the MAC address that is causing the security violation to a trap entry in the forwarding table.
shutdown	Shuts down the port.

Defaults

The **auth-fail-timeout** time is 60 seconds.

The **reauth-timeout** time is 3600 seconds.

The **shutdown-timeout** time is 60 seconds.

Reauthentication is disabled.

RADIUS accounting is disabled.

The violation mode is **shutdown**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you specify a shutdown timeout period of 0 seconds, the automatic port-enable function is disabled and you will need to manually reenable the ports.

Examples

This example shows how to specify the shutdown timeout period:

```
Console> (enable) set mac-auth-bypass shutdown-timeout 40
Shutdown Timeout set to 40 seconds.
Console> (enable)
```

This example shows how to specify the AuthFail timeout period:

```
Console> (enable) set mac-auth-bypass auth-fail-timeout 60
Authfail Timeout set to 60 seconds.
Console> (enable)
```

This example shows how to specify the reauthentication timeout period:

```
Console> (enable) set mac-auth-bypass reauth-timeout 400
Reauth Timeout set to 400 seconds.
Console> (enable)
```

This example shows how to globally enable MAC address authentication bypass reauthentication:

```
Console> (enable) set mac-auth-bypass reauthentication enable
Global reauthentication mode enabled.
Console> (enable)
```

This example shows how to specify the “restricted” option in the event of a security violation:

```
Console> (enable) set mac-auth-bypass violation restrict
Mac-Auth-Bypass security violation mode set to restrict.
Console> (enable
```

Related Commands

set port mac-auth-bypass
show mac-auth-bypass
show port mac-auth-bypass

set macro

To create user-defined SmartPorts macros, use the **set macro** command.

set macro name *macro_name*

set macro variable *variable_name variable_value* [*mod/port*]

Syntax Description

name	Creates a user-defined SmartPorts template.
macro_name	Name of the macro. See the "Usages Guidelines" section for more information about macro names.
variable	Defines a user-defined SmartPorts macro variable.
variable_name	Name of the variable. See the "Usage Guidelines" section for more information about macro variables.
variable_value	Value of the variable.
mod/port	(Optional) Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The maximum length of a macro name is 16 characters. The maximum number of command lines in a macro is 64. A user-defined macro cannot have the same name as a static macro.

You can have a macro inside a macro in user-defined and static macros.

If you attempt to apply a macro on a port and the macro has some valid and some invalid commands in its definition, the macro is still applied on the port and an appropriate error message is displayed when the invalid command is executed. This does not affect the definition of the macro.

To modify an existing user-defined macro, use the **set macro name** *macro_name* command. When modifying a macro, the new definition replaces the old definition, but the new definition is not automatically applied to all the ports on which it was previously applied. You need to explicitly apply the modified macro.

When you apply a macro, a record of the macro being applied is not stored in the configuration file or NVRAM. However, for each port there is a record of the latest macro that was applied to it.

Once a macro is applied to a port, you cannot clear the macro. However, one way to cancel a macro on a port is to define another macro that clears the configurations on the port, and then apply the newly created macro on the port.

You can define a variable on a per-port basis or a global basis. When a macro is applied to a port, the variables are replaced with the values that you have defined. The maximum length of a variable name is 16 characters. A macro definition can use multiple variables in a single line. Per-port variables are defined on a per-port basis. Individual ports can be configured with different values by defining variables with different values for different ports. Global variables are such that if a variable definition does not have port information, then it is treated as a global variable. The global variable definition is used if the per-port variable is not defined.

A macro could have a variable that is not predefined, in which case the variable would get its value when the macro is applied. MODPORT is one such variable. For example, if a macro has the variable MODPORT in its definition, when the macro is applied on a module/port, the variable MODPORT is replaced by the module/port (*mod/port*) on which the macro is applied.

Note MODPORT is currently the only special variable supported.

If you attempt to apply a macro on a port and the macro has a variable that is not defined in its definition, the macro is not applied on the port and an appropriate error message is displayed. This does not affect the definition of the macro.

You can have a macro within a macro definition. When the root macro is applied to a port, the macro inside the root macro gets replaced by its definition and the root macro is applied to the port. You can also have a static macro (such as ciscoswitch or ciscorouter) inside a user-defined macro definition.

Enter the **set port macro** *mod/num macro_name* command to apply the user-defined macro.

For more information about SmartPorts macros, see the "Configuring a VoIP Network" chapter of the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows you how to create a SmartPorts macro. Note that after you enter **set macro name** *macro_name*, you are prompted to list all the commands that are contained in the macro. Enter @ at the end of the list of commands.

```
Console> (enable) set macro name videophone
Enter macro commands one per line. End with character ‘@’.
set port enable #MODPORT
set vlan $DATAVLAN #MODPORT
set port auxiliaryvlan #MODPORT $AUXVLAN
set qos autoqos
@
Console> (enable)
```

This example shows the message that appears on the console when you change the command list in a macro that already exists:

```
Console> (enable) set macro name fileserver
Enter macro commands one per line. End with the character '@'.
<cmd2>
<cmd3>
@
Warning: The macro fileserver has been modified; Do you want to modify (y/n)y
Console> (enable)
```

This example shows how to define a variable:

```
Console> (enable) set macro variable $DATAVLAN 3 3/2

Variable DATAVLAN successfully created
Console> (enable) set macro variable $DATAVLAN 5 3/3
Console> (enable) set macro variable $AUXVLAN 4 3/2

Variable AUXVLAN successfully created
Console> (enable)
```

If a port is not specified in the variable definition, the variable is considered a global variable.

```
Console> (enable) set macro variable $CDPVER v2

Variable CDPVER successfully created
Console> (enable)
```

Related Commands

clear macro
set port macro
show macro

set macro ciscosmartports

To set the global Cisco SmartPorts template, use the **set macro ciscosmartports** command.

set macro ciscosmartports

Syntax Description

This command has no keywords or arguments

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enter the **set macro ciscosmartports** global macro command, the following configuration is displayed:

```
set macro ciscosmartports
----------------------------------------------------
set udld enable
set errdisable-timeout enable udld
set errdisable-timeout enable duplex-mismatch
set errdisable-timeout enable channel-misconfig
set errdisable-timeout enable bpdu-guard
set errdisable-timeout interval 60
set cdp enable
set cdp version v2
set spantree mode rapid-pvst+
set spantree macreduction enable
set spantree portfast bpdu-guard enable
set spantree global-default loop-guard enable
set qos autoqos
```

Examples

This example shows how to enable the Cisco SmartPorts global macro:

```
Console> (enable) set macro ciscosmartports
Console> (enable)
```

Related Commands

set port macro

set mls agingtime

To specify the MLS aging time of shortcuts to an MLS entry in the Catalyst 6500 series switches, use the **set mls agingtime** command.

set mls agingtime ip *agingtime*

set mls agingtime fast {*fastagingtime*} {*pkt_threshold*}

set mls agingtime long-duration {*longagingtime*}

Syntax Description

ip	Specifies IP MLS.
agingtime	MLS aging time of shortcuts to an MLS entry; valid values are from 1 to 1920 seconds.
fast	Specifies the MLS aging time of shortcuts to an MLS entry that has no more than *pkt_threshold* packets switched within *fastagingtime* seconds after it is created.
fastagingtime	MLS aging time of shortcuts to an MLS entry; valid values are from 0 to 128 seconds.
pkt_threshold	Packet threshold value; valid values are from 0 to 127 packets.
long-duration	Sets the aging time for active flows.
longagingtime	MLS aging time of shortcuts to an MLS entry; valid values are 0 (to disable) and 8 to 1920 seconds.

Defaults

- The default IP *agingtime* is 16 seconds.
- The default *fastagingtime* is 0, no fast aging.
- The default *pkt_threshold* is 0.
- The default *longagingtime* is 320.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use the **ip** keyword, you are specifying a shortcut for IP MLS.

If you enter **0** for the *fastagingtime* value, fast aging is disabled.

If you do not specify *fastagingtime* or *pkt_threshold*, the default value is used.

If you enter any of the **set mls** commands on a Catalyst 6500 series switch without MLS, this warning message displays:

```
MLS not supported on feature card.
```

The *fastagingtime* value can be configured in the range of 0 to 128 seconds.

The default *pkt_threshold* value is 0. If you do not configure *fastagingtime* exactly the same for these values, it adjusts to the closest value. A typical value for *fastagingtime* and *pkt_threshold* is 32 seconds and 0 packet, respectively. (It means no packet switched within 32 seconds after the entry was created.)

The *agingtime* value applies to an MLS entry that has no more than *pkt_threshold* packets switched within *fastagingtime* seconds after it is created. A typical example is the MLS entry destined to or sourced from a DNS or TFTP server. This entry may never be used again once it is created. For example, only one request goes to a server and one reply returns from the server, and then the connection is closed.

The **agingtime fast** option is used to purge entries associated with very short flows, such as DNS and TFTP.

Keep the number of MLS entries in the MLS cache below 32,000. If the number of MLS entries exceed 32,000, some flows (less than 1 percent) are sent to the router.

To keep the number of MLS cache entries below 32,000, decrease the aging time up to 8 seconds. If your switch has a lot of short flows used by only a few packets, then you can use fast aging.

If cache entries continue to exceed 32,000, decrease the normal aging time in 64-second increments from the 256-second default.

You can force an active flow to age out by entering the **set mls agingtime long-duration** command. You can specify the aging time of the active flow in the range of 64 to 1920 seconds in increments of 64.

Examples

These examples show how to set the aging time:

```
Console> (enable) set mls agingtime 512
IP Multilayer switching aging time set to 512 seconds.
Console> (enable)
```

This example shows how to set the fast aging time:

```
Console> (enable) set mls agingtime fast 32 0
Multilayer switching fast aging time set to 32 seconds for entries with no more than 0
packet switched.
Console> (enable)
```

This example shows how to set the aging time for active flows:

```
Console> (enable) set mls agingtime long-duration 128
Multilayer switching agingtime set to 128 seconds for long duration flows
Console> (enable)
```

Related Commands

clear mls statistics entry
show mls

set mls bridged-flow-statistics

To enable or disable statistics for bridged flows for specified VLANs, use the **set mls bridged-flow-statistics** command.

set mls bridged-flow-statistics {**enable** | **disable**} {*vlanlist*}

Syntax Description

enable	Enables statistics for bridged flows.
disable	Disables statistics for bridged flows.
vlanlist	Number of the VLAN or VLANs; valid values are 1 to 4094. See the "Usage Guidelines" section for more information.

Defaults

By default, bridged-flow statistics is disabled on all VLANs.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can enter one or multiple VLANs. The following examples are valid VLAN lists: 1; 1,2,3; 1-3,7.

Bridged flows are exported through NDE when bridged flow statistics is enabled.

Examples

This example shows how to enable bridged-flow statistics on the specified VLANs:

```
Console> (enable) set mls bridged-flow-statistics enable 1-21
Netflow statistics is enabled for bridged packets on vlan(s) 1-21.
Console> (enable)
```

Related Commands

show mls nde
show mls entry
show mls statistics

set mls cef load-balance

To include or exclude Layer 4 ports in a load-balancing hash, use the **set mls cef load-balance** command.

set mls cef load-balance {**full** | **source-destination-ip**}

Syntax Description

full	Bases the hash on Layer 4 ports and source and destination IP addresses.
source-destination-ip	Bases the hash on source and destination IP addresses.

Defaults

By default, the load-balancing hash is based on source and destination IP addresses.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When multiple paths are available to reach a destination, the new hash is used to choose the path to be used for forwarding.

Examples

This example shows how to base the hash on Layer 4 ports and source and destination IP addresses:

```
Console> (enable) set mls cef load-balance full
Console> (enable)
```

This example shows how to base the hash on source and destination IP addresses:

```
Console> (enable) set mls cef load-balance source-destination-ip
Console> (enable)
```

Related Commands

show mls

set mls cef maximum-routes

To set the maximum number of routes that can be programmed in the FIB TCAM for a protocol, use the **set mls cef maximum-routes** command.

set mls cef maximum-routes {**ip** | **ip-multicast**} *routes*

Syntax Description

ip	Specifies IP MLS.
ip-multicast	Specifies IP multicasting MLS.
routes	Number of routes that can be programmed in the FIB TCAM.

Defaults

The *routes* argument is 0, which means that the system-determined bootup default is used:

- IP version 4 unicast—192,000.
- IP version 4 multicast—32,000.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is only available on the Supervisor Engine 720.

Routes that exceed the specified number of routes are not installed in the hardware. Packets that take those routes are switched by MSFC. The *routes* argument is a unit of 1,000 entries. Setting the *routes* argument to 0 returns the system to a system-determined default value.

When no protocols are set, an initial default value is assigned for each protocol. When at least one protocol is set, the default value for other unassigned protocols might change as the system tries to assign the remaining space to the unassigned protocols.

This command has the following characteristics:

- Changing the setting takes effect only after rebooting the active supervisor engine. The change does not take effect after a switchover.
- The setting on the standby supervisor engine is synchronized with the active supervisor engine. If the standby supervisor is inserted, both the bootup setting and new setting, if existing, on the active supervisor engine are synchronized with the standby supervisor engine. The standby supervisor engine uses the bootup setting to configure the FIB TCAM. The standby supervisor engine might need to be reset if its original bootup setting is different from the bootup setting of the active supervisor engine. An informational message (FIB_MAXROUTES_RESET) is printed on the active supervisor engine console if this situation occurs.
- To maximize the TCAM utilization, we recommend that you set the maximum routes for IP unicast as a multiple of 16,000 and set the maximum routes for IP multicast as a multiple of 8,000. The internal allocation scheme uses 16,000 as the allocation unit for unicast and 8,000 as the allocation unit for multicast. For example, if IP unicast is set to 1,000, 16,000 entries are reserved, but only 1,000 is allowed.

- When the maximum routes is exceeded or the allocated TCAM space for a protocol is full, a system message (FIB_ALLOC_TCAM_FULL) displays. Note that because of the internal software allocation scheme, the allocated TCAM space might be full before the maximum routes is exceeded.

Note The sum of the number of maximum routes for all protocols cannot exceed 256,000.

Note If the *routes* values for all protocols are set to 0, the bootup default is used. When you set the *routes* value for one protocol to a non-zero value, the default value for the other protocol changes to the remaining size.

Examples

This example shows how to set the maximum number of routes for IP unicast:

```
Console> (enable) set mls cef maximum-routes ip 220
Configuration change will take effect after next reboot.
Console> (enable)
```

Related Commands

show mls cef maximum-routes

set mls cef per-prefix-statistics

To set MLS CEF per-prefix statistics mode, use the **set mls cef per-prefix statistics** command.

set mls cef per-prefix statistics {**enable** | **disable**}

Syntax Description

enable	Enables per-prefix statistics for all FIB entries
disable	Disables per-prefix statistics for all FIB entries.

Defaults

MLS CEF per-prefix statistics mode is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When the **set mls cef per-prefix-statistics** command is enabled, the switch makes a best effort to allocate adjacencies with statistics for each prefix. Statistics for a prefix are computed by adding up the packet/byte counts of all the adjacencies that are associated with the prefix. Because only half of the adjacency table entries have statistics, all prefixes might not be associated with adjacencies that have statistics.

Examples

This example shows how to enable per-prefix statistics for all FIB entries:

```
Console> (enable) set mls cef per-prefix-stats enable
Per prefix stats is enabled
Console> (enable)
```

This example shows how to disable per-prefix statistics for all FIB entries:

```
Console> (enable) set mls cef per-prefix-stats disable
Per prefix stats is disabled
Console> (enable)
```

Related Commands

show mls

set mls exclude protocol

To exclude an MLS protocol port on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC, use the **set mls exclude protocol** command. To exclude protocols from statistics gathering on switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2), use the **set mls exclude protocol** command.

set mls exclude protocol {**tcp** | **udp** | **both**} {*port_number* | *port_name*}

Syntax Description

tcp | **udp** | **both**	Specifies a TCP, UDP port, or that the port be applied to both TCP and UDP traffic.
port_number	Number of the protocol port; valid values are from 1 to 65535.
port_name	Name of the port; valid values are **dns**, **ftp**, **smtp**, **telnet**, **x**, **www**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter any of the **set mls** commands on a Catalyst 6500 series switch without MLS, this warning message is displayed:

```
MLS not supported on feature card.
```

You can add a maximum of four protocol ports to the exclude table.

MLS exclusion is supported in full flow mode only.

If you enter **x** for the port name, this specifies the Layer 4 port used by the X-windows application.

Examples

This example shows how to exclude TCP packets on protocol port 6017:

```
Console> (enable) set mls exclude protocol tcp 6017
TCP packets with protocol port 6017 will be switched by RP.
Console> (enable)
```

This example shows how to exclude UDP packets on protocol port 6017:

```
Console> (enable) set mls exclude protocol udp 6017
TCP and UDP packets with protocol port 6017 will be switched by RP.
Console> (enable)
```

Related Commands

show mls

set mls flow

To specify the minimum flow mask used for MLS, use the **set mls flow** command. This command is needed to collect statistics for the supervisor engine.

set mls flow {**destination** | **destination-source** | **full** | **null**}

Caution

Use this command carefully. This command *purges all existing shortcuts* and affects the number of active shortcuts. This command can increase the cache usage and increase the load on the router.

Caution

Be extremely careful if you enter this command on a switch that already has a large number of shortcuts (greater than 16,000).

Caution

Do not place this command in scripts that are frequently executed—changing the MLS flow mask purges all MLS cache entries.

Syntax Description

destination	Sets the minimum flow mask to destination flow.
destination-source	Sets the minimum flow mask to source flow.
full	Sets the minimum flow mask to an extended access list.
null	Clears the flow mask.

Defaults

In software release 8.5(1) and subsequent releases, **null** is the default action.

Before software release 8.5(1), if there are no access lists on any MLS-RP, the flow mask is set to **destination** flow.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command specifies the minimum MLS flow mask. Depending on the MLS-RP configuration, the actual flow mask used might be more specific than the specified minimum flow mask. For example, if you configure the minimum flow mask to **destination-source**, but an MLS-RP interface is configured with IP extended access lists, the actual flow mask used will be **full**.

If you configure a more specific flow mask (for example, **destination-source** or **full**), the number of active flow entries increases. To limit the number of active flow entries, you might need to decrease the MLS aging time.

This command is intended to be used for gathering very detailed statistics at the protocol port level—for example, when NetFlow data is exported to an RMON2 probe.

In software release 8.5(1) and subsequent releases, multiple flow masks are supported on the Supervisor Engine 720. Various RP features, such as NAT in the hardware, are also supported. Because of flow mask resolution requirements in NDE and NAT, if the NDE flow mask has been configured and you need to use NAT, the NDE flow mask must be cleared. To clear the flow mask, use the **null** keyword.

When the flow mask is set to **null** and no feature is driving a more specific flow mask, all the netflows will match the same null flow. The counters for that flow are incremented each time another flow hits it. When the flow mask is set to **null** and you enter the **show mls stat entry** command, the command output will show information about this null flow.

If NDE is enabled when the **null** option is configured, NDE will not export any flows.

If you uprade the software from software release 8.4 to release 8.5, the NVRAM configuration is preserved. You will not encounter issues during an upgrade from previous images to 8.5(1) or subsequent releases if the switch configuration mode is set to binary. In text configuration mode, if you had entered the **destination** keyword, then you must set the flow mask again after upgrade.

Examples

These examples show how to specify that only expired flows to subnet 171.69.194.0 are exported:

```
Console> (enable) set mls flow destination
Configured flow mask is set to destination flow.
Console> (enable)

Console> (enable) set mls flow destination-source
Configured flow mask is set to destination-source flow.
Console> (enable)

Console> (enable) set mls flow full
Configured flow mask is set to full flow.
Console> (enable)
```

Related Commands

show config mode
show mls
show mls flowmask

set mls nde

To configure the NetFlow Data Export (NDE) feature in the Catalyst 6500 series switches to allow command-exporting statistics to be sent to the preconfigured collector, use the **set mls nde** command.

set mls nde {**enable** | **disable**}

set mls nde {*collector_ip* | *collector_name*} {*udp_port_num*}

set mls nde version {**1** | **5** | **7** | **8**}

set mls nde flow [**exclude** | **include**] [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*]

set mls nde {**destination-ifindex** | **source-ifindex**} {**enable** | **disable**}

Syntax Description

enable	Enables NDE.
disable	Disables NDE.
collector_ip	IP address of the collector if DNS is enabled.
collector_name	Name of the collector if DNS is enabled.
udp_port_num	Number of the UDP port to receive the exported statistics.
version	Specifies the version of the NDE; valid versions are **1**, **5**, **7**, and **8**.
1 | **5** | **7** | **8**	Version of the NDE feature.
flow	Adds filtering to NDE.
exclude	(Optional) Allows exporting of all flows except the flows matching the given filter.
include	(Optional) Allows exporting of all flows matching the given filter.
destination	(Optional) Specifies the destination IP address.
ip_addr_spec	(Optional) Full IP address or a subnet address in these formats: *ip_addr*, *ip_addr/netmask*, or *ip_addr/maskbit.*
source	(Optional) Specifies the source IP address.
protocol	(Optional) Specifies the protocol type.
protocol	(Optional) Protocol type; valid values can be a number from 0 to 255 or **ip**, **ipinip**, **icmp**, **igmp**, **tcp**, or **udp**. **0** indicates “do not care.”
src-port *src_port*	(Optional) Specifies the number of the TCP/UDP source port (decimal). Used with **dst-port** to specify the port pair if the **protocol** is **tcp** or **udp**. **0** indicates “do not care.”
dst-port *dst_port*	(Optional) Specifies the number of the TCP/UDP destination port (decimal). Used with **src-port** to specify the port pair if the **protocol** is **tcp** or **udp**. **0** indicates “do not care.”
destination-ifindex	Specifies destination ifIndex support.
source-ifindex	Specifies source ifIndex support.
enable	Enables ifIndex support.
disable	Disables ifIndex support.

Defaults

The defaults are Netflow Data Export version 7, and all expired flows are exported until the filter is specified explicitly. Destination ifIndex support and source ifIndex support are enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter any **set mls nde** commands on a Catalyst 6500 series switch without MLS, this warning message is displayed:

```
mls not supported on feature card.
```

When you try to enable NDE and there are previously configured filtered flows on the switch, this warning message is displayed:

```
Console> (enable) set mls nde enable
Netflow export configured for port 80 on host 172.20.25.101
Netflow export enabled.
Warning!! There is a potential statistics mismatch due to existing excluded
protocols.
```

When you try to add a filter to exclude some protocol packets and NDE is currently enabled, this warning message is displayed:

```
Console> (enable) set mls nde flow exclude protocol tcp 80
Netflow tables will not create entries for TCP packets with protocol port 80.
Warning!! There's a potential statistics mismatch due to enabled NDE.
```

Before you use the **set mls nde** command for the first time, you must configure the host to collect MLS statistics. The host name and UDP port number are saved in NVRAM, so you do not need to specify them. If you specify a host name and UDP port, values in NVRAM overwrite the old values. Collector values in NVRAM do not clear when NDE is disabled because this command configures the collector but does not enable NDE automatically.

The **set mls nde enable** command enables NDE, exporting statistics to the preconfigured collector.

If the *protocol* is not **tcp** or **udp**, set the **dst-port** *dst_port* and **src-port** *src_port* values to 0; otherwise, no flows are displayed.

If you try to enable NDE without first specifying a collector, you see this display:

```
Console> (enable) set mls nde enable
Please set host name and UDP port number with 'set mls nde <collector_name | collector_ip>
<udp_port_number>'.
Console> (enable)
```

The **set mls nde flow** command adds filtering to the NDE. Expired flows matching the specified criteria are exported. These values are stored in NVRAM and do not clear when NDE is disabled. If any option is not specified in this command, it is treated as a wildcard. The NDE filter in NVRAM does not clear when NDE is disabled.

In software releases before 8.3(1), only one filter can be active at a time. If you do not enter the **exclude** or **include** keyword, the filter is assumed to be an inclusion filter.

In software release 8.3(1) and later releases, the dual destination feature allows NetFlow export data to be sent to two destinations simultaneously. With this enhancement, you can set up two unique collectors. The same NetFlow data is exported to both the destinations. However, the count of the packets to the two collectors may differ depending on the time the two destinations were created. The count of the packets sent to the individual collectors is maintained separately. Apart from the count, the other NetFlow parameters for both the destinations are the same.

NDE cannot be enabled unless a collector is set up. Both the primary and secondary destinations should be set up before enabling NDE. The secondary destination IP address and port number cannot be equal to the primary destination IP address and port number.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the short subnet address format. The trailing decimal number 00 in an IP address YY.YY.YY.00 specifies the boundary for an IP subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 173.24.00.00/255.255.0.0). However, this format can identify only a subnet address of 8, 16, or 24 bits.
- *ip_addr/subnet_mask*—This is the long subnet address format. For example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip_addr* is a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip_addr* is a full host address, such as 193.22.253.1/22, which has the same subnet address as the *ip_subnet_addr*.

When you use the **set mls nde** {*collector_ip* | *collector_name*} {*udp_port_num*} command, the host name and UDP port number are saved in NVRAM and need not be specified again. If you specify a host name and UDP port, the new values overwrite the values in NVRAM. Collector values in NVRAM do not clear when you disable NDE.

If NDE is enabled when you set the MLS flow mask to null by entering the **set mls flow null** command, NDE will not export any flows.

Examples

This example shows how to set the NDE version to 5:

```
Console> (enable) set mls nde version 5
Multilayer switching netflow data export version set to 5
Console> (enable)
```

This example shows how to specify that only expired flows to a specific subnet are exported:

```
Console> (enable) set mls nde flow include destination 171.69.194.140/24
NDE destination filter set to 171.69.194.0/24
Console> (enable)
```

This example shows how to specify that only expired flows to a specific host are exported:

```
Console> (enable) set mls nde flow include destination 171.69.194.140
NDE destination filter set to 171.69.194.140/32.
Console> (enable)
```

This example shows how to specify that only expired flows from a specific subnet to a specific host are exported:

```
Console> (enable) set mls nde flow include destination 171.69.194.140/24 source
171.69.173.5/24
```

```
NDE destination filter set to 171.69.194.0/24, source filter set to 171.69.173.0/24
Console> (enable)
```

This example shows how to specify that only flows from a specific port are exported:

```
Console> (enable) set mls nde flow include dst_port 23
NDE source port filter set to 23.
Console> (enable)
```

This example shows how to specify that only expired flows from a specific host that are of a specified protocol are exported:

```
Console> (enable) set mls nde flow include source 171.69.194.140 protocol 51
NDE destination filter set to 171.69.194.140/32, protocol set to 51.
Console> (enable)
```

This example shows how to specify that all expired flows except those from a specific host to a specific destination port are exported:

```
Console> (enable) set mls nde flow exclude source 171.69.194.140 dst_port 23
NDE destination filter set to 171.69.194.140/32, source port filter set to 23.
Flows matching the filter will be excluded.
Console> (enable)
```

This example shows how to disable destination ifIndex support:

```
Console> (enable) set mls nde destination-ifindex disable
destination-index export has been disabled.
Console> (enable)
```

This example shows how to disable source ifIndex support:

```
Console> (enable) set mls nde source-ifindex disable
source-index export has been disabled.
Console> (enable)
```

This example shows how to specify an NDE collector when no other collectors have been configured:

```
Console> (enable) set mls nde 10.6.1.10 7772
Number of collectors configured is 1
Netflow export configured for port 7772 on host 10.6.1.10
Netflow export is not enabled. Please enable it now.
Console> (enable)
```

This example shows how to specify an NDE collector when one collector has already been configured:

```
Console> (enable) set mls nde 10.6.1.10 7775
Number of collectors configured is 2
Netflow export configured for port 7775 on host 10.6.1.10
Netflow export is not enabled. Please enable it now.
Console> (enable)
```

This example shows the message that displays if a collector with the same IP address and port already exists:

```
Console> (enable) set mls nde 10.6.1.10 7772
Collector Exists with same IP address and port Number
Failed to set Netflow Data Export
Console> (enable)
```

This example shows the message that displays when two collectors have already been configured:

```
Console> (enable) set mls nde 10.6.1.10 7777
Collector Not set up
A maximum of 2 collectors allowed
Please clear an exiting Collector first
```

```
Failed to set Netflow Data Collector.
Console> (enable)
```

Related Commands

clear mls nde flow
show mls
show mls nde

set mls netflow-entry-create

To specify the VLANs on which you can enable or disable the creation of NetFlow entries, use the **set mls netflow-entry-create** command.

set mls netflow-entry-create {**enable** | **disable**} *vlan_list*

Syntax Description

enable	Specifies that NetFlow entry creation can be enabled on the specified VLANs.
disable	Specifies that NetFlow entry creation cannot be enabled on the specified VLANs.
vlan_list	VLAN numbers; valid values are from 1 to 4094.

Defaults

This command is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The status of the creation of NetFlow entries on specific VLANs (whether this feature is enabled or disabled) is displayed as part of the **show mls** command output. The VLANs that have entry creation enabled are displayed as part of the VLANs that have the bridged flow statistics feature enabled.

NetFlow entries on the specified VLANs are not created until you enter the **set mls netflow-per-interface enable** command.

Related Commands

set mls netflow-per-interface
show mls

set mls netflow-per-interface

To enable or disable the creation of NetFlow entries on a per-VLAN basis, use the **set mls netflow-per-interface** command.

set mls netflow-per-interface {**enable** | **disable**}

Syntax Description

enable	Enables the creation of NetFlow entries on a per-VLAN basis.
disable	Disables the creation of NetFlow entries on a per-VLAN basis.

Defaults

This feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Entering the **set mls netflow-per-interface disable** command results in the creation of NetFlow entries for all VLANs.

If you enable this feature, NetFlow entries are created both for VLANs on which bridged-flow statistics is enabled and for VLANs on which NetFlow entry creation is enabled. Enabling this feature on specific VLANs causes bridged-flow statistics to be enabled automatically.

For example, if you enable Layer 3 per-VLAN entry creation on VLANs 100 and 200 and at the same time you want to enable bridged-flow statistics on VLANs 150 and 250, NetFlow entry creation and bridged-flow statistics are both enabled on all four VLANs. To collect only bridged-flow statistics for VLAN 150 and 250, you must disable the per-VLAN entry creation feature.

Use the **set mls netflow-entry-create** command to specify the VLANs for which NetFlow entry creation can be enabled or disabled.

Related Commands

set mls netflow-entry-create
show mls

set mls rate

To set the rate at which index-directed packets are sent to the MSFC, use the **set mls rate** command.

set mls rate *kpps*

Syntax Description

kpps	MLS rate in thousands of packets per second; valid values are from 0 to 700. See the "Usage Guidelines" section for more information.

Defaults

The kpps argument is 0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You disable MLS rate limiting when you set the *kpps* argument to 0. When you disable MLS rate limiting, the switch bridges packets to the MSFC; packets are not index-directed.

Examples

This example shows how to set MLS rate limiting to 100 kpps:

```
Console> (enable) set mls rate 100
MLS rate limiting set to 100 Kpps
Console> (enable)
```

This example shows how to disable MLS rate limiting:

```
Console> (enable) set mls rate 0
MLS rate limiting disabled
Console> (enable)
```

Related Commands

show mls

set mls statistics protocol

To add protocols to the protocols statistics list, use the **set mls statistics protocol** command.

set mls statistics protocol *protocol src_port*

Syntax Description

protocol	Name or number of the protocol; valid values are from 1 to 255, **ip**, **ipinip**, **icmp**, **igmp**, **tcp**, and **udp**.
src_port	Number or type of the source port; valid values are from 1 to 65535, **dns**, **ftp**, **smtp**, **telnet**, **x**, and **www**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter any **set mls** commands on a Catalyst 6500 series switch without MLS, this warning message is displayed:

```
MLS not supported on feature card.
```

You can configure a maximum of 64 ports using the **set mls statistics protocol** command.

If you enter **x** for the source port, this specifies the Layer 4 port used by the X-windows application.

Examples

This example shows how to set protocols for statistic collection:

```
Console> (enable) set mls statistics protocol 17 1934
Protocol 17 port 1934 is added to protocol statistics list.
Console> (enable)
```

Related Commands

clear mls statistics entry
show mls statistics

set mls verify

To enable or disable checksum or packet checking based on packet length, use the **set mls verify** command.

set mls verify checksum {**enable** | **disable**}

set mls verify length ip inconsistent {**enable** | **disable**}

Syntax Description

checksum	Specifies IP checksum.
enable	Enables IP checksum.
disable	Disables IP checksum.
length	Specifies checking IP packets based on packet length.
ip	Specifies IP packet.
inconsistent	Specifies checking inconsistent packet length. See the "Usage Guidelines" section for more information.
enable	Enables checking IP packets based on packet length.
disable	Disables checking IP packets based on packet length.

Defaults

IP checksum is enabled.

Checking IP packets based on inconsistent packet length is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set mls verify** command is available on Supervisor Engine 2 (WS-X6K-SUP2-2GE).

If you enable IP checksum or packet checking based on packet length, the Layer 3 ASIC drops Layer 3 error packets that it encounters. If you disable this feature, the packets are not dropped.

Note We recommend that you do not disable IP checksum or packet checking based on packet length unless you have a specific need to pass nonstandard packets.

Checking for inconsistent packet length means that the switch checks for an inconsistency between the physical length of the packet and the length coded in the packet.

Examples

This example shows how to enable IP checksum:

```
Console> (enable) set mls verify checksum enable
Ip checksum verification enabled
Console> (enable)
```

This example shows how to enable checking inconsistent IP packet length:

```
Console> (enable) set mls verify length ip inconsistent enable
Ip inconsistant length verification enabled
Console> (enable)
```

Related Commands

show mls verify

set module

To enable or disable a module, use the **set module** command.

set module enable | **disable** *mod*

Syntax Description

enable	Enables a module.
disable	Disables a module.
mod	Number of the module.

Defaults

The default is all modules are enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Avoid disabling a module when you are connected through a Telnet session; if you disable your session, you will disconnect your Telnet session.

If there are no other network connections to a Catalyst 6500 series switch (for example, on another module), you have to reenable the module from the console.

You can specify a series of modules by entering a comma between each module number (for example, 2,3,5). You can specify a range of modules by entering a dash between module numbers (for example, 2-5).

The **set module disable** command does not cut off the power to a module, it only disables the module. To turn off power to a module, refer to the **set module power** command.

If an individual port on a module was previously disabled, enabling the module does not enable the disabled port.

Examples

This example shows how to enable module 2:

```
Console> (enable) set module enable 2
Module 2 enabled.
Console> (enable)
```

This example shows how to disable module 3 when connected through the console port:

```
Console> (enable) set module disable 3
Module 3 disabled.
Console> (enable)
```

This example shows how to disable module 2 when connected through a Telnet session:

```
Console> (enable) set module disable 2
This command may disconnect your telnet session.
Do you want to continue (y/n) [n]? y
Module 2 disabled.
Console> (enable)
```

Related Commands

show module

set module autoshut

To enable or disable automatic module shutdown, use the **set module autoshut** command.

set module autoshut {**enable** | **disable**} *mod*

Syntax Description

enable	Enables automatic module shutdown.
disable	Disables automatic module shutdown
mod	Module number.

Defaults

Automatic module shutdown is disabled. If enabled, the defaults are as follows:

- Frequency is three times.
- Period is 2 minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can shut down a module manually using the **set module disable** or the **set module power down** commands.

After the module shuts down, you must reenable the module manually.

This command is supported on Ethernet modules only.

Each time a module shuts down by automatic module shutdown, the following SYSLOG message is sent to the configured logging destination:

```
%SYS-5-MOD_AUTOSHUT: Module 2 shutdown automatically, reset 4 times in last 5 minutes
due to inband failure
```

Each time a module exceeds the reset frequency but occurs over a period greater than the configured period, the following SYSLOG message is sent to the configured logging destination:

```
%%SYS-4-MOD_AUTOSHUT_SLOW:Module 1 reset frequency exceeded threshold but over 46
mins. Hence NOT powering down module
```

Examples

This example shows how to enable automatic module shutdown on a module:

```
Console> (enable) set module autoshut enable 2
Console> (enable)
```

This example shows how to disable automatic module shutdown on a module:

```
Console> (enable) set module autoshut disable 2
Console> (enable)
```

Related Commands	
	clear autoshut set autoshut show autoshut

set module name

To set the name for a module, use the **set module name** command.

set module name *mod* [*mod_name*]

Syntax Description

mod	Number of the module.
mod_name	(Optional) Name created for the module.

Defaults

The default is no module names are configured for any modules.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If no module name is specified, any previously specified name is cleared.

Use the **set module name** command to set the module for the MSM. Additional **set module** commands are not supported by the MSM.

Examples

This example shows how to set the name for module 1 to Supervisor:

```
Console> (enable) set module name 1 Supervisor
Module name set.
Console> (enable)
```

Related Commands

show module

set module power

To turn the power on or off to a module, use the **set module power** command.

set module power {**up** | **down**} *mod* [*pm_option*]

Syntax Description

up	Turns on the power to a module.
down	Turns off the power to a module.
mod	Number of the module.
pm_option	(Optional) Power management bit; valid values are 0 to 15.

Defaults

The default is power is on to a module.

The power management bit is set to 0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set module power up** command allows you to check if adequate power is available in the system to turn the power on. If not enough power is available, the module status changes from power-down to power-deny, and this message is displayed:

```
Module 4 could not be powered up due to insufficient power.
```

The *pm_option* argument allows you to set the power management bit for the module on which disaster recovery is needed. Setting the power management bit triggers the downloading of the image from supervisor engine flash memory to the Communication Media Module (CMM) every time the CMM is reset. For more information about disaster recovery and power management bit values on different supervisor engines, see the "Disaster Recovery for CMM Software Upgrades" section of the *Catalyst 6500 Series and Cisco 7600 Series CMM Installation and Configuration Note*. This note is located here:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_14107.htm

Examples

This example shows how to power up module 4:

```
Console> (enable) set module power up 4
Module 4 powered up.
Console> (enable)
```

This example shows how to power down module 4:

```
Console> (enable) set module power down 4
Module 4 powered down.
Console> (enable)
```

Related Commands

set poll
show environment

set module shutdown

To shut down the NAM and Intrusion Detection System Module (IDSM), use the **set module shutdown** command.

set module shutdown {**all** | *mod*}

Syntax Description

all	Shuts down NAM and IDSMs.
mod	Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use the **set module shutdown** command, the configuration is not saved in NVRAM. The next time when the module boots up, it will come online. You can either reinsert or reset the module to bring it online.

If there are no other network connections to a Catalyst 6500 series switch (for example, on another module), you have to reenable the module from the console.

You can specify a series of modules by entering a comma between each module number (for example, 2,3,5).

Examples

This example shows how to shutdown the NAM or IDSM:

```
Console> (enable) set module shutdown 2
Console> (enable)
```

set msfcautostate

To enable or disable the line protocol state determination of the Multilayer Switch Feature Cards (MSFCs) due to port state changes, use the **set msfcautostate** command.

set msfcautostate {**enable** | **disable**}

set msfcautostate {**exclude** | **track**} *mod/ports*

set msfcautostate track {**enable** | **disable**} *vlan_list*

Syntax Description

enable	Activates the line protocol state determination.
disable	Deactivates the line protocol state determination.
exclude	Excludes ports from autostate.
track	Tracks ports for autostate.
mod/ports	Module number and port numbers.
enable	Enables autostate tracking on a VLAN or VLANs.
disable	Disable autostate tracking on a VLAN or VLANs.
vlan_list	VLAN numbers; valid values are from 1 to 4094.

Defaults

The default is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This feature is used to accurately reflect the Layer 3 interface status based on the underlying Layer 2 interface status so that routing and other protocols converge faster. Faster protocol convergence prevents traffic from being discarded without notice.

When you enable the MSFC auto state feature, VLAN interfaces on the MSFC are active only when there is at least one other active interface in the spanning tree forwarding state on the Catalyst 6500 series switch. This interface could be a physical end-user port, a trunk connection for which the VLAN is active, or even another MSFC with an equivalent VLAN interface.

If you enable and then disable or disable and then enable the **set msfcautostate** command, you might have to use the **shutdown** and **no shutdown** commands to disable and then restart the VLAN and WAN interfaces on the MSFC.

If your FXS module ports are in an auxiliary VLAN and there are no switching module ports active in the VLAN, the FXS module will not initialize because the MSFC auto state feature shuts down all MSFC interfaces and subinterfaces. We recommend that you add a physical Ethernet port to the VLAN.

Caution You should not disable the MSFC auto state feature because the Layer 3 interface status might not accurately reflect the Layer 2 interface status. If you disable this feature, traffic might be discarded without notice even though other valid traffic paths might exist.

Autostate exclude mode allows you to specify the ports to exclude from autostate. In normal autostate mode, Layer 3 interfaces remain up if at least one port in the VLAN remains up. If there are appliances like load balancers or firewall servers that are connected to ports in the VLAN, you can configure these ports to be excluded from the autostate feature to make sure that the forwarding SVI does not go down if these ports become inactive.

Autostate exclude mode affects all VLANs to which the port belongs and is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet ports only.

You can use autostate track mode to track key VLAN or port connections to the MSFC. When you configure the autostate track mode, the SVI stays up if any tracked connections remain up in the VLAN. Track mode requires that you define a global tracked VLAN group. The VLANs in this group will be tracked by MSFC autostate whether or not you define a member port to be tracked.

When you configure a VLAN and ports to be tracked by autostate, tracked SVIs remain down until at least one tracked Ethernet port in the VLAN moves to the Spanning Tree Protocol (STP) forwarding state. Conversely, tracked SVIs remain up if at least one tracked Ethernet port stays in the STP forwarding state.

Autostate track mode is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet ports only.

Note You cannot configure both autostate exclude mode and autostate track mode on the same port.

Examples

This example shows how to disable the line protocol state determination of the MSFC:

```
Console> (enable) set msfcautostate disable
Console> (enable)
```

This example shows how to exclude a port from MSFC autostate:

```
Console> (enable) set msfcautostate exclude 3/1
Port 3/1 configured as excluded port
Console> (enable)
```

This example shows how to configure autostate to track ports 1-5 on module 3:

```
Console> (enable) set msfcautostate track 3/1-5
Port 3/1-5 configured as tracked port
Console> (enable)
```

This example shows how to configure autostate to track VLANs 20, 21, 22, and 28:

```
Console> (enable) set msfcautostate track enable 20-22,28
Vlans 20-22,28 added to MSFC autostate track vlan group
Console> (enable)
```

Related Commands

clear msfcautostate
show msfcautostate

8.6 EFT Copy

set msmautostate

To enable or disable the line protocol state determination of the MSMs due to port state changes, use the **set msmautostate** command.

set msmautostate {**enable** | **disable**}

Syntax Description

enable	Activates the line protocol state determination.
disable	Deactivates the line protocol state determination.

Defaults

The default configuration has line protocol state determination disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This feature is useful for discontinuing the advertisement of routing paths when access to them is severed (either through fault or administrative disabling).

When you enable **msmautostate**, VLAN interfaces on the MSM are active only when there is at least one other active interface within the Catalyst 6500 series switch. This could be a physical end-user port, a trunk connection for which the VLAN is active, or even another MSM with an equivalent VLAN interface.

If you disable **msmautostate**, you might have to use the **shutdown** and **no shutdown** commands to disable and then restart the VLAN interface to bring the MSM back up.

Examples

This example shows how to enable the line protocol state determination of the MSM:

```
Console> (enable) set msmautostate enable
MSM port auto state enabled.
Console> (enable)
```

This example shows how to disable the line protocol state determination of the MSM:

```
Console> (enable) set msmautostate disable
MSM port auto state disabled.
Console> (enable)
```

Related Commands

show msmautostate

set multicast ratelimit

To configure multicast rate limiting, use the **set multicast ratelimit** command.

set multicast ratelimit {**enable** | **disable**}

set multicast ratelimit rate *rate*

Syntax Description

enable	Enables multicast rate limiting.
disable	Disables multicast rate limiting.
rate *rate*	Specifies the rate limit in packets per second (pps); valid values are from 0 to 10000.

Defaults

Multicast rate limiting is disabled.

The default rate is 0 pps.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Because the default rate is 0, multicast rate limiting is still operationally disabled even after entering the **set multicast ratelimit enable** command. You must enter a non-zero rate to enable it.

Examples

This example shows how to enable multicast rate limiting:

```
Console> (enable) set multicast ratelimit enable
Enabling Multicast Ratelimiting
Set a non-zero threshold rate to operationally enable multicast ratelimiting
Console> (enable)
```

This example shows how to set the rate limit in pps:

```
Console> (enable) set multicast ratelimit rate 300
Multicast ratelimit watermark rate is set to 300 pps
Console> (enable)
```

This example shows how to disable multicast rate limiting:

```
Console> (enable) set multicast ratelimit disable
Multicast Ratelimiting already disabled
Console> (enable)
```

Related Commands

show multicast ratelimit-info

8.6 EFT Copy

set multicast router

To configure a port manually as a multicast router port, use the **set multicast router** command.

set multicast router *mod/port*

Syntax Description

mod/port	Number of the module and port on the module.

Defaults

The default is no ports are configured as multicast router ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enable IGMP snooping, the ports to which a multicast-capable router is attached are identified automatically. The **set multicast router** command allows you to configure multicast router ports statically.

Examples

This example shows how to configure a multicast router port:

```
Console> (enable) set multicast router 3/1
Port 3/1 added to multicast router port list.
Console> (enable)
```

Related Commands

clear multicast router
set igmp
show multicast group count
show multicast router

set ntp broadcastclient

To enable or disable NTP in broadcast-client mode, use the **set ntp broadcastclient** command.

set ntp broadcastclient {**enable** | **disable**}

Syntax Description

enable	Enables NTP in broadcast-client mode.
disable	Disables NTP in broadcast-client mode.

Defaults

The default is broadcast-client mode is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The broadcast-client mode assumes that a broadcast server, such as a router, sends time-of-day information regularly to a Catalyst 6500 series switch.

Examples

This example shows how to enable an NTP broadcast client:

```
Console> (enable) set ntp broadcastclient enable
NTP Broadcast Client mode enabled.
Console> (enable)
```

This example shows how to disable an NTP broadcast client:

```
Console> (enable) set ntp broadcastclient disable
NTP Broadcast Client mode disabled.
Console> (enable)
```

Related Commands

show ntp

set ntp broadcastdelay

To configure a time-adjustment factor so the Catalyst 6500 series switch can receive broadcast packets, use the **set ntp broadcastdelay** command.

set ntp broadcastdelay *microseconds*

Syntax Description

microseconds	Estimated round-trip time, in microseconds, for NTP broadcasts; valid values are from 1 to 999999.

Defaults

The default is the NTP broadcast delay is set to 3000 milliseconds.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the NTP broadcast delay to 4000 milliseconds:

```
Console> (enable) set ntp broadcastdelay 4000
NTP broadcast delay set to 4000 microseconds.
Console> (enable)
```

Related Commands

show ntp

set ntp client

To enable or disable a Catalyst 6500 series switch as an NTP client, use the **set ntp client** command.

set ntp client {**enable** | **disable**}

Syntax Description

enable	Enables a Catalyst 6500 series switch as an NTP client.
disable	Disables a Catalyst 6500 series switch as an NTP client.

Defaults

The default is NTP client mode is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure NTP in either broadcast-client mode or client mode. The broadcast-client mode assumes that a broadcast server, such as a router, sends time-of-day information regularly to a Catalyst 6500 series switch. The client mode assumes that the client (a Catalyst 6500 series switch) regularly sends time-of-day requests to the NTP server.

Examples

This example shows how to enable NTP client mode:

```
Console> (enable) set ntp client enable
NTP client mode enabled.
Console> (enable)
```

Related Commands

show ntp

set ntp server

To specify the NTP server address and configure an NTP server authentication key, use the **set ntp server** command.

set ntp server *ip_addr* [**key** *public_keynum*]

Syntax Description

ip_addr	IP address of the NTP server.
key *public_keynum*	(Optional) Specifies the key number; valid values are 1 to 4292945295.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The client mode assumes that the client (a Catalyst 6500 series switch) sends time-of-day requests regularly to the NTP server. A maximum of ten servers per client is allowed.

Examples

This example shows how to configure an NTP server:

```
Console> (enable) set ntp server 172.20.22.191
NTP server 172.20.22.191 added.
Console> (enable)
```

Related Commands

clear ntp server
show ntp

set ntp summertime

To set the clock ahead one hour during daylight saving time, use the **set ntp summertime** command.

set ntp summertime {**enable** | **disable**} [*zone*]

set ntp summertime recurring [{*week*} {*day*} {*month*} {*hh***:***mm*} {*week* | *day* | *month* | *hh***:***mm*} [*offset*]]

set ntp summertime date {*month*} {*date*} {*year*} {*hh***:***mm*}{*month* | *date* | *year* | *hh***:***mm*} [*offset*]

Syntax Description

enable	Causes the system to set the clock ahead one hour during daylight saving time.
disable	Prevents the system from setting the clock ahead one hour during daylight saving time.
zone	(Optional) Time zone used by the **set summertime** command.
recurring	Specifies the summertime dates that recur every year.
week	(Optional) Week of the month (**first**, **second**, **third**, **fourth**, **last**, 1...5).
day	(Optional) Day of the week (**Sunday**, **Monday**, **Tuesday**, and so forth).
month	Month of the year (**January**, **February**, **March**, and so forth).
hh:mm	Hours and minutes.
offset	(Optional) Amount of offset in minutes (1 to 1440 minutes).
date	Specifies summertime dates for specific non-recurring dates.
date	Day of the month (1 to 31).
year	Number of the year (1993 to 2035).

Defaults

By default, the **set ntp summertime** command is disabled. Once enabled, the default for *offset* is 60 minutes, following U.S. standards.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After you enter the **clear config** command, the dates and times are set to default.

Unless you configure it otherwise, this command advances the clock one hour at 2:00 a.m. on the first Sunday in April and moves back the clock one hour at 2:00 a.m. on the last Sunday in October.

Examples

This example shows how to cause the system to set the clock ahead one hour during daylight saving time:

```
Console> (enable) set ntp summertime enable PDT
Summertime is enabled and set to "PDT".
Console> (enable)
```

This example shows how to prevent the system from setting the clock ahead one hour during daylight saving time:

```
Console> (enable) set ntp summertime disable
Summertime disabled.
Console> (enable)
```

This example shows how to set daylight saving time to the zonename AUS and repeat every year, starting from the third Monday of February at noon and ending at the second Saturday of August at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set ntp summertime AUS recurring 3 Mon Feb 12:00 2 Saturday Aug 15:00 30
Summer time is disabled and set to ’AUS’ with offset 30 minutes.
   start: 12:00:00 Sun Feb 13 2000
   end:   14:00:00 Sat Aug 26 2000
   Recurring, starting at 12:00:00 on Sunday of the third week of February and ending
   on Saturday of the fourth week of August.
Console> (enable)
```

This example shows how to set the daylight saving time to start on January 29, 1999 at 2:00 a.m. and end on August 19, 2004 at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set ntp summertime date jan 29 1999 02:00 aug 19 2004 15:00 30
Summertime is disabled and set to ''
Start : Fri Jan 29 1999, 02:00:00
End   : Thu Aug 19 2004, 15:00:00
Offset: 30 minutes
Recurring: no
Console> (enable)
```

This example shows how to set recurring to reset default to US summertime:

```
Console> (enable) set ntp summertime recurring 3 mon feb 4 thurs oct 8:00 500
Command authorization none.
Summertime is enabled and set to ‘’
Start : Mon Feb 21 2000, 03:00:00
End   : Fri Oct 20 2000, 08:00:00
Offset: 500 minutes (8 hours 20 minutes)
Recurring: yes, starting at 03:00am of third Monday of February and ending on 08:00am of
fourth Thursday of October.
Console> (enable)
```

Related Commands

show ntp

8.6 EFT Copy

set ntp timezone

To configure the time offset from Greenwich Mean Time, use the **set ntp timezone** command.

set timezone [*zone_name*] [*hours* [*minutes*]]

Syntax Description

zone_name	(Optional) Name of the time zone.
hours	(Optional) Time offset (hours) from Greenwich Mean Time; valid values are from –12 to 12 hours.
minutes	(Optional) Time offset (minutes) from Greenwich Mean Time; valid values are 0 to 59 minutes.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set ntp timezone** command is effective only when NTP is running. If you set the time explicitly and NTP is disengaged, the **set ntp timezone** command has no effect. If you have enabled NTP and have not entered the **set timezone** command, the Catalyst 6500 series switch displays UTC by default.

Examples

This example shows how to set the time zone to Pacific Standard Time with an offset of minus 8 hours from UTC:

```
Console> (enable) set ntp timezone PST -8
Timezone set to "PST", offset from UTC is -8 hours.
Console> (enable)
```

Related Commands

clear ntp timezone
show ntp

set packet-capture

To specify the source module and port for Mini Protocol Analyzer packet capturing and to start or stop packet capturing, use the **set packet-capture** command.

set packet-capture *mod/port*

set packet-capture {**start** | **stop**}

Syntax Description

mod	Number of the module.
port	Number of the port on the module.
start	Starts packet capturing.
stop	Stops packet capturing.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set packet-capture** *mod/port* command is stored in NVRAM and becomes effective when the **set packet-capture start** command is entered and SPAN is running. The **packet-capture start** command will not work if a *mod/port* argument has not been entered. Only one **set packet-capture** *mod/port* command is in effect at any one time. A new command will cancel an old one.

Examples

This example shows how to specify a port on a module for packet capturing:

```
Console> (enable) set packet-capture 1/1
Capturing port set to 1/1.
Console> (enable)
```

This example shows how to start packet capturing on a port:

```
Console> (enable) set packet-capture start
Packet capturing can result in ptotocol packets(STP, UDLD, PAGP, etc.)
getting dropped resulting in network instability. Also, it can affect
system performance or inband connectivity as sc0/sc1 interface packets
can be dropped without warning
Do you want to continue(y/n) [n]? y
Succesfully started the packet capture task.
Console> (enable)
```

This example shows the message that is displayed when you attempt to start packet capturing without specifying a source port for packet capturing:

```
Console> (enable) set packet-capture start
Failed to start packet capturing as the source port has not been specified.
Console> (enable)
```

Related Commands

clear packet-capture
set packet-capture dump-file
set packet-capture filter
set packet-capture limit
set packet-capture snap-length
show packet-capture

set packet-capture dump-file

To specify the device and file where the dumped packets for the Mini Protocol Analyzer feature are to be stored, use the **set packet-capture dump-file** command.

set packet-capture dump-file [*device:file-id*]

Syntax Description

device	Device where the dumped packets are to be stored.
file-id	File where the dumped packets are to be stored.

Defaults

The default file name will be **bootflash:eth_mm:dd_hh:mm** where **mm:dd_hh:mm** is the date and time at the start of packet capturing.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set packet-capture dump-file** command is stored in NVRAM and so persists over a power cycle and becomes effective when the **set packet-capture start** command is issued and SPAN is running. Can this command be executed without an argument to get back to the default?

Examples

This example shows messages displayed during the execution of this command:

```
Console> (enable) set packet-capture dump-file bootflash:Sniff
Sniffer Dump File name set to  bootflash:Sniff
Console> (enable)
Console> (enable) set packet-capture dump-file
bootflash:qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
File name qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq exceeds the max
length allowed (29 chars).
Failed to set the packet capture dump file to
bootflash:qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
Console> (enable)s
```

Related Commands

clear packet-capture
set packet-capture
set packet-capture filter
set packet-capture limit
set packet-capture snap-length
show packet-capture

set packet-capture filter

To configure Mini Protocol Analyzer packet-capturing filters, use the **set packet-capture filter** command.

set packet-capture filter {**source** | **destination**} **mac** *mac-address*

set packet-capture filter {**source** | **destination**} **ip** *ip-address* [*ipmask*]

Syntax Description

source	Sets a source MAC address or IP address as the packet-capturing filter.
destination	Sets a destination MAC address or IP address as the packet-capturing filter.
mac *mac-address*	MAC address.
ip *ip-address*	IP address.
ipmask	IP subnet mask.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The packets can be captured based on either the source or the destination MAC or IP address. The MAC address will be of the format **aa-bb-cc-dd-ee-ff**.

The packets can be captured based on either the source or the destination MAC or IP address. The IP address will be of the format **a.b.c.d**.

Examples

This example shows how to set a packet-capturing filter based on a destination MAC address:

```
Console> (enable) set packet-capture filter destination mac 10-10-10-10-10-10
Succesfully added the filter string.
Console> (enable)
```

This example shows how to set a packet-capturing filter based on a destination IP address:

```
Console> (enable) set packet-capture filter destination ip 10.12.12.12
Succesfully added the filter string.
Console> (enable)
```

Related Commands	
	clear packet-capture set packet-capture set packet-capture dump-file set packet-capture limit set packet-capture snap-length show packet-capture

set packet-capture limit

To specify the number of packets to be captured before the Mini Protocol Analyzer stops, use the **set packet-capture limit** command.

set packet-capture limit *num_packets*

Syntax Description

num_packets	Number of packets to capture before the mini protocol analyzer stops; valid values are from 0 to 32000.

Defaults

The default is that the mini protocol analyzer keeps running until all the space on the flash device is filled.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you enter **0** for the *num_packets* argument, packet capturing continues until the flash device is filled. To specify the flash device, use the **set packet-capture dump-file** command.

Examples

This example shows messages displayed during the execution of this command:

```
Console> (enable) set packet-capture limit 32
Packet capture number set to 32.
Console> (enable)
```

Related Commands

clear packet-capture
set packet-capture
set packet-capture dump-file
set packet-capture filter
set packet-capture snap-length
show packet-capture

set packet-capture snap-length

To specify the length in bytes of packets that are captured for the Mini Protocol Analyzer feature, use the **set packet-capture snap-length** command.

set packet-capture snap-length *pkt_snap_len*

Syntax Description

pkt_snap_len	Length of captured packets; valid values are from 0 to 10258.

Defaults

The *pkt_snap_len* argument is 0.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Captured packets are truncated to snap-length bytes of data. If you enter **0** for the *pkt_snap_len* argument, full packets are captured.

Examples

This example shows how to specify packet length:

```
Console> (enable) set packet-capture snap-length 78
Packets captured will be truncated to 78 bytes.
Console> (enable)
```

Related Commands

clear packet-capture
set packet-capture
set packet-capture dump-file
set packet-capture filter
set packet-capture limit
show packet-capture

8.6 EFT Copy

set password

To change the login password on the CLI, use the **set password** command.

set password

Syntax Description

This command has no arguments or keywords.

Defaults

The default is no password is configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Passwords are case sensitive and may be from 0 to 19 characters in length, including spaces.

The command prompts you for the old password. If the password you enter is valid, you are prompted to enter a new password and to verify the new password. A zero-length password is allowed by pressing **Return**.

Examples

This example shows how to set an initial password:

```
Console> (enable) set password
Enter old password: <old_password>
Enter new password: <new_password>
Retype new password: <new_password>
Password changed.
Console> (enable)
```

set pbf

To enable policy-based forwarding (PBF) and to set a MAC address for the PFC2, use the **set pbf** command.

set pbf [**mac** *mac_address*]

Syntax Description

mac *mac_address*	(Optional) Specifies MAC address for the PFC2.

Defaults

You can use the default MAC address, or you can specify a MAC address. See the “Usage Guidelines” section for more information.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must set a MAC address for the PFC2. We recommend that you use the default MAC address provided by the MAC PROM. When you specify your own MAC address using the **set pbf mac** command, if the MAC address is a duplicate of a MAC address already in use, packets might be dropped.

PBF is not supported with an operating (booted) MSFC2 in the Catalyst 6500 series switch that is being used for PBF. If an MSFC2 is present but not booted, you can configure PBF.

PBF may require some configuration on attached hosts. When a router is not present in the network, ARP table entries have to be statically added on each host participating in PBF. Refer to the “Configuring Policy-Based Forwarding” section of Chapter 16, “Configuring Access Control,” in the *Catalyst 6500 Series Software Configuration Guide* for detailed information on configuring hosts.

Note PBF does not work with 802.1Q tunnel traffic. PBF is supported on Layer 3 IP unicast traffic, but it is not applicable to Layer 2 traffic. At the intermediate (PBF) switch, all 802.1Q tunnel traffic appears as Layer 2 traffic.

Examples

This example shows how to set the default MAC address for the PFC2:

```
Console> (enable) set pbf
Console> (enable) Operation successful.
Console> (enable)
```

This example shows how to set a specific MAC address for the PFC2:

```
Console> (enable) set pbf mac 00-01-64-61-39-c2
Console> (enable) Operation successful.
Console> (enable)
```

Related Commands

clear pbf
show pbf

set pbf arp-inspection

To add an ARP-inspection ACE to the ACL for a client list or a gateway, use the **set pbf arp-inspection** command.

set pbf arp-inspection *list_name*

Syntax Description

list_name	Client list or gateway list.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to add an ARP-inspection ACE to the ACL for a client list:

```
Console> (enable) set pbf arp-inspection cl1
.ccl1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) ACL commit in progress.

ACL '.ccl1' successfully committed.
Console> (enable)
```

Related Commands

clear pbf arp-inspection
show pbf arp-inspection

set pbf client

To add new hosts to a PBF client list, use the **set pbf client** command.

set pbf client *client_list ip_addr mac_addr vlan*

Syntax Description

client_list	Client list name.
ip_addr	IP address.
mac_addr	MAC address.
vlan	VLAN number.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use this command with the **set pbf gw** command and the **set pbf-map** command to simplify the process of setting and committing the security ACLs and adjacency information. The **set pbf-map** command creates the security ACLs and adjacency information based on your input, commits them to the hardware, and maps them to VLANs. As part of creating the necessary VACLs to redirect traffic from one VLAN to another, the ARP packets are redirected to the software, and the supervisor engine generates ARP replies for the gateway and client requests.

PBF clients and PBF gateways must be on different VLANs. No clients or gateways can have the same IP address. The maximum number of entries is 1024.

The client name and gateway name must be no more than 12 characters.

If you create a PBF map between two VLANs that already have VACLs attached, the PBF ACLs overwrite the previous configuration. The opposite is also true. If you map a new VACL to VLANs with PBF ACLs that were created by using the **set pbf-map** command, the new VACL overwrites the previous configuration.

Note The number of PBF-client groups that can be mapped to a single PBF gateway is dependent on the number of ACLs that are already configured. For example, if the number of supported ACLs is 250 and you already have 20 ACLs defined, you can have 229 client groups mapped to a gateway.

For more information about using the **set pfb client**, **set pbf gw**, and **set pbf-map** commands, refer to the "Configuring Policy-Based Forwarding" section of Chapter 16, "Configuring Access Control," in the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to add a new host to a client list:

```
Console> (enable) set pbf client cl1 21.1.1.1 00-00-00-00-40-01 101
Commit operation successful.
Console> (enable)
```

Related Commands

clear pbf client
clear pbf gw
clear pbf-map
set pbf gw
set pbf-map
show pbf client
show pbf gw
show pbf-map

8.6 EFT Copy

set pbf gw

To add a PBF gateway to handle connections between VLANs, use the **set pbf gw** command.

set pbf gw *gw_name ip_addr ip_mask mac_addr vlan*

Syntax Description

gw_name	Gateway name.
ip_addr	IP address.
ip_mask	IP mask.
mac_addr	MAC address.
vlan	VLAN number.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use this command with the **set pbf gw** command and the **set pbf-map** command to simplify the process of setting and committing the security ACLs and adjacency information. The **set pbf-map** command creates the security ACLs and adjacency information based on your input, commits them to the hardware, and maps them to VLANs. As part of creating the necessary VACLs to redirect traffic from one VLAN to another, the ARP packets are redirected to the software, and the supervisor engine generates ARP replies for the gateway and client requests.

PBF clients and PBF gateways must be on different VLANs. No clients or gateways can have the same IP address. The maximum number of entries is 1024.

The client name and gateway name must be no more than 12 characters.

If you create a PBF map between two VLANs that already have VACLs attached, the PBF ACLs overwrite the previous configuration. The opposite is also true. If you map a new VACL to VLANs with PBF ACLs that were created by using the **set pbf-map** command, the new VACL overwrites the previous configuration.

Note The number of PBF-client groups that can be mapped to a single PBF gateway is dependent on the number of ACLs that are already configured. For example, if the number of supported ACLs is 250 and you already have 20 ACLs defined, you can have 229 client groups mapped to a gateway.

For more information about using the **set pfb client**, **set pbf gw**, and **set pbf-map** commands, refer to the “Configuring Policy-Based Forwarding” section of Chapter 16, “Configuring Access Control,” in the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to add a PBF gateway to handle connections between VLANs:

```
Console> (enable) set pbf gw gw1 21.0.0.128 255.0.0.0 00-a0-c9-81-e1-13 102
Commit operation successful.
Console> (enable)
```

Related Commands

clear pbf client
clear pbf gw
clear pbf-map
set pbf client
set pbf-map
show pbf client
show pbf gw
show pbf-map

set pbf-map

To create security ACLs and to set adjacency information or to map a list of hosts to a gateway, use the **set pbf-map** command.

set pbf-map {*ip_addr_1*} {*mac_addr_1*} {*vlan_1*} {*ip_addr_2*} {*mac_addr_2*} {*vlan_2*}

set pbf-map {*client_list*} {*gw_name*}

Syntax Description

ip_addr_1	IP address of host 1.
mac_addr_1	MAC address of host 1.
vlan_1	Number of the first VLAN.
ip_addr_2	IP address of host 2.
mac_addr_2	MAC address of host 2.
vlan_2	Number of the second VLAN.
client_list	Client list name.
gw_name	Gateway name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set pbf-map** command does not change existing commands or NVRAM.

The **set pbf-map** command creates security ACLs and adjacency information based on your input, and then automatically commits the ACLs. This command simplifies the configuration of policy-based forwarding.

An example of the simplified syntax is **set pbf-map 1.1.1.1 0-0-0-0-0-1 11 2.2.2.2 0-0-0-0-0-2 12**.

The above example is equivalent to all of the following PBF commands, which were released prior to 7.4:

set security acl adjacency PBF_MAP_ADJ_0 11 0-0-0-0-0-1
set security acl adjacency PBF_MAP_ADJ_1 12 0-0-0-0-0-2
commit security acl adjacency
set security acl ip PBF_MAP_ACL_11 redirect PBF_MAP_ADJ_1 ip host 1.1.1.1 host 2.2.2.2
set security acl ip PBF_MAP_ACL_12 redirect PBF_MAP_ADJ_0 ip host 2.2.2.2 host 1.1.1.1

If the **permit ip any any** ACE is missing, the following two entries are added:

set security acl ip PBF_MAP_ACL_11 permit ip any any
set security acl ip PBF_MAP_ACL_12 permit ip any any
commit security acl ip PBF_MAP_ACL_11

commit security acl ip PBF_MAP_ACL_12
set security acl map PBF_MAP_ACL_11 11
set security acl map PBF_MAP_ACL_12 12

Each entry in the ACL that is added by the **set pbf-map** command is inserted before the default **permit ip any any** ACE.

If you want to add entries other then redirect ACEs to the adjacency table, use the **set security acl ip PBF_MAP_ACL_(VLAN_ID)** command.

Once the map is created between the client and gateway lists by entering the **set pbf-map** {*client_list*} {*gw_name*} command, no more mapping can be added for these two lists. Subsequent clients and gateways can be added.

For more information about using the **set pfb client**, **set pbf gw**, and **set pbf-map** commands, refer to the "Enhancements to PBF Configuration" section of Chapter 16, "Configuring Access Control," in the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to specify a PBF_MAP_ACL:

```
Console> (enable) set pbf-map 1.1.1.1 0-0-0-0-0-1 11 2.2.2.2 0-0-0-0-0-2 22

Commit operation successful.
Commit operation successful.

ACL 'PBF_MAP_ACL_11' successfully committed.
Console> (enable)
ACL PBF_MAP_ACL_11 successfully mapped to VLAN 11.
Console> (enable)
ACL 'PBF_MAP_ACL_22' successfully committed.
Console> (enable)
ACL PBF_MAP_ACL_22 successfully mapped to VLAN 22.
Console> (enable) Operation successful.
Console> (enable)
```

This example show how to map a list of hosts to a gateway:

```
Console> (enable) set pbf-map cl1 gw1
.ccl1 editbuffer modified. Use 'commit' command to apply changes.
.ggw1 editbuffer modified. Use 'commit' command to apply changes.
.ccl1 editbuffer modified. Use 'commit' command to apply changes.
.ggw1 editbuffer modified. Use 'commit' command to apply changes.
.ccl1 editbuffer modified. Use 'commit' command to apply changes.
.ggw1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) ACL commit in progress.
Console> (enable) ACL commit in progress.

ACL '.ccl1' successfully committed.
Console> (enable)
ACL '.ggw1' successfully committed.
Console> (enable) Mapping in progress.
Please configure VLAN 101.

ACL .ccl1 successfully mapped to VLAN 101.
Console> (enable) Mapping in progress.
Please configure VLAN 102.

ACL .ggw1 successfully mapped to VLAN 102.
Console> (enable)
```

Related Commands

clear pbf client
clear pbf gw
clear pbf-map
set pbf client
set pbf gw
show pbf client
show pbf gw
show pbf-map

set pbf vlan

To create policy-based forward (PBF) Layer 2 CAM entries on a VLAN, use the **set pbf vlan** command.

set pbf vlan *vlan*

Syntax Description

vlan	VLAN number.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Note Specifying the PBF MAC address on a VLAN is only required on the Supervisor Engine 720 with PFC3.

This command creates PBF Layer 2 CAM entries on the VLANs that you specify. Packets matching these entries are classified as Layer 3 packets. The Layer 2 entries are created only if the PBF MAC address is set using the **set pbf mac** command before entering the **set pbf vlan** command.

Using the **clear pbf** command does not clear the VLANs enabled for PBF. The **clear pbf** command does clear the Layer 2 table entries associated with the VLANs (because the MAC address is no longer valid). You must explicitly clear the PBF-enabled VLANs to remove them from NVRAM by entering the **clear pbf vlan** *vlan_list* command.

You can specify a range of VLANs in the CLI.

Examples

This example shows how to specify the PBF MAC address on VLANs 11 and 12:

```
Console> (enable) set pbf vlan 11-12
Console> (enable) PBF enabled on vlan(s) 11-12.
Operation successful.
Console> (enable)
```

In this example, the message "Operation successful" indicates that the PBF MAC address was saved in NVRAM.

Related Commands

clear pbf vlan
set pbf
show pbf

8.6 EFT Copy

set policy

To configure an authentication policy group and name, use the **set policy** command.

set policy group *group_name* **ip-address** *ip_addr* [*ip_mask*]

set policy name *policy_name* **group** *group_name*

set policy name *policy_name* **url-redirect** *url-redirect-string*

Syntax Description

group *group_name*	Sets policy-based group memberships.
ip-address *ip_addr*	Specifies an IP address to be added to the policy group.
ip_mask	(Optional) IP mask.
name *policy_name*	Specifies the policy name.
url-redirect *url-redirect-string*	Maps a URL to a policy name. The *url-redirect-string* argument can be a maximun of 255 characters.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set policy group** *group_name* **ip-address** *ip_addr* command allows you to add an IP address to an existing policy group. This command fails if the group name is not already present in the group database.

You can add a policy group to a policy template by entering the **set policy name** *policy_name* **group** *group-name* command. If a policy template does not exist, the switch creates it. Similarly, if the policy group name does not exist, the switch creates it.

Examples

This example shows how to add an IP address to an existing policy group:

```
Console> (enable) set policy group grp1 ip-address 100.1.1.1 255.255.255.255
Added IP 100.1.1.1/255.255.255.255 to policy group grp1.
Console> (enable)
```

This example shows how to add a policy group to the policy template:

```
Console> (enable) set policy name pol1 group grp1
Added group grp1 to policy template pol1.
Console> (enable)
```

This example shows how to map a URL to a policy name:

```
Console> (enable) set policy name exception_policy url-redirect http://cisco.com
Url Redirect http://cisco.com mapped successfully to policy name exception_policy
Console> (enable)
```

Related Commands

clear policy
show policy

set poll

To enable or disable system polling, use the **set poll** command.

set poll {**enable** | **disable**}

Syntax Description

enable	Enables system polling.
disable	Disables system polling.

Defaults

System polling is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set poll** command is part of a recovery procedure that you can follow if the Communication Media Module (CMM) software image fails to load properly. For more information about this procedure, see the "Disaster Recovery for CMM Software Upgrades" section of the *Catalyst 6500 Series and Cisco 7600 Series CMM Installation and Configuration Note*. This note is located here:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_14107.htm

The **set poll disable** command disables the periodic polling of modules by the supervisor engine over the Ethernet Out-of-Band Channel (EOBC) link.

Note Be careful when using the **set poll disable** command. If a failure occurs on the control plane with Serial Communication Protocol (SCP) communication and periodic polling of modules is disabled, the failure will not be immediately detected.

Note If system polling is disabled, communication failures between the supervisor engine and the modules are not detected.

Examples

This examples shows how to disable system polling:

```
Console> (enable) set poll disable
System polling disabled.
Console> (enable)
```

Related Commands

set module power
show poll

set port arp-inspection

To set Address Recognition Protocol (ARP) inspection thresholds and the ARP trust feature on a per-port basis, use the **set port arp-inspection** command.

set port arp-inspection *mod/port* **drop-threshold** *rate* **shutdown-threshold** *rate*

set port arp-inspection *mod/port* **trust** {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port or ports on the module.
drop-threshold	Indicates the drop threshold.
rate	Number of packets per second; valid values are from 0 to 1000 pps.
shutdown-threshold	Indicates the shutdown threshold.
trust	Specifies the ARP trust feature.
enable	Enables the trust feature on a port or ports. See the “Usage Guidelines” section for more information.
disable	Disables the trust feature on a port or ports.

Defaults

Both threshold rates are 0 packets per second.

The trust feature is disabled.

Command Types

Switch command

Command Modes

Privileged.

Usage Guidelines

If the number of packets exceeds the drop-threshold rate, the excess packets are dropped. The excess packets are still counted toward the shutdown-threshold rate. If the number of packets exceeds the shutdown-threshold rate, the port is shut down.

When the threshold rates are both at 0 packets per second, per-port rate limiting is not on.

The **set port arp-inspection** *mod/port* **trust** {**enable** | **disable**} command enables or disables the ARP inspection trust feature. The ARP packets from trusted ports are forwarded without inspection. Untrusted packets are intercepted and subject to matching both dynamic DHCP snooping and static ARP inspection rules.

Do not enable Dynamic ARP Inspection (DAI) on VLANs that have ports with static IP addresses unless the ports are trusted.

Examples

This example shows how to set the drop-threshold to 500 and the shutdown-threshold to 1000 for port 2/1:

```
Console> (enable) set port arp-inspection 2/1 drop-threshold 500 shutdown-threshold 1000
Drop Threshold=500, Shutdown Threshold=1000 set on port 2/1.
Console> (enable)
```

This example shows how to enable the ARP inspection trust feature on port 2 of module 2:

```
Console> (enable) set port arp-inspection 2/2 trust enable
Port(s)  2/2 state set to trusted for ARP Inspection.
Console> (enable)
```

This example shows how to disable the ARP inspection trust feature on port 2 of module 2:

```
Console> (enable) set port arp-inspection 2/2 trust disable
Port  2/2 state set to untrusted for ARP Inspection.
Console> (enable)
```

Related Commands

set security acl arp-inspection
show port arp-inspection

set port auto-mdix

To enable or disable the automatic Media-Dependent Interface Crossover (MDIX) function, use the **set port auto-mdix** feature.

set port auto-mdix *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Module number and port number.
enable	Enables automatic MDIX function.
disable	Disables automatic MDIX function.

Defaults

The automatic MDIX function is enabled on all WS-X6748-GE-TX ports.

The automatic MDIX function is disabled on the Supervisor Engine 720. See the “Usage Guidelines” section for more information.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Auto-MDI/MDIX has always been enabled on the following modules:

- WS-X6548-RJ-45, WS-X6548-RJ-21, WS-X6148-GE-TX, WS-X6548-GE-TX

  Auto-MDI/MDIX works in 10-, 100-, and 1000-Mbps modes with autonegotiated and fixed speeds.
- WS-X6516-GE-TX

  Auto-MDI/MDIX works with the speed set to auto/1000 Mbps, but not with the speed set to 10 Mbps or 100 Mbps.
- WS-X6316-GE-TX

With software release 8.2(1), auto-MDIX is also enabled on the following modules:

- WS-X6748-GE-TX, Supervisor Engine 720 port 2 (RJ-45)

  Auto-MDI/MDIX works with the speed set to auto/1000, but not with the speed set to 10 Mbps or 100 Mbps
- WS-X6148X2-RJ-45, WS-X6148X2-45AF

  Auto-MDI/MDIX works with the speed set to auto, but not with the speed set to 10 Mbps or 100 Mbps.

Note Auto-MDI/MDIX is not supported on any other 10/100-Mbps Ethernet modules or GBIC, SFP, and XENPAK ports.

Examples

This example shows how to enable the automatic MDIX funtion on port 4/1:

```
Console> (enable) set port 4/1 auto-mdix
Console> (enable)
```

Related Commands

show port auto-mdix

set port auxiliaryvlan

To configure the auxiliary VLAN ports, use the **set port auxiliaryvlan** command.

set port auxiliaryvlan *mod*[*/port*] {*vlan* | **untagged** | **dot1p** | **none**} [**cdpverify** {**enable** | **disable**}]

Syntax Description

mod[*/port*]	Number of the module and (optional) port or multiple ports.
vlan	Number of the VLAN; valid values are from 1 to 4094.
untagged	Specifies the connected device send and receive untagged packets without 802.1p priority.
dot1p	Specifies the connected device send and receive packets with 802.1p priority.
none	Specifies that the switch does not send any auxiliary VLAN information in the CDP packets from that port.
cdpverify	(Optional) Sets automatic detection of IP phones by using CDP.
enable	(Optional) Enables the automatic detection of IP phones.
disable	(Optional) Disables the automatic detection of IP phones.

Defaults

The default setting is **none**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a port, all ports are selected.

This command is not supported by the NAM.

The *vlan* option specifies that the connected device sends packets that are tagged with a specific VLAN.

If you enter the **none** option, voice information will not be sent or received.

Dynamic VLAN support for voice VLAN identifier (VVID) includes these restrictions to the following multiple VLAN access port (MVAP) configuration on the switch port:

- You can configure any VVID on a dynamic port including dot1p and untagged, except when the VVID is equal to **dot1p** or **untagged**. If this is the case, you must configure VMPS with the MAC address of the IP phone. When you configure the VVID as **dot1p** or **untagged** on a dynamic port, this warning message is displayed:

```
VMPS should be configured with the IP phone mac’s.
```

- For dynamic ports, the auxiliary VLAN ID cannot be the same as the native VLAN ID assigned by VMPS for the dynamic port.
- You cannot configure trunk ports as dynamic ports, but an MVAP can be configured as a dynamic port.

The presence of an IP phone is determined through CDP packet exchange between the switch and the phone. This detection method is used for both inline-powered IP phones and wall-powered IP phones.

If the auxiliary VLAN ID equals the port-VLAN ID or when the auxiliary VLAN ID is configured as **none**, **dot1p**, or **untagged**, this feature cannot be applied to the port. If any command entry results in the auxiliary VLAN ID equaling the port-VLAN ID, the feature is disabled and the following warning message is displayed:

```
cdpverify feature on port mod/port is disabled.
```

Examples

This example shows how to set the auxiliary VLAN port to **untagged**:

```
Console> (enable) set port auxiliaryvlan 5/7 untagged
Port 5/7 allows the connected device send and receive untagged packets and
without 802.1p priority.
Console> (enable)
```

This example shows how to set the auxiliary VLAN port to **dot1p**:

```
Console> (enable) set port auxiliaryvlan 5/9 dot1p
Port 5/9 allows the connected device send and receive packets with 802.1p priority.
Console> (enable)
```

This example shows how to set the auxiliary VLAN port to **none**:

```
Console> (enable) set port auxiliaryvlan 5/12 none
Port 5/12 will not allow sending CDP packets with AuxiliaryVLAN information.
Console> (enable)
```

This example shows how to set the auxiliary VLAN port to a specific module, port, and VLAN:

```
Console> (enable) set port auxiliaryvlan 2/1-3 222
Auxiliaryvlan 222 configuration successful.
AuxiliaryVlan AuxVlanStatus Mod/Ports
------------- ------------- -------------------------
222           active        1/2,2/1-3
Console> (enable)
```

Related Commands

show port auxiliaryvlan

set port broadcast

To set broadcast, multicast, or unicast suppression for one or more ports, use the **set port broadcast** command. The threshold limits the backplane traffic received from the module.

set port broadcast *mod/port threshold%* [**violation** {**drop-packets** | **errdisable**}]
[**multicast** {**enable** | **disable**}] [**unicast** {**enable** | **disable**}]

Syntax Description

mod/port	Number of the module and the port on the module.
threshold%	Percentage of total available bandwidth that can be used by traffic; valid values are decimal numbers from 0.00% to 100% or whole numbers from 0% to 100%.
violation	(Optional) Specifies an action when suppression occurs.
drop-packets	(Optional) Drops packets when suppression occurs.
errdisable	(Optional) Errdisables the port when suppression occurs.
multicast	(Optional) Specifies multicast suppression.
enable | **disable**	(Optional) Enables or disables the suppression type.
unicast	(Optional) Specifies unicast suppression.

Defaults

The default is 100% (no broadcast limit).

The default action is **drop-packets** if a broadcast violation occurs.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

You can enter the threshold value in two ways:

- A decimal number followed by a percent sign (for example 0.33%)
- A whole number followed by a percent sign (for example 33%)

The percent sign (%) is required when entering the threshold value.

The **multicast** and **unicast** keywords are supported on Gigabit Ethernet modules only.

If you enter the command without using the **multicast** or **unicast** keyword, only broadcast traffic is suppressed. If you enter the **multicast** or **unicast** keyword, both broadcast and the selected traffic type are suppressed.

Examples

This example shows how to limit broadcast traffic to 20 percent:

```
Console> (enable) set port broadcast 4/3 20%
Port 4/3 broadcast traffic limited to 20.00%.
Console> (enable)
```

This example shows how to limit broadcast traffic to 90 percent and to errdisable when suppression occurs:

```
Console> (enable) set port broadcast 4/6 90% violation errdisable
Port 4/6 broadcast traffic limited to 90.00%.
On broadcast suppression port 4/6 is configured to move to errdisabled state.
Console> (enable)
```

This example shows how to allow a specific amount of multicast traffic to a range of ports:

```
Console> (enable) set port broadcast 4/1-24 80% multicast enable
Port 4/1-24 multicast traffic limited to 80%.
Console> (enable)
```

This example shows how to limit broadcast and multicast traffic to 91 percent, to disable unicast traffic, and to errdisable when suppression occurs:

```
Console> (enable) set port broadcast 4/2 91% violation errdisable multicast enable unicast
disable
Port 4/2 broadcast and multicast traffic limited to 91.00%.
On broadcast suppression port 4/2 is configured to move to errdisabled state.
Console> (enable)
```

This example shows how to limit broadcast, multicast, and unicast traffic to 91 percent:

```
Console> (enable) set port broadcast 4/2 91% multicast enable unicast enable
Port 4/2 broadcast, multicast and unicast traffic limited to 91.00%.
Console> (enable)
```

Related Commands

clear port broadcast
show port broadcast

set port channel

To configure EtherChannel on Ethernet module ports, use the **set port channel** command.

set port channel *mod/port* [*admin_group*]

set port channel *mod/port* **mode** {**on** | **off** | **desirable** | **auto**} [**silent** | **non-silent**]

set port channel all mode off

set port channel all distribution {**ip** | **mac**} [**source** | **destination** | **both**]

set port channel all distribution {**session**} [**source** | **destination** | **both**]

set port channel all distribution {**ip-vlan-session**} [**source** | **destination** | **both**]

Syntax Description

mod/port	Number of the module and the port on the module.
admin_group	(Optional) Number of the administrative group; valid values are from 1 to 1024.
mode	Specifies the EtherChannel mode.
on	Enables and forces specified ports to channel without PAgP.
off	Prevents ports from channeling.
desirable	Sets a PAgP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending PAgP packets.
auto	Sets a PAgP mode that places a port into a passive negotiating state, in which the port responds to PAgP packets it receives, but does not initiate PAgP packet negotiation.
silent	(Optional) Uses with **auto** or **desirable** when no traffic is expected from the other device to prevent the link from being reported to STP as down.
non-silent	(Optional) Uses with **auto** or **desirable** when traffic is expected from the other device.
all mode off	Turns off channeling on all ports globally.
all distribution	Applies frame distribution to all ports in the Catalyst 6500 series switch.
ip	Specifies the frame distribution method using IP address values.
mac	Specifies the frame distribution method using MAC address values.
source	(Optional) Specifies the frame distribution method using source address values.
destination	(Optional) Specifies the frame distribution method using destination address values.
both	(Optional) Specifies the frame distribution method using source and destination address values.
session	Allows frame distribution of Layer 4 traffic.
both	(Optional) Specifies the frame distribution method using source and destination Layer 4 port number.
ip-vlan-session	Specifies the frame distribution method based on the source or destination IP address, the forwarding index derived from the VLAN, and the source or destination Layer 4 port.

Defaults

The default is EtherChannel is set to **auto** and **silent** on all module ports. The defaults for frame distribution are **ip** and **both**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

This command is not supported by non-EtherChannel-capable modules.

The **set port channel all distribution session** command is supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) and the Supervisor Engine 720.

Make sure that all ports in the channel are configured with the same port speed, duplex mode, and so forth. For more information on EtherChannel, refer to the *Catalyst 6500 Series Software Configuration Guide*.

With the **on** mode, a usable EtherChannel exists only when a port group in **on** mode is connected to another port group in **on** mode.

If you are running QoS, make sure that bundled ports are all of the same trust types and have similar queueing and drop capabilities.

Disable the port security feature on the channeled ports (see the **set port security** command). If you enable port security for a channeled port, the port shuts down when it receives packets with source addresses that do not match the secure address of the port.

You can configure up to eight ports on the same switch in each administrative group.

When you assign ports to an existing administrative group, the original ports associated with the administrative group will move to a new automatically picked administrative group. You cannot add ports to the same administrative group.

If you do not enter an *admin_group* value, a new administrative group is created with the *admin_group* value selected automatically. The next available administrative group is automatically selected.

If you do not enter the channel mode, the channel mode of the ports addressed are not modified.

The **silent | non-silent** parameters only apply if **desirable** or **auto** modes are entered.

If you do not specify **silent** or **non-silent**, the current setting is not affected.

The **ip-vlan-session** keyword is supported only on the Supervisor Engine 720.

Note With software releases 6.2(1) and earlier, the 6- and 9-slot Catalyst 6500 series switches support a maximum of 128 EtherChannels.

With software releases 6.2(2) and later, due to the port ID handling by the spanning tree feature, the maximum supported number of EtherChannels is 126 for a 6- or 9-slot chassis and 63 for a 13-slot chassis. Note that the 13-slot chassis was first supported in software release 6.2(2).

Examples

This example shows how to set the channel mode to **desirable**:

```
Console> (enable) set port channel 2/2-8 mode desirable
Ports 2/2-8 channel mode set to desirable.
Console> (enable)
```

This example shows how to set the channel mode to **auto**:

```
Console> (enable) set port channel 2/7-8,3/1 mode auto
Ports 2/7-8,3/1 channel mode set to auto.
Console> (enable)
```

This example shows how to group ports 4/1 through 4 in an administrative group:

```
Console> (enable) set port channel 4/1-4 96
Port(s) 4/1-4 are assigned to admin group 96.
Console> (enable)
```

This example shows the display when the port list is exceeded:

```
Console> (enable) set port channel 2/1-9 1
No more than 8 ports can be assigned to an admin group.
Console> (enable)
```

This example shows how to disable EtherChannel on module 4, ports 4 through 6:

```
Console> (enable) set port channel 4/4-6 mode off
Port(s) 4/4-6 channel mode set to off.
Console> (enable)
```

This example shows the display output when you assign ports to an existing administrative group. This example moves ports in admin group 96 to another admin group and assigns ports 4/4 through 6 to admin group 96:

```
Console> (enable) set port channel 4/4-6 96
Port(s) 4/1-3 are moved to admin group 97.
Port(s) 4/4-6 are assigned to admin group 96.
Console> (enable)
```

This example shows how to set the channel mode to **off** for ports 4/4 through 6 and assign ports 4/4 through 6 to an automatically selected administrative group:

```
Console> (enable) set port channel 4/4-6 off
Port(s) 4/4-6 channel mode set to off.
Port(s) 4/4-6 are assigned to admin group 23.
Console> (enable)
```

This example shows how to configure the EtherChannel load-balancing feature:

```
Console> (enable) set port channel all distribution ip destination
Channel distribution is set to ip destination.
Console> (enable)
```

Related Commands

show channel
show channel group
show port channel

set port cops

To create port roles, use the **set port cops** command.

set port cops *mod/port* **roles** *role1* [*role2*]...

Syntax Description

mod/port	Number of the module and the port on the module.
roles *role#*	Specifies the roles.

Defaults

The default is all ports have a default role of null string, for example, the string of length 0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

A port may have multiple roles. You can configure a maximum of 64 total roles per switch. You can specify multiple roles in a single command.

Examples

This example shows how to create roles on a port:

```
Console> (enable) set port cops 3/1 roles backbone_port main_port
New role 'backbone_port' created.
New role 'main_port' created.
Roles added for port 3/1-4.
Console> (enable)
```

This example shows the display if you attempt to create a roll and exceed the maximum allowable number of roles:

```
Console> (enable) set port cops 3/1 roles access_port
Unable to add new role. Maximum number of roles is 64.
Console> (enable)
```

Related Commands

clear port cops
show port cops

8.6 EFT Copy

set port critical

To enable or disable the Inaccessible Authentication Bypass (IAB) feature on a port that is configured to use 802.1X, LPIP, MAC authentication bypass, or Web Authentication, use the **set port critical** command.

set port critical *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables IAB on the specified port.
disable	Disables IAB on the specified port.

Defaults

IAB is disabled.

Command Types

Switch.

Command Modes

Privileged.

Usage Guidelines

Use the **set port critical** command in place of the **set port dot1x** *mod/port* **critical** command.

Examples

This example show how to enable IAB on port 1, module 5:

```
Console> (enable) set port critical 5/1 enable
Port, 5/1 Critical feature enabled.
Console> (enable)
```

Related Commands

show port critical
show port mac-auth-bypass
show port web-auth

set port debounce

To enable or disable the debounce timer or configure the timer setting on a per-port basis, use the **set port debounce** command.

set port debounce *mod/port* {**enable** | **disable**}

set port debounce *mod/port* **delay** *time*

Syntax Description

mod/port	Number of the module and the port on the module.
enable | **disable**	Enables or disables the debounce timer.
delay	Sets the debounce timer for gigabit fiber ports.
time	Amount of time the firmware waits before notifying the supervisor engine of a link change; valid values are 200 milliseconds or from 300 to 5000 milliseconds. This is supported on gigabit fiber ports only. See the "Usage Guidelines" section for more information.

Defaults

By default, the debounce timer is disabled on all ports.

When the debounce timer is disabled, the default debounce timer values are as follows:

- 10BASE-FL ports—300 milliseconds
- 10/100BASE-TX ports —300 milliseconds
- 100BASE-FX ports—300 milliseconds
- 10/100/1000BASE-TX ports—300 milliseconds
- 1000BASE-TX ports—300 milliseconds
- Fiber Gigabit Ethernet ports—10 milliseconds
- 10-Gigabit Ethernet ports—10 milliseconds

When the debounce timer is enabled, the default debounce timer values are as follows:

- 10BASE-FL ports—3100 milliseconds
- 10/100BASE-TX ports —3100 milliseconds
- 100BASE-FX ports—3100 milliseconds
- 10/100/1000BASE-TX ports—3100 milliseconds
- 1000BASE-TX ports—3100 milliseconds
- Fiber Gigabit Ethernet ports—100 milliseconds
- 10-Gigabit Ethernet ports—100 milliseconds

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The debounce timer is the time the firmware waits before notifying the supervisor engine of a link change at the physical layer.

Setting the debounce timer value to 200 milliseconds or from 300 to 5000 milliseconds is possible only for gigabit fiber ports. You do not need to enable the debounce timer on a gigabit fiber port before adjusting the timer. Any timer value that is greater than the default value in disabled state is considered a value that enables the timer.

For 10/100 ports and 100BASE-FX ports in the disabled state, the firmware may take up to 600 milliseconds to notify the supervisor engine of a link change because the firmware polling time is every 300 milliseconds.

For 10/100 ports and 100BASE-FX ports in the enabled state, the firmware may take up to 3400 milliseconds to notify the supervisor engine of a link change because the firmware polling time is every 300 milliseconds.

Examples

This example shows how to enable the debounce timer for a specific port on a specific module:

```
Console> (enable) set port debounce 1/1 enable
Debounce is enabled on port 1/1.
Warning:Enabling port debounce causes Link Up/Down detections to be delayed.
It results in loss of data traffic during debouncing period, which might
affect the convergence/reconvergence of various Layer 2 and Layer 3
protocols.
Use with caution.
Console> (enable)
```

Related Commands

show port debounce

set port description

To include a description that identifies a port, use the **set port description** command.

set port description *mod/port* [*port_description*]

Syntax Description

mod/port	Number of the module and the port on the module.
port_description	(Optional) Description that identifies the specified port. See the "Usage Guidelines" section for more information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set port description** command adds another 43 characters to the existing limit of 21 characters that can be set when you enter the **set port name** command.

The **set port description** command is only supported in text configuration mode.

If you do not enter a *port_description* argument, the port description is cleared.

Examples

This example shows how to include a port description:

```
Console> (enable) set port description 7/1 sarahtom 172.30.8.35 00-0a-5e-44-8b-8 2/2
Port 7/1 description set.
Console> (enable)
```

This example shows how to clear a port description:

```
Console> (enable) set port description 7/1
Port 7/1 description cleared.
Console> (enable)
```

Related Commands

set port name
show config mode
show port description

set port dhcp-snooping

To configure DHCP snooping on a port, use the **set port dhcp-snooping** command.

set port dhcp-snooping *mod/port* {**trust** | **source-guard**} {**enable** | **disable**}

set port dhcp-snooping *mod/port* **binding-limit** *count*

set port dhcp-snooping *mod/port* **add-binding** *ip-addr mac-addr* [*vlan*]

Syntax Description

mod/port	Number of the module and port on the module.
trust	Specifies the trust feature.
source-guard	Specifies the IP Source-Guard feature.
enable	Enables the specified DHCP-Snooping feature.
disable	Disables the specified DHCP-Snooping feature.
binding-limit	Specifies the number of IP-to-MAC bindings that are allowed on a port.
count	Number of bindings that are allowed on a port; valid values are from 1 to 100.
add-binding	Adds an IP-to-MAC binding.
ip-addr	IP address.
mac-addr	MAC address.
vlan	(Optional) Number of the VLAN.

Defaults

Trust and source-guard are disabled.

The binding limit on a port is 32.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter the **set port dhcp-snooping** *mod/ports* **trust disable** command, the DHCP snooping feature performs checks on packets coming from the ports that you specify. If you enter the **enable** keyword, the feature trusts the packets from those ports and does not perform checks.

If you enter the **set port dhcp-snooping** *mod/ports* **source-guard enable** command, the IP addresses learned through DHCP snooping are the only source IP addresses allowed on incoming traffic. All packets that contain other IP addresses are dropped. If a new binding is added, the IP address associated with that binding is added to the port. If a binding is deleted, the IP address associated with that binding is removed from the port.

If DHCP snooping is disabled on a VLAN, the bindings for that VLAN are deleted.

If you enable IP Source Guard on a port, that port should be untrusted. Also, the security ACL mode should be port-based or merge-mode, and no PACLs should be on the port.

8.6 EFT Copy

IP source guard is supported only on the PFC3 or later.

Note the following when configuring DHCP-related features:

- ARP inspection is supported on Supervisor Engine 2, Supervisor Engine 720, and Supervisor Engine 32, but not on Supervisor Engine 1.
- DHCP snooping is supported on all supervisor engines.
- IP Source Guard is supported on Supervisor Engine 720 and Supervisor Engine 32, but not on Supervisor Engine 1 or Supervisor Engine 2.
- Dynamic ARP Inspection is support on Supervisor Engine 2, Supervisor Engine 720, and Supervisor Engine 32, but not on Supervisor Engine 1.
- You must configure DHCP snooping on a server port when configured on per-port basis. The server port must be trusted.
- You can enable IP source guard only when the ACL mode is port based.

Examples

This example shows how to enable DHCP trust on port 2 of module 2:

```
Console> (enable) set port dhcp-snooping 2/2 trust enable
Port(s)  2/2 state set to trusted for DHCP Snooping.
Console> (enable)
```

This example shows how to enable IP source-guard on port 2 of module 2:

```
Console> (enable) set port dhcp-snooping 2/2 source-guard enable
Enabling IP Source Guard on port(s) 2/2.
Console> (enable)
```

This example shows how to limit the number of bindings to 48 on port 4 and port 5 of module 3:

```
Console> (enable) set port dhcp-snooping 3/4-5 binding-limit 48
Ports 3/4-5 DHCP snooping binding limit is set to 48
Console> (enable)
```

This example show how to add a binding to a specified port:

```
<need example>
```

Related Commands

clear dhcp-snooping bindings
show port dhcp-snooping

set port disable

To disable a port or a range of ports, use the **set port disable** command.

set port disable *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

The default system configuration has all ports enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

It takes approximately 30 seconds for this command to take effect.

Examples

This example shows how to disable a port using the **set port disable** command:

```
Console> (enable) set port disable 5/10
Port 5/10 disabled.
Console> (enable)
```

Related Commands

set port enable
show port

set port dot1q-all-tagged

To enable the 802.1Q tagging feature on specific ports, use the **set port dot1q-all-tagged** command.

set port dot1q-all-tagged {*mod/port*} {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables the dot1q-all-tagged feature.
disable	Disables the dot1q-all-tagged feature.

Defaults

The 802.1Q tagging feature is enabled on a per-port basis. See the "Usage Guidelines" section for more information.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Although 802.1Q tagging is enabled by default on a per-port basis, tagging only takes effect when you enable the feature globally by entering the **set dot1q-all-tagged enable** command. When the global command is enabled, if you do not want tagging on a specific port, you must disable the feature on that port.

Examples

This example shows how to enable the dot1q tagging feature on specific ports:

```
Console> (enable) set port dot1q-all-tagged 1/1-2 enable
Packets on native vlan will be tagged on port(s) 1/1-2.
Console> (enable)
```

This example shows how to enable the dot1q tagging feature on all ports:

```
Console> (enable) set port dot1q-all-tagged all enable
Packets on native vlan will be tagged on all applicable ports.
Console> (enable)
```

This example shows how to disable the dot1q tagging feature on specific ports:

```
Console> (enable) set port dot1q-all-tagged 1/1-2 disable
Packets on native vlan will not be tagged for port(s) 1/1-2.
Console> (enable)
```

This example shows how to disable the dot1q tagging feature on all ports:

```
Console> (enable) set port dot1q-all-tagged all disable
Packets on native vlan will not be tagged on all applicable ports.
Console> (enable)
```

Related Commands

set dot1q-all-tagged
show dot1q-all-tagged
show port dot1q-all-tagged

set port dot1q-ethertype

To set the EtherType field in the IEEE 802.1Q tag to a custom value, use the **set port dot1q-ethertype** command.

set port dot1q-ethertype *mod/port* {*value* | **default**}

Syntax Description

mod/port	Number of the module and the port on the module.
value	Hexadecimal number of the two-byte EtherType field.
default	Specifies the default value of 0x8100 for the two-byte EtherType field.

Defaults

The EtherType field is set to **default**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you specify a custom EtherType field, your network can support Cisco and non-Cisco switches that do not use the standard 0x8100 EtherType to identify 802.1Q-tagged frames. When you specify a custom EtherType field, you can identify 802.1Q tagged frames and switch the frames to a specified VLAN. The two bytes immediately following the EtherType are interpreted as a standard 802.1Q tag. Specify the value of the two-byte EtherType field as a hexadecimal number.

To return the custom EtherType field to the default value (0x8100), use the **set port dot1q-ethertype** *mod/port* **default** command.

Note A custom 802.1Q EtherType field is supported on the following modules only: Supervisor Engine 2 and Supervisor Engine 720 uplink ports, WS-X6516-GBIC, WS-X6516A-GBIC, WS-X6516-GE-TX, WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6748-GE-TX, WS-X6724-SFP, WS-X6704-10GE, WS-X6501-10GEX4, and WS-X6502-10GE.

Note EtherChannels do not support a custom 802.1Q EtherType field. If you configure a port with a custom 802.1Q EtherType field, the port cannot join a channel. If a channel is already configured, you cannot change the 802.1Q EtherType on any of the channel ports.

Note On the WS-X6516A-GBIC, WS-X6516-GBIC, and WS-X6548-GE-TX modules, if you configure a port with a custom 802.1Q EtherType in the port groups 1 through 8 or 9 through 16, all ports in the group are configured with the custom 802.1Q EtherType. On the WS-X6516-GE-TX module, if you configure a port with a custom 802.1Q EtherType in the port groups 1 through 4, 5 through 8, 9 through 12, or 13 through 16, all ports in the group are configured with the custom 802.1Q EtherType.

Note You can use a custom 802.1Q EtherType field on trunk ports, 802.1Q access ports, and 802.1Q/802.1p multi-VLAN access ports. Additionally, you should configure the custom EtherType value the same on both ends of a link.

Examples

This example shows how to set the 802.1Q EtherType to 0x1234 on module 2, port 1:

```
Console> (enable) set port dot1q-ethertype 2/1 1234
All the group ports 2/1-2 associated with port 2/1 will be modified.
Do you want to continue (y/n) [n]?y
Dot1q Ethertype value set to 0x1234 on ports 2/1-2.
Console> (enable)
```

This example shows how to return the 802.1Q EtherType field to the standard EtherType field (0x8100) on module 2, port 1:

```
Console> (enable) set port dot1q-ethertype 2/1 default
All the group ports 2/1-2 associated with port 2/1 will be modified.
Do you want to continue (y/n) [n]?y
Dot1q Ethertype value set to 0x8100 on ports 2/1-2.
Console> (enable)
```

Related Commands

show port dot1q-ethertype

set port dot1qtunnel

To configure the dot1q tunnel mode for the port, use the **set port dot1qtunnel** command.

set port dot1qtunnel *mod/port* {**access** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
access	Turns off the port trunking mode.
disable	Disables dot1q tunneling.

Defaults

Dot1q tunnel mode is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You cannot enable the dot1q tunneling feature on a port until dot1q-tagged-only mode is enabled.

You cannot disable dot1q-tagged-only mode on the switch until dot1q tunneling is disabled on all the ports on the switch.

You cannot set the dot1q tunnel mode to access if port security is enabled.

You cannot set the dot1q tunnel mode to access on a port with an auxiliary VLAN configured.

An interconnected network can have redundant paths to the same edge switch of ISP, but it cannot have redundant paths to two different edge switches of ISP.

Note PBF does not work with 802.1Q tunnel traffic. PBF is supported on Layer 3 IP unicast traffic, but it is not applicable to Layer 2 traffic. At the intermediate (PBF) switch, all 802.1Q tunnel traffic appears as Layer 2 traffic.

If you enable dot1q-tagged globally, the dot1q-tagged per-port setting controls whether or not the frames are tagged. If you disable dot-1q-tagged globally, the default group is never tagged and the per-port setting has no effect.

Examples

This example shows how to set dot1q tunneling on the port to access:

```
Console> (enable) set port dot1qtunnel 4/1 access
Dot1q tunnel feature set to access mode on port 4/1.
Port 4/2 trunk mode set to off.
Console> (enable)
```

This example shows the output if you try to turn on trunking on a port that has dot1q tunneling mode set:

```
Console> (enable) set trunk 4/1 on
Failed to set port 4/1 to trunk mode on.
The dot1q tunnel mode for the port is currently set to access.
Console> (enable)
```

Related Commands

show port dot1qtunnel

8.6 EFT Copy

set port dot1x

To configure 802.1X on a port, use the **set port dot1x** command.

set port dot1x *mod/port* **multiple-host** {**enable** | **disable**}

set port dot1x *mod/port* **port-control** *port_control_value*

set port dot1x *mod/port* **initialize**

set port dot1x *mod/port* **re-authenticate**

set port dot1x *mod/port* **re-authentication** {**enable** | **disable**}

set port dot1x *mod/port* **multiple-authentication** {**enable** | **disable**}

set port dot1x *mod/port* **guest-vlan** {*vlan* | **none**}

set port dot1x *mod/port* **shutdown-timeout** {**enable** | **disable**}

set port dot1x *mod/port* **port-control-direction** {**both** | **in**}

set port dot1x *mod/port* **auth-fail-vlan** {*vlan* | **none**}

set port dot1x *mod/port* **critical** {**enable** | **disable**}

set port dot1x *mod/port* **re-authperiod server** {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and port on the module.
multiple-host	Specifies multiple-user access; see the “Usage Guidelines” section for more information.
enable	Enables multiple-user access.
disable	Disables multiple-user access.
port-control *port_control_value*	Specifies the port control type; valid values are **force-authorized**, **force-unauthorized**, and **auto**.
initialize	Initializes 802.1X on the port.
re-authenticate	Manually initiates a reauthentication of the entity connected to the port.
re-authentication	Automatically initiates reauthentication of the entity connected to the port within the reauthentication time period; see the “Usage Guidelines” section for more information.
enable	Enables automatic reauthentication.
disable	Disables automatic reauthentication.
multiple-authentication	Specifies multiple authentications so that more than one host can gain access to the port; see the “Usage Guidelines” section for more information.
enable	Enables multiple authentication.
disable	Disables multiple authentication.
guest-vlan	Specifies an active VLAN as an 802.1X guest VLAN.
vlan	Number of the VLAN; valid values are from 1 to 4094.

none	Clears the guest VLAN on the port.
shutdown-timeout	Specifies the shutdown-timeout period for a port after a security violation. See the "Usage Guidelines" section for more information.
enable	Activates the automatic reenabling of a port after the shutdown timeout period.
disable	Deactivates the automatic reenabling of a port after the shutdown timeout period.
port-control-direction	Specifies the traffic control direction on a port.
both	Blocks traffic in both directions.
in	Blocks traffic only in the incoming direction.
auth-fail-vlan	Sets the VLAN that provides limited access to end hosts that have failed 802.1X authentication. See the "Usage Guidelines" section for more information.
none	Clears the authentication failure VLAN on a port.
critical	Sets the 802.1X port as a critical port. See the "Usage Guidelines" section for more information.
enable	Enables the critical option on the 802.1X port.
disable	Disables the critical option on the 802.1X port.
re-authperiod server	Sets session timeout override on the 802.1X port. See the "Usage Guidelines" section for more information.
enable	Applies the session timeout value that is received from the RADIUS server.
disable	Applies the reauthentication period value that was configured through the CLI.

Defaults

The default settings are as follows:

- The multiple host feature is disabled.
- The *port_control_value* is set to **force-authorized**.
- The reauthentication feature is disabled.
- The multiple authentication feature is disabled.
- The guest VLAN feature is set to **none**.
- The shutdown-timeout feature is disabled.
- The port control direction is set to **both**.
- The **auth-fail-vlan** VLAN is set to **none**.
- The **critical** option is disabled.
- The **re-authperiod server** option is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The 802.1X port will not be allowed to become a trunk port, MVAP, channel port, dynamic port, or a secure port.

When setting the port control type, the following applies:

- **force-authorized** forces the controlled port to transition to the authorized state unconditionally and is equivalent to disabling 802.1X restriction in the port.
- **force-unauthorized** forces the controlled port to transit to the unauthorized state unconditionally and prevents the authorized services of the authenticator to the supplicant.
- **auto** enables 802.1X control on the port.

If you disable the multiple host feature, once a 802.1X port is authorized through a successful authentication of a supplicant, only that particular host (MAC address) is allowed on that port. When the system detects another host (different MAC address) on the authorized port, it shuts down the port and displays a syslog message. This is the default system behavior.

If you enable the multiple host feature, once a 802.1X port is authorized through a successful authentication of a supplicant, any host (any MAC address) is allowed to send or receive traffic on that port.

If you enable reauthentication, you can set the reauthentication time period in seconds by entering the **set dot1x re-authperiod** *seconds* command. The default for the reauthentication time period is 3600 seconds.

You can enable either multiple host mode or multiple authentication mode.

On an 802.1X-enabled port, an administratively configured VLAN cannot be equal to an auxiliary VLAN.

To specify the number of seconds that a port is shut down after a security violation, enter the **set dot1x shutdown-timeout** command. Then enter the **set port dot1x** *mod/port* **shutdown-timeout enable** command to activate automatic reenabling of the port after the shutdown-timeout period has elapsed.

If you enter the **set port dot1x** *mod/port* **port-control-direction in** command, all incoming traffic is dropped. If you enter the **set port dot1x** *mod/port* **port-control-direction both** command, all incoming and outgoing traffic is dropped.

When you configure 802.1X unidirectional or bidirectional ports, follow these guidelines:

- Auxiliary VLANs—To support auxiliary VLANs on a port when you configure the port as a unidirectional port, the auxiliary VLAN is moved to the spanning tree “forwarding” state to ensure that the connected IP phone is operational immediately. To prevent any disturbance of the incoming traffic, initially the port VLAN is also moved to the spanning tree “forwarding” state and then if any traffic is seen on the port VLAN, the port is moved to the spanning tree “blocking” state to drop all additional traffic. The connected host is then requested to get authorized to send any traffic.
- Guest VLANs—Guest VLANs are supported only on ports configured as bidirectional ports. If a guest VLAN is enabled on a port, that port cannot be configured as a unidirectional port and vice versa.
- Port mode—The port mode (single-authentication mode, multiple-host mode, or multiple-authentication mode) for a port configured as a unidirectional port must be single-authentication mode (the default port mode).

You can provide limited access to an end host that does not have valid credentials for 802.1X authentication. After three failed attempts at authentication, the end host will obtain network connectivity through a VLAN that you configure for users that fail authentication. To configure this VLAN, enter the **set port dot1x** *mod/port* **auth-fail-vlan** *vlan* command. To disable this feature, enter the **set port dot1x** *mod/port* **auth-fail-vlan none** command.

When configuring the authentication failure VLAN, follow these configuration guidelines and be aware of these restrictions:

- After three failed 802.1X authentication attempts by the supplicant, the port is moved to the authentication failure VLAN where the supplicant can access the network. These three attempts introduce a delay of 3 minutes before the port is enabled in the authentication failure VLAN and the EAP success packet is sent to the supplicant (1 minute per failed attempt based on the default quiet period of 60 seconds after each failed attempt).
- The number of failed 802.1X authentication attempts is counted from the time of the linkup to the point where the port is moved into the authentication failure VLAN. When the port moves into the authentication failure VLAN, the failed-attempts counter is reset.
- Only the authenticated-failed users are moved to the authentication failure VLAN.
- The authentication failure VLAN is supported only in the single-authentication mode (the default port mode).
- The authentication failure VLAN is not supported on a port that is configured as a unidirectional port.
- The supplicant's MAC address is added to the CAM table and only its MAC address is allowed on the authentication failure VLAN port. Any new MAC address that appears on the port is treated as a security violation.
- The authentication failure VLAN port cannot be part of an RSPAN VLAN or a private VLAN.
- On multiple VLAN access ports (MVAPs), the authentication failure VLAN and the auxiliary VLAN cannot be the same.
- The authentication failure VLAN and port security features do not conflict with each other. Additionally, other security features such as Dynamic ARP Inspection (DAI), Dynamic Host Configuration Protocol (DHCP) snooping, and IP source guard can be enabled and disabled independently on the authentication failure VLAN.
- The authentication failure VLAN is independent of the guest VLAN. However, the guest VLAN can be the same VLAN as the authentication failure VLAN. If you do not want to differentiate between the non-802.1X-capable hosts and the authentication-failed hosts, you may configure both to the same VLAN (either a guest VLAN or an authentication failure VLAN).
- High availability is supported with the authentication failure VLAN.

When you enter the **set port dot1x** *mod/port* **critical enable** command, 802.1X still attempts to authenticate the specified port in the normal way. However, if attempts to reach the authentication server fail, the port is still given access to the network in the administratively-configured VLAN or in the native VLAN of the port. A port can only be configured as a critical port if it is in single-authentication mode.

After a critical port has been given access to the network, if the authentication server becomes available, the critical port returns to the unauthorized state. The normal authentication process is restarted, and after the port is authenticated, it is moved into the RADIUS server-specified VLAN. At this point, you need to initialize the port manually by entering the **set port dot1x** *mod/port* **initialize** command.

If the authentication server goes down after a host has already been authenticated through the normal authentication process, the switch checks to see if the port is a critical port. If the port is a critical port, the normal reauthentication process is temporarily disabled for the port. The port is given network access until the authentication server becomes active and restarts the authentication process.

By default, the session timeout value from the RADIUS server takes precedence over the reauthentication value that is configured by entering **set dot1x** **re-authperiod** *seconds*. With the session timeout override option, you can specify on a per-port basis which timeout value has is applied. If session timeout override is enabled, the session timeout value from the RADIUS server is applied. If session timeout override is disabled, the configured reauthentication value is applied.

Examples

This example shows how to set the port control type automatically:

```
Console> (enable) set port dot1x 4/1 port-control auto
Port 4/1 dot1x port-control is set to auto.
Console> (enable)
```

This example shows how to initialize 802.1X on a port:

```
Console> (enable) set port dot1x 4/1 initialize
dot1x port 4/1 initializing...
dot1x initialized on port 4/1.
Console> (enable)
```

This example shows how to manually reauthenticate a port:

```
Console> (enable) set port dot1x 4/1 re-authenticate
dot1x port 4/1 re-authenticating...
dot1x re-authentication successful...
dot1x port 4/1 authorized.
Console> (enable)
```

This example shows how to enable multiple-user access on a specific port:

```
Console> (enable) set port dot1x 4/1 multiple-host enable
Multiple hosts allowed on port 4/1.
Console> (enable)
```

This example shows how to enable automatic reauthentication on a port:

```
Console> (enable) set port dot1x 4/1 re-authentication enable
Port 4/1 re-authentication enabled.
Console> (enable)
```

This example shows how to activate automatic reenabling of a port after the shutdown-timeout period has elapsed:

```
Console> (enable) set port dot1x 2/1 shutdown-timeout enable
Dot1x shutdown_timeout enabled
Console> (enable)
```

This example shows how to configure a port to drop all incoming traffic:

```
Console> (enable) set port dot1x 3/1 port-control-direction in
Port 3/1 Port Control Direction set to In.
Console> (enable)
```

This example shows how to configure a port to drop both incoming and outgoing traffic:

```
Console> (enable) set port dot1x 3/1 port-control-direction both
Port 3/1 Port Control Direction set to Both.
Console> (enable)
```

This example shows how to specify a VLAN on a port for users that have failed 802.1X authentication:

```
Console> (enable) set port dot1x 3/33 auth-fail-vlan 81
Port 3/33 Auth Fail Vlan is set to 81
Console> (enable)
```

This example shows how to disable the 802.1X authentication failure VLAN feature on a port:

```
Console> (enable) set port dot1x 2/1 auth-fail-vlan none
Port 2/1 Auth Fail Vlan is cleared
Console> (enable)
```

This example shows how to specify a port as a critical port:

```
Console> (enable) set port dot1x 5/48 critical enable
Port 5/48 critical-port option is enabled
Console> (enable)
```

This example shows how to apply the session timeout value that is received from the RADIUS server on a port:

```
Console> (enable) set port dot1x 5/10 re-authperiod server enable
Port 5/10 session-timeout-override option is enabled
Console> (enable)
```

Related Commands

set dot1x
show dot1x
show port dot1x

set port duplex

To configure the duplex type of an Ethernet port or a range of ports, use the **set port duplex** command.

set port duplex *mod/port* {**full** | **half**}

Syntax Description

mod/port	Number of the module and the port on the module.
full	Specifies full-duplex transmission.
half	Specifies half-duplex transmission.

Defaults

The default configuration for 10-Mbps and 100-Mbps modules has all Ethernet ports set to half duplex.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure Ethernet and Fast Ethernet interfaces to either full duplex or half duplex.

The **set port duplex** command is not supported on Gigabit Ethernet ports. Gigabit Ethernet ports support full-duplex mode only.

If the transmission speed on a 16-port RJ-45 Gigabit Ethernet port is set to 1000, duplex mode is set to full. If the transmission speed is changed to 10 or 100, the duplex mode stays at full. You must configure the correct duplex mode when transmission speed is changed to 10 or 100 from 1000.

Examples

This example shows how to set port 1 on module 2 to full duplex:

```
Console> (enable) set port duplex 2/1 full
Port 2/1 set to full-duplex.
Console> (enable)
```

Related Commands

show port

set port enable

To enable a port or a range of ports, use the **set port enable** command.

set port enable *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

The default is all ports are enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

It takes approximately 30 seconds for this command to take effect.

Examples

This example shows how to enable port 3 on module 2:

```
Console> (enable) set port enable 2/3
Port 2/3 enabled.
Console> (enable)
```

Related Commands

set port disable
show port

set port eou

To configure Extensible Authentication Protocol over User Datagram Protol (EoU) on a per-port basis, use the **set port eou** command.

set port eou *mod/port* {**bypass** | **enable** | **disable**}

set port eou *mod/port* **initialize**

set port eou *mod/port* **revalidate**

set port eou *mod/port* **aaa-fail-policy** *policy-name*

Syntax Description

mod/port	Number of the module and the port on the module.
bypass	Bypasses EoU on a specified port.
enable	Enables EoU on a specified port.
disable	Disables EoU on a specified port.
initialize	Initializes EoU for hosts on a specified port.
revalidate	Revalidates EoU credentials for hosts on a specified port.
aaa-fail-policy	Maps an AAA fail policy for EoU to a specified port.
policy-name	Policy name to be mapped to the port.

Defaults

EoU is disabled on a port.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Before you can use the **set port eou** *mod/port* **aaa-fail-policy** *policy-name* command, the template for the policy must be created.

After you have specified a policy template for a port, any changes to the policy template affect only those hosts that have been moved to AAA fail state after the policy template was changed. Hosts in already existing sessions use the policy template that was in place before any changes were made.

When you specify a different policy for a port, hosts in already existing sessions maintain the previously specified policy. The newly specified policy affects only new hosts entering AAA fail state.

Examples

This example shows how to enable EoU on a specified port:

```
Console> (enable) set port eou 5/3 enable
EoU LPIP enabled on port 5/3
Console> (enable)
```

This example shows how to initialize EoU for hosts on specified ports:

```
Console> (enable) set port eou 3/1-5 initialize
EoU LPIP restarted for ports 3/1-5
Console> (enable)
```

This example shows how to revalidate EoU credentials on specified ports:

```
Console> (enable) set port eou 3/1-5 revalidate
EoU LPIP revalidation started for ports 3/1-5
Console> (enable)
```

Related Commands

clear eou
set eou
set security acl ip
show eou
show port eou

set port errdisable-timeout

To prevent an errdisabled port from being enabled, use the **set port errdisable-timeout** command.

set port errdisable-timeout *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables errdisable timeout.
disable	Disables errdisable timeout.

Defaults

By default, the errdisable timeout for each port is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When the global timer times out, the port will be reenabled. Use the **set port errdisable-timeout** command if you want the port to remain in the errdisabled state.

Examples

This example shows how to prevent port 3/3 from being enabled when it goes into errdisabled state:

```
Console> (enable) set port errdisable-timeout 3/3 disable
Successfully disabled errdisable-timeout for port 3/3.
Console> (enable)
```

Related Commands

set errdisable-timeout
show errdisable-timeout
show port errdisable-timeout

set port errordetection

To enable or disable link error monitoring on an EtherChannel port, use the **set port errordetection** command.

set port errordetection *mod/port* {**inerrors** | **rxcrc** | **txcrc**} {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
inerrors	Specifies monitoring for inerrors on the port.
rxcrc	Specifies monitoring for RXCRC (CRCAlignErrors) errors on the port.
txcrc	Specifies monitoring for TXCRC errors on the port.
enable	Enables monitoring.
disable	Disables monitoring.

Defaults

- Monitoring for inerrors is disabled.
- Monitoring for RXCRC and TXCRC errors is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

All ports in an EtherChannel should have the same port error-detection settings.

Examples

This example shows how to enable RXCRC port error detection on port 3/1:

```
Console> (enable) set port errordetection 3/1 rxcrc enable
Port(s)  3/1 set to errordetection rxcrc enable.
Console> (enable)
```

Related Commands

set errordetection
show errordetection
show port errordetection

set port ethernet-cfm

To enable or disable CFM on a port, to configure a port as a Maintenance End Point (MEP) for a specific maintenance level, or to configure a port as a Maintenance Intermediate Point (MIP) for a specific domain or a specific maintenance level, use the **set port ethernet-cfm** command.

set port ethernet-cfm *mod/port* {**enable** | **disable**}

set port ethernet-cfm *mod/port* **mep level** *level* **mpid** *mpid* **vlan** *vlans*

set port ethernet-cfm *mod/port* **mip** [**level** *level*]

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables CFM on a port.
disable	Disables CFM on a port.
mep	Configures a MEP.
level *level*	Specifies a maintenance level for the MEP; valid values are from 0 to 7.
mpid	Sets a CFM Maintenance Point Identification.
mpid	Specifies the MP Identification.
vlan *vlans*	Specifies the number of the VLAN or range of VLANs to associate to a MEP; valid values are from 1 to 4094.
mip	Configures a MIP.
level *level*	Specifies a maintenance level for the MIP; valid values are from 0 to 7.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must configure a MIP on the port before configuring a MEP. The MEP must be configured at a lower level than the level of the MIP.

The MPID string is a string with a maximum 256 characters. The MPID identifies the MEP on the network.

The interface defined as MEP or MIP must be a trunk or an 802.1Q tunnel port. If you specify a port that is not one of these, the set port ethernet-cfm command will fail.

A MIP or MEP can be a logical interface, such as a port channel.

Examples

This example shows how to initialize a MIP at module 3, port1, at level 50:

```
Console> (enable) set ethernet-cfm 3/1 mip level 50
Port 3/1 set to MIP with ME Level 50.
Console> (enable)
```

8.6 EFT Copy

set port ethernet-oam

To enable or disable the IEEE 802.3ah Operations, Administrations, and Maintenance (OAM) feature on a specified port, use the **set port ethernet-oam** command.

set port ethernet-oam *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables OAM on the specified port.
disable	Disables OAM on the specified port.

Defaults

OAM is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When OAM is disabled on a port, the system functions as if OAM is not configured on that port. When OAM is enabled, OAM on that port functions as if OAM had never been enabled before.

Examples

This example shows how to enable OAM on a specified port:

```
Console> (enable) set port ethernet-oam 1/1 enable
OAM enabled on port 1/1
Console> (enable)
```

Related Commands

clear port ethernet-oam
set port ethernet-oam action
set port ethernet-oam link-monitor
set port ethernet-oam mode
set port ethernet-oam remote-loopback
show port ethernet-oam

set port ethernet-oam action

To configure an action for OAM link events, use the **set port ethernet-oam action** command.

set port ethernet-oam *mod/port* {**link-fault** | **dying-gasp** | **critical-event**} **action** {**errordisable** | **none** | **warning**}

Syntax Description

mod/port	Number of the module and the port on the module.
link-fault	Sets the link fault configuration.
dying-gasp	Sets the dying-gasp configuration. See the "Usage Guidelines" section for more information.
critical-event	Sets the critical event configuration.
action	Configures action that is taken for corresponding link events.
errordisable	Sends port to errordisable state.
none	Takes no action when corresponding link event occurs.
warning	Generates system message when corresponding link event occurs.

Defaults

The system generates a warning message when a link event occurs.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you specify the **dying-gasp** keyword, the errordisable option is not available.

Examples

This example shows how to configure the action that the specified port takes when a link fault occurs:

```
Console> (enable) set port ethernet-oam 1/1 link-fault action errordisable
OAM link-fault event action set to errordisable.
Console> (enable)
```

Related Commands

clear port ethernet-oam
set port ethernet-oam
set port ethernet-oam link-monitor
set port ethernet-oam mode
set port ethernet-oam remote-loopback
show port ethernet-oam

8.6 EFT Copy

set port ethernet-oam link-monitor

To configure the OAM link monitoring feature on a port, use the **set port ethernet-oam link-monitor** command.

set port ethernet-oam *mod/port* **link-monitor** {**enable** | **disable**}

set port ethernet-oam *mod/port* **link-monitor** {**symbol-period** | **frame** | **frame-period**} **window** *size*

set port ethernet-oam *mod/port* **link-monitor** {**symbol-period** | **frame** | **frame-period**} **low-threshold** *count* [**action** {**none** | **warning**}]

set port ethernet-oam *mod/port* **link-monitor** {**symbol-period** | **frame** | **frame-period**} **high-threshold** *count* [**action** {**errordisable** | **none** | **warning**}]

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables the OAM link monitor feature.
disable	Disables the OAM link monitor feature.
symbol-period	Sets monitoring by the number of symbols with errors.
frame	Sets monitoring by the number of frames with errors.
frame-period	Sets monitoring by frame period.
window	Sets link monitor window size for corresponding link events.
size	• **symbol-period**: valid values are from 1 to 1000000 (1 = 1 million symbols). • **frame**: valid values are from 10 to 65535 (in 100-millisecond increments). • **frame-period**: valid values are from 200 to 2000000000 frames.
low-threshold	Sets the low-threshold count for corresponding link events.
count	Valid values are from 0 to 65535.
action	(Optional) Configures action that is taken for corresponding link events.
none	Takes no action when corresponding link event occurs.
warning	Generates system message when corresponding link event occurs.
high-threshold	Sets the high-threshold count for corresponding link events.
count	Valid values are from 1 to 65535.
errordisable	Sends port to errordisable state.

Defaults

- Link monitoring is enabled.
- The **symbol-period** event is 625 million symbols.
- The **frame** event is 30 seconds.
- The **frame-period** event is 10 million frames.
- The **low-threshold** is 1 error.
- For **low-threshold**, the action is a **warning**.

- The **high-threshold** is 10 million errors.
- For **high-threshold**, the action is a **warning**.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the window size for symbol-period link monitoring:

```
Console> (enable) set port ethernet-oam 1/1 link-monitor symbol-period window 100
OAM errored symbol period window set to 100M symbols on port 1/1
Console> (enable)
```

This example shows how to set the link monitoring low threshold for frame events to 10 errors:

```
Console> (enable) set port ethernet-oam 1/1 link-monitor frame low-threshold 10
OAM errored frame low-threshold set to 10 errors
Console> (enable)
```

This example show how to set the link monitoring high threshold for frame-period events to 100 errors and to errordisable the port if the high threshold is reached:

```
Console> (enable) set port ethernet-oam 1/1 link-monitor frame-period high-threshold 100
action errordisable
OAM errored frame period high-threshold set to 100 errors on port 1/1, and action set to
errordisable.
Console> (enable)
```

Related Commands

clear port ethernet-oam
set port ethernet-oam
set port ethernet-oam action
set port ethernet-oam mode
set port ethernet-oam remote-loopback
show port ethernet-oam

set port ethernet-oam mode

To set the OAM mode on a port, use the **set port ethernet-oam mode** command.

set port ethernet-oam *mod/port* **mode** {**active** | **passive**}

Syntax Description

mod/port	Number of the module and the number of the port on the module.
active	Sets the specified port to OAM active mode.
passive	Sets the specified port to OAM passive mode.

Defaults

OAM is active on all ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

An OAM entity can be in active or passive mode. An active-mode OAM entity can exert more control on its peer than a passive-mode OAM entity can. For example, an active-mode entity can put a passive-mode entity into loopback mode, but a passive-mode entity cannot put an active-mode entity into loopback mode.

Table 2-17 describes the functions that are allowed in active and passive modes.

Table 2-17 Functions Allowed in Active Mode and Passive Mode

Function	Active Entity	Passive Entity
Initiates OAM Discovery process	Yes	No
Reacts to OAM Discovery process initiation	Yes	Yes
Required to send informational OAMPDUs	Yes	Yes
Permitted to send Event Notification OAMPDUs	Yes	Yes
Permitted to send Variable Request OAMPDUs	Yes	Yes
Permitted to send Variable Response OAMPDUs	Yes[1]	Yes
Permitted to send Loopback Control OAMPDUs	Yes	No
Reacts to Loopback Control OAMPDUs	Yes[1]	Yes
Permitted to send organization specific OAMPDUs	Yes	Yes

[1] The peer entity must be in active mode.

Examples

This example shows how to set the OAM on a specific port to active:

```
Console> (enable) set port ethernet-oam 1/1 mode active
OAM mode set to active on port 1/1
Console> (enable)
```

Related Commands

clear port ethernet-oam
set port ethernet-oam
set port ethernet-oam action
set port ethernet-oam link-monitor
set port ethernet-oam remote-loopback
show port ethernet-oam

set port ethernet-oam remote-loopback

To configure the OAM remote loopback feature on a port, use the **set port ethernet-oam remote-loopback** command.

set port ethernet-oam *mod/port* **remote-loopback** {**deny** | **permit**}

set port ethernet-oam *mod/port* **remote-loopback** {**enable** | **disable**}

set port ethernet-oam *mod/port* **remote-loopback test** [*number_of_packets* [*packet_size*]]

Syntax Description

mod/port	Number of the module and the port on the module.
deny	Denies OAM remote loopback requests on the specified port.
permit	Permits OAM remote loopback requests on the specified port.
enable	Initiates the OAM remote loopback test on the specified port.
disable	Ends the OAM remote loopback test on the specified port.
test	Tests the OAM remote loopback feature.
number_of_packets	(Optional) Number of packets that are sent from the specified port.
packet_size	(Optional) Packet size in bytes.

Command Default

OAM remote loopback requests are permitted.

If you do not specify the number of packets or the packet size, 10,000 64-byte packets are sent.

Command Types

Switch command.

Command Modes

Privileged mode.

Usage Guidelines

The **set port ethernet-oam** *mod/port* **remote-loopback** {**enable** | **disable**} command initiates or ends a loopback test on a port. You should use this command only on a port for which the peer OAM entity is capable of performing in OAM remote-loopback mode. After you enter the **disable** keyword, the switch displays a remote-loopback summary.

The **set port ethernet-oam** *mod/port* **remote-loopback** {**enable** | **disable**} command is not a configuration command and is not saved in NVRAM.

The **set port ethernet-oam** *mod/port* **remote-loopback test** command should only be run on a port whose status shows “remote OAM in loopback.” When a test is run, the specified number of packets are sent on the port. Ensure that those packets are looped back. A summary of the test is displayed after the test is finished.

The **set port ethernet-oam** *mod/port* **remote-loopback test** command is not a configuration command and is not saved in NVRAM.

Examples

This example shows how to deny remote loopback requests on a port:

```
Console> (enable) set port ethernet-oam 1/1 remote-loopback deny
OAM remote loopback request will be denied on port 1/1
Console> (enable)
```

This example shows how to initiate a loopback test on a port:

```
Console> (enable) set port ethernet-oam 1/1 remote-loopback enable
OAM remote loopback operation enabled on port 1/1
Warning:enabling OAM remote loopback operation moves the port into diagnostic mode.
Console> (enable)
```

This example shows how to end a loopback test on a port. When you disable the test, a summary of the loopback test is displayed:

```
Console> (enable) set port ethernet-oam 1/1 remote-loopback disable
OAM remote loopback summary on port 1/1
Port  TxTotal    RxTotal    Error
----  ---------  ---------  --------
1/1   999999     999444     111

OAM remote loopback mode disabled on port 1/1
Console> (enable)
```

This example shows how to test the remote loopback feature on a port:

```
Console> (enable) set port ethernet-oam 1/1 remote-loopback test 999999
Transmitting 999999 (64 byte) packets on port 1/1.
Please wait…
OAM remote loopback summary on port 1/1 (loopback master):
Port  TxTotal    RxTotal    Error
----  ---------  ---------  --------
1/1   999999     999444     111
Console> (enable)
```

Related Commands

clear port ethernet-oam
set port ethernet-oam
set port ethernet-oam action
set port ethernet-oam link-monitor
set port ethernet-oam mode
show port ethernet-oam

set port flexlink

To specify a Flexlink active port and a backup (peer) port, use the **set port flexlink** command.

set port flexlink *mod/port* **peer** *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.
peer	Specifies the peer port for the Flexlink active port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Flexlink redundancy allows you to specify two ports to form a redundant link capability. You configure one port as the active port and the other port is configured as the backup or peer port. The active port is in the forwarding state while the backup port is in the blocking state. The backup port does not allow traffic to pass.

When configuring Flexlink redundancy, follow these guidelines and restrictions:

- The maximum number of Flexlink pairs (one active port and one backup port) is 16 per switch.
- Flexlink ports cannot be part of an EtherChannel.
- Flexlink ports do not join STP operations. Flexlink ports do not generate STP BPDUs, and they drop all received BPDUs.
- Because it works with STP, VTP pruning does not work on Flexlink ports.
- SPAN works with Flexlink ports.
- IGMP works with Flexlink ports.
- DTP can run on Flexlink ports.
- Flexlink redundancy is for simple access topologies (two uplinks from a leaf node). You must ensure that there is a loop-free path from the wiring closet to the access network. Unlike STP, Flexlink is not designed to detect loops.
- Deploying STP in the core while running Flexlink redundancy on the edge is an acceptable configuration.
- Flexlink converges faster only if the directly connected link fails. Any other failure in the network is not improved by Flexlink fast convergence.

Examples

This example shows how to specify port 3/48 as the Flexlink active port and port 3/47 as the Flexlink backup (peer) port:

```
Console> (enable) set port flexlink 3/48 peer 3/47
Flexlink is successfully set on the port 3/48 and 3/47
Console> (enable)
```

This example shows the message that is displayed if you try to specify the same port as the active and the backup port:

```
Console> (enable) set port flexlink 2/2 peer 2/2
Port(s) can not backup itself.
Console> (enable)
```

Related Commands

clear port flexlink
show port flexlink

set port flowcontrol

To configure a port to send or receive pause frames, use the **set port flowcontrol** command. Pause frames are special packets that signal a source to stop sending frames for a specific period of time because the buffers are full.

set port flowcontrol *mod/port* {**receive** | **send**} {**off** | **on** | **desired**}

Syntax Description

mod/port	Number of the module and the port on the module.
receive	Specifies that a port processes pause frames.
send	Specifies that a port sends pause frames.
off	Prevents a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
on	Enables a local port to receive and process pause frames from remote ports or send pause frames to remote ports.
desired	Obtains predictable results regardless of whether a remote port is set to **on**, **off**, or **desired**.

Defaults

Flow-control defaults vary depending upon port speed:

- Gigabit Ethernet ports default to **off** for receive (Rx) and **desired** for transmit (Tx)
- Fast Ethernet ports default to **off** for receive and **on** for transmit

On the 24-port 100BASE-FX and 48-port 10/100 BASE-TX RJ-45 modules, the default is **off** for receive and **off** for send.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

When you configure the 24-port 100BASE-FX and 48-port 10/100 BASE-TX RJ-45 modules, you can set the receive flow control to **on** or **off** and the send flow control to **off**.

All Catalyst Gigabit Ethernet ports can receive and process pause frames from remote devices.

To obtain predictable results, use these guidelines:

- Use **send on** only when remote ports are set to **receive on** or **receive desired**.
- Use **send off** only when remote ports are set to **receive off** or **receive desired**.
- Use **receive on** only when remote ports are set to **send on** or **send desired**.
- Use **send off** only when remote ports are set to **receive off** or **receive desired**.

Table 2-18 describes guidelines for different configurations of the **send** and **receive** keywords.

Table 2-18 send and receive Keyword Configurations

Configuration	Description
send on	Enables a local port to send pause frames to remote ports.
send off	Prevents a local port from sending pause frames to remote ports.
send desired	Obtains predictable results whether a remote port is set to **receive on**, **receive off**, or **receive desired**.
receive on	Enables a local port to process pause frames that a remote port sends.
receive off	Prevents a local port from sending pause frames to remote ports.
receive desired	Obtains predictable results whether a remote port is set to **send on**, **send off**, or **send desired**.

Examples

This example shows how to configure port 1 of module 5 to receive and process pause frames:

```
Console> (enable) set port flowcontrol receive 5/1 on
Port 5/1 flow control receive administration status set to on
(port will require far end to send flowcontrol)
Console> (enable)
```

This example shows how to configure port 1 of module 5 to receive and process pause frames if the remote port is configured to send pause frames:

```
Console> (enable) set port flowcontrol receive 5/1 desired
Port 5/1 flow control receive administration status set to desired
(port will allow far end to send flowcontrol if far end supports it)
Console> (enable)
```

This example shows how to configure port 1 of module 5 to receive but NOT process pause frames on port 1 of module 5:

```
Console> (enable) set port flowcontrol receive 5/1 off
Port 5/1 flow control receive administration status set to off
(port will not allow far end to send flowcontrol)
Console> (enable)
```

This example shows how to configure port 1 of module 5 to send pause frames:

```
Console> (enable) set port flowcontrol send 5/1 on
Port 5/1 flow control send administration status set to on
(port will send flowcontrol to far end)
Console> (enable)
```

This example shows how to configure port 1 of module 5 to send pause frames and yield predictable results even if the remote port is set to **receive off**:

```
Console> (enable) set port flowcontrol send 5/1 desired
Port 5/1 flow control send administration status set to desired
(port will send flowcontrol to far end if far end supports it)
Console> (enable)
```

Related Commands

show port flowcontrol

set port gmrp

To enable or disable GMRP on the specified ports in all VLANs, use the **set port gmrp** command.

set port gmrp *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables GVRP on a specified port.
disable	Disables GVRP on a specified port.

Defaults

The default is GMRP is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

You can enter this command even when GMRP is not enabled, but the values come into effect only when you enable GMRP using the **set gmrp enable** command.

Examples

This example shows how to enable GMRP on module 3, port 1:

```
Console> (enable) set port gmrp 3/1 enable
GMRP enabled on port(s) 3/1.
GMRP feature is currently disabled on the switch.
Console> (enable)
```

This example shows how to disable GMRP on module 3, ports 1 through 5:

```
Console> (enable) set port gmrp 3/1-5 disable
GMRP disabled on port(s) 3/1-5.
Console> (enable)
```

Related Commands

show gmrp configuration

set port gvrp

To enable or disable GVRP on the specified ports in all VLANs, use the **set port gvrp** command.

set port gvrp *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables GVRP on a specified port.
disable	Disables GVRP on a specified port.

Defaults

The default is GVRP is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

When you enable VTP pruning, it runs on all the GVRP-disabled trunks.

To run GVRP on a trunk, you need to enable GVRP both globally on the switch and individually on the trunk.

You can configure GVRP on a port even when you globally enable GVRP. However, the port will not become a GVRP participant until you globally enable GVRP.

You can enable GVRP on an 802.1Q trunk only.

If you enter the **set port gvrp** command without specifying the port number, GVRP is affected globally in the switch.

Examples

This example shows how to enable GVRP on module 3, port 2:

```
Console> (enable) set port gvrp 3/2 enable
GVRP enabled on 3/2.
Console> (enable)
```

This example shows how to disable GVRP on module 3, port 2:

```
Console> (enable) set port gvrp 3/2 disable
GVRP disabled on 3/2.
Console> (enable)
```

This example shows what happens if you try to enable GVRP on a port that is not an 802.1Q trunk:

```
Console> (enable) set port gvrp 4/1 enable
Failed to set port 4/1 to GVRP enable. Port not allow GVRP.
Console> (enable)
```

This example shows what happens if you try to enable GVRP on a specific port when GVRP has not first been enabled using the **set gvrp** command:

```
Console> (enable) set port gvrp 5/1 enable
GVRP enabled on port(s) 5/1.
GVRP feature is currently disabled on the switch.
Console> (enable)
```

Related Commands

clear gvrp statistics
set gvrp
show gvrp configuration

8.6 EFT Copy

set port host

To optimize the port configuration for a host connection, use the **set port host** command.

set port host *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

To optimize the port configuration, the **set port host** command sets channel mode to off, enables spanning tree PortFast, sets the trunk mode to off, and disables the dot1q tunnel feature. Only an end station can accept this configuration.

Because spanning tree PortFast is enabled, you should enter the **set port host** command only on ports connected to a single host. Connecting hubs, concentrators, switches, and bridges to a fast-start port can cause temporary spanning tree loops.

Enable the **set port host** command to decrease the time it takes to start up packet forwarding.

Examples

This example shows how to optimize the port configuration for end station/host connections on ports 2/1 and 3/1:

```
Console> (enable) set port host 2/1,3/1

Warning: Span tree port fast start should only be enabled on ports connected to a single
host.  Connecting hubs, concentrators, switches, bridges, etc. to a fast start port can
cause temporary spanning tree loops.  Use with caution.

Spantree ports 2/1,3/1 fast start enabled.
Dot1q tunnel feature disabled on port(s)  4/1.
Port(s) 2/1,3/1 trunk mode set to off.
Port(s) 2/1 channel mode set to off.

Console> (enable)
```

Related Commands

clear port host

set port inlinepower

To set the inline power mode of a port or group of ports, use the **set port inlinepower** command.

set port inlinepower *mod/port* {**auto** | **static** | **limit**} [*max-wattage*]

set port inlinepower *mod/port* **off**

Syntax Description

mod/port	Number of the module and the port on the module.
auto	Powers up the port only if the switching module has discovered the phone.
static	Powers up the port to a preallocated value so that the port is guaranteed power. See the "Usage Guidelines" section for more information.
limit	Limits power on the specified port. See the "Usage Guidelines" section for more information.
max-wattage	(Optional) The maximum power allowed on the port in either auto or static mode; valid values are from 4000 to 15400 milliwatts.
off	Prevents the port from providing power to an external device.

Defaults

The default is **auto**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you specify **auto** or **static** mode but do not specify a *max-wattage* argument, the maximum wattage that is supported by the hardware is used.

If you specify **static** mode, power is preallocated to the specified port even if no devices are connected to that port. Connecting any device to that port ensures priority of service because that port is guaranteed power.

If you enter the **off** keyword, the inline power-capable device is not detected.

Each port isin one of the following modes (configured through the set port inlinepower CLI command):

- **auto**—The supervisor engine directs the switching module to power up the port only if the switching module discovers the phone. You can specify the maximum wattage that is allowed on the port. If you do not specify a wattage, then the switch will deliver no more than the hardware-supported maximum value.
- **static**—The supervisor engine directs the switching module to power up the port to the wattage you specify only if the switching module discovers the phone. You can specify the maximum wattage that is allowed on the port. If you do not specify a wattage, then the switch allows the hardware-supported maximum value. The maximum wattage, whether determined by the switch or specified by you, is preallocated to the port. If the switch does not have enough power for the allocation, the command will fail.

- **limit**—Discovery is enabled, and you can limit the power allocated for an external device. If the wattage value that you specify with the **limit** keyword is less than the power that is specified by IEEE classification, instead of denying power, the lesser of these two values is allocated. If the device consumes more than the configured value, the port is shut down and a syslog message is displayed. The **limit** keyword is supported only on modules with the WS-F6K-48-AF daughter card.
- **off**—Prevents the port from providing the power to an external device. If the external device is wall-powered and inline power is off, the port should still link up, join the bridge group, and go to the STP forwarding state.

Each port also has a status, defined as one of the following:

- on—Power is supplied by the port.
- off—Power is not supplied by the port.
- Power-deny—The supervisor engine does not have enough power to allocate to the port, or the power that is configured for the port is less than the power that is required by the port; the power is not being supplied by the port.
- err-disable—The port is unable to provide the power to the connected device that is configured in Static mode.
- faulty—The port failed the diagnostics tests.

If you enter this command on a port that does not support the IP phone power feature, an error message is displayed.

You can enter a single port or a range of ports, but you cannot enter the module number only.

Caution Damage can occur to equipment connected to the port if you are not using a phone that can be configured for the IP phone phantom power feature.

Examples

This example shows how to set the inline power to off:

```
Console> (enable) set port inlinepower 2/5 off
Inline power for port 2/5 set to off.
Console> (enable)
```

This example shows the output if the inline power feature is not supported:

```
Console> (enable) set port inlinepower 2/3-9 auto
Feature not supported on module 2.
Console> (enable)
```

Related Commands

set inlinepower
show environment
show port inlinepower

set port jumbo

To enable or disable the jumbo frame feature on a per-port basis, use the **set port jumbo** command.

set port jumbo *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables jumbo frames on a specified port.
disable	Disables jumbo frames on a specified port.

Defaults

If you enable the jumbo frame feature, the MTU size for packet acceptance is 9216 bytes for nontrunking ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM. The jumbo frame feature is supported on any Ethernet port and on the sc0 interface. The MSFC2 supports routing of jumbo frames. The Gigabit Switch Router (GSR) supports jumbo frames.

You can use the jumbo frame feature to transfer large frames or jumbo frames through Catalyst 6500 series switches to optimize server-to-server performance.

The Multilayer Switch Feature Card (MSFC) and the Multilayer Switch Module (MSM) do not support the routing of jumbo frames; if jumbo frames are sent to these routers, router performance is significantly degraded.

Examples

This example shows how to enable the jumbo frames feature on module 3, port 2:

```
Console> (enable) set port jumbo 3/2 enable
Jumbo frames enabled on port 5/3.
Console> (enable)
```

This example shows how to disable the jumbo frames feature on module 3, port 2:

```
Console> (enable) set port jumbo 3/2 disable
Jumbo frames disabled on port 3/2.
Console> (enable)
```

Related Commands

set trunk
show port jumbo

set port l2protocol-tunnel

To set Layer 2 protocol tunneling parameters, use the **set port l2protocol-tunnel** command.

set port l2protocol-tunnel *mod/port* {**cdp** | **eoam** | **stp** | **vtp**} {**enable** | **disable**}

set port l2protocol-tunnel *mod/port* {**drop-threshold** *drop-threshold*} {**shutdown-threshold** *shutdown-threshold*} [**cdp** | **eoam** | **stp** | **vtp**]

Syntax Description

mod/port	Number of the module and the port or range of ports.
cdp | **eoam** | **stp** | **vtp**	Specifies the protocol type. See the "Usage Guidelines" section for more information.
enable | **disable**	Enables or disables the protocol.
drop-threshold *drop-threshold*	Specifies the drop threshold factor on a port or range of ports; valid values are from 0 to 65535. See the "Usage Guidelines" section for more information.
shutdown-threshold *shutdown-threshold*	Specifies the shutdown threshold factor on a port or range of ports; valid values are from 0 to 65535. See the "Usage Guidelines" section for more information.

Defaults

Protocol tunneling is disabled on all ports.

The default for the drop threshold and the shutdown threshold is **0**. The **0** value indicates that no limit is set.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can specify more than one protocol type at a time. In the CLI, separate protocol types with a space.

The recommended maximum value for the shutdown threshold is 1000. This value reflects the number of PDUs an edge switch can handle per second (without dropping any) while performing egress and ingress tunneling. For an edge switch, the shutdown threshold value also determines the number of Layer 2 protocol tunneling ports that can be connected to customer switches and the number of customer VLANs per Layer 2 protocol tunneling port. In determining the recommended maximum value of 1000, egress tunneling from the service provider network was also taken into consideration.

To determine the number of Layer 2 protocol tunneling ports (links) and the number of customer VLANs per Layer 2 protocol tunneling port (VLANs per link) that an edge switch can handle, use the following formula: Multiply the number of Layer 2 protocol tunneling ports by the number of VLANs and the result should be less than or equal to 1000. Some examples of acceptable configurations are as follows:

- 1 Layer 2 protocol tunneling port x 1000 VLANs
- 2 Layer 2 protocol tunneling port x 500 VLANs

- 5 Layer 2 protocol tunneling port x 200 VLANs
- 10 Layer 2 protocol tunneling port x 100 VLANs
- 20 Layer 2 protocol tunneling port x 50 VLANs
- 100 Layer 2 protocol tunneling port x 10 VLANs

Note The shutdown threshold factor should exceed the drop threshold factor. After reaching the drop threshold factor, the port or range of ports starts dropping PDUs. After reaching the shutdown threshold factor, the port or range of ports goes into errdisable state and is restored after timeout.

Note With software release 8.4(1) and later releases, you can specify the drop and shutdown thresholds for individual protocols on a per-port basis. If you configure thresholds only and do not specify a protocol, the packets are rate limited cumulatively irrespective of protocols. If you specify a threshold for a protocol on a port, the packets are rate limited on a cumulative basis, and then per-protocol thresholds are applied to the packets. The range for the per-port protocols drop threshold and shutdown threshold is from 0 to 65535.

Examples

This example shows how to enable CDP on a range of ports:

```
Console> (enable)  set port l2protocol-tunnel 7/1-2 cdp enable
Layer 2 protocol tunneling enabled for CDP on ports 7/1-2.
Console> (enable)
```

This example shows how to enable STP and VTP on a range of ports:

```
Console> (enable)  set port l2protocol-tunnel 7/1-2 stp vtp enable
Layer 2 protocol tunneling enabled for STP VTP on ports 7/1-2.
Console> (enable)
```

This example shows how to disable CDP, STP, and VTP on a range of ports:

```
Console> (enable)  set port l2protocol-tunnel 7/1-2 cdp stp vtp disable
Layer 2 protocol tunneling disabled for CDP STP VTP on ports 7/1-2.
Console> (enable)
```

This example shows how to set the drop threshold to 1000 and the shutdown threshold to 20000 on a port:

```
Console> (enable) set port l2protocol-tunnel 7/1 drop-threshold 1000 shutdown-threshold 
20000
Drop Threshold=1000, Shutdown Threshold=20000 set on port 7/1.
Console> (enable)
```

This example shows how to specify a drop threshold of 100 and a shutdown threshold of 400 for CDP packets on a port:

```
Console> (enable) set port l2protocol-tunnel 3/1 drop-threshold 200 shutdown-threshold 400 
cdp
Drop Threshold=200, Shutdown Threshold=400 set on port 3/1.
Console> (enable)
```

This example shows how to enable the EOAM protocol on a range of ports:

```
Console> (enable)  set port l2protocol-tunnel 7/1-2 eoam enable
Layer 2 protocol tunneling enabled for EOAM on ports 7/1-2.
Console> (enable)
```

Related Commands

clear l2protocol-tunnel cos
clear l2protocol-tunnel statistics
set l2protocol-tunnel cos
show l2protocol-tunnel statistics
show port l2protocol-tunnel

set port lacp-channel

To set the priority value for physical ports, to assign an administrative key to a particular set of ports, or to change the channel mode for a set of ports that were previously assigned to the same administrative key, use the **set port lacp-channel** command.

set port lacp-channel *mod/ports* **port-priority** *value*

set port lacp-channel *mod/ports* [*admin-key*]

set port lacp-channel *mod/ports* **mode** {**on** | **off** | **active** | **passive**}

Syntax Description

mod/ports	Number of the module and the ports on the module.
port-priority	Specifies the priority for physical ports.
value	Number of the port priority; valid values are from 1 to 255. See the "Usage Guidelines" section for more information about the priority value.
admin-key	(Optional) Number of the administrative key; valid values are from 1 to 1024. See the "Usage Guidelines" section for more information about the administrative key.
mode	Specifies the channel mode for a set or ports.
on | **off** | **active** | **passive**	Specifies the status of the channel mode.

Defaults

LACP is supported on all Ethernet interfaces.

The default port priority value is **128**.

The default mode is **passive** for all ports that are assigned to the administrative key.

For differences between PAgP and LACP, refer to the "Guidelines for Port Configuration" section of the "Configuring EtherChannel" chapter of the *Catalyst 6500 Series Software Configuration Guide*.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command can only be used for ports belonging to LACP modules. This command cannot be used on ports running in PAgP mode.

Higher priority values correspond to lower priority levels.

The following usage guidelines apply when you assign an administrative key to ports:

- If you do not enter a value for the administrative key, the switch chooses a value automatically.
- If you choose a value for the administrative key, but this value is already used in your switch, all the ports associated with this value are moved to a new administrative key that is assigned automatically. The previously used value is now associated with new ports.

- You can assign a maximum of 8 ports to an administrative key.
- If you assign an administrative key to a channel that was previously assigned a particular mode, the channel will maintain that mode after you enter the administrative key value.

Examples

This example shows how to set the priority of ports 1/1 to 1/4 and 2/6 to 2/8 to 10:

```
Console> (enable) set port lacp-channel 4/1-4
Ports 4/1-4 being assigned admin key 96.
Console> (enable)
```

This example shows how to assign ports 4/1 to 4/4 to an administrative key that the switch automatically chooses:

```
Console> (enable) set port lacp-channel 4/1-4
Ports 4/1-4 being assigned admin key 96.
Console> (enable)
```

This example shows how to assign ports 4/4 to 4/6 to administrative key 96 when that key was previously assigned to ports 4/1 to 4/3:

```
Console> (enable) set port lacp-channel 4/4-6 96
admin key 96 already assigned to port 4/1-3.
Port(s) 4/1-3 being assigned to admin key 97.
Port(s) 4/4-6 being assigned to admin key 96.
Console> (enable)
```

Related Commands

clear lacp-channel statistics
set channelprotocol
set lacp-channel system-priority
set spantree channelcost
set spantree channelvlancost
show lacp-channel
show port lacp-channel

set port mac-auth-bypass

To configure the MAC authentication bypass feature on a port, use the **set port mac-auth-bypass** command.

set port mac-auth-bypass *mod/port* {**enable** | **disable**}

set port mac-auth-bypass *mod/port* {**initialize** | **reauthenticate**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables the MAC authentication bypass feature on a port.
disable	Disables the MAC authentication bypass feature on a port.
initialize	Initializes the MAC address authentication bypass state for a port so the port can participate in authentication again.
reauthenticate	Reauthenticates the MAC address of a port.

Defaults

The MAC authentication bypass feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enable the MAC authentication bypass feature on a port, you automatically enable PortFast on that port. When you disable the MAC authenticaion bypass feature on a port, you automatically disable PortFast on that port.

When you enter **set port mac-auth-bypass** *mod/port* **initialize**, the specified port is moved to the waiting state and any required cleanup is performed (such as unauthorizing the port, cleaning up any static/trap CAM entries, and so on).

The **set port mac-auth-bypass** *mod/port* **reauthenticate** command is accepted only when the port is in authenticated state; otherwise, the command is ignored.

For more information about the states and events that are associated with the MAC authentication bypass feature, see the “Configuring MAC Address Authentication Bypass” chaper of the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to enable MAC address authentication bypass on a port:

```
Console> (enable) set port mac-auth-bypass 3/1 enable
MAC-Auth-Bypass successfully enabled on 3/1.
Console> (enable)
```

This example shows how to initialize the MAC address authentication bypass state for a port so that the port can participate in authentication again:

```
Console> (enable) set port mac-auth-bypass 3/1 initialize
Mac-Auth-Bypass successfully Initialized 3/1.
Console> (enable)
```

This example shows how to reauthenticate the MAC address of a port:

```
Console> (enable) set port mac-auth-bypass 3/1 reauthenticate
Reauthenticating MAC address 00-00-00-00-00-01 on port 3/1 using Mac-Auth-Bypass.
Console> (enable)
```

Related Commands

set mac-auth-bypass
show mac-auth-bypass
show port mac-auth-bypass

8.6 EFT Copy

set port macro

To execute a configuration macro on a per-port basis, use the **set port macro** command.

set port macro *mod/ports...* **ciscoipphone vlan** *vlan* [**auxvlan** *auxvlan*]

set port macro *mod/ports...* **ciscosoftphone vlan** *vlan*

set port macro *mod/ports...* **ciscodesktop vlan** *vlan*

set port macro *mod/ports...* **ciscorouter nativevlan** *nativevlan* [**allowedvlans** *vlan*]

set port macro *mod/ports...* **ciscoswitch nativevlan** *nativevlan* [**allowedvlans** *vlan*]

set port macro *mod/ports... macro_name*

Syntax Description

mod/ports...	Number of the module and the ports on the module.
ciscoipphone	Specifies the Cisco IP Phone SmartPort configuration macro.
vlan	Specifies a VLAN interface.
vlan	Number of the VLAN or VLANs.
auxvlan	(Optional) Specifies an auxiliary VLAN.
auxvlan	(Optional) Number of the auxiliary VLAN.
ciscosoftphone	Specifies the Cisco Softphone SmartPort configuration macro.
ciscodesktop	Specifies the Cisco Desktop SmartPort configuration macro.
ciscorouter	Specifies the Cisco Router SmartPort configuration macro.
nativevlan	Specifies the native VLAN for IP phone traffic.
nativevlan	Number of the native VLAN.
allowedvlans	(Optional) Specifies the VLAN or VLANs that are allowed on the trunk.
ciscoswitch	Specifies the Cisco Switch SmartPort configuration macro.
macro_name	Name of a user-defined macro to apply to a port. See the "Usage Guidelines" section for more information about applying a user-defined macro.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you use automatic voice configuration with the **ciscoipphone** keyword, some of the QoS configuration requires phone-specific configuration (trust-ext, ext-cos), which is supported only on the following phones: Cisco IP Phone 7910, Cisco IP Phone 7940, Cisco IP Phone 7960, and Cisco IP Phone 7935. However, the **ciscoipphone** keyword is not exclusive to these models only; any phone can benefit from all the other QoS settings that are configured on the switch.

To configure the QoS settings and the trusted boundary feature on the Cisco IP Phone, you must enable Cisco Discovery Protocol (CDP) version 2 or later on the port. You need to enable CDP only for the **ciscoipphone** QoS configuration; CDP does not affect the other components of the automatic voice configuration feature.

The automatic voice configuration commands do not support channeling.

A PFC or PFC2 is not required for the **ciscoipphone** keyword.

A PFC or PFC2 is required for the **ciscosoftphone** keyword.

The **ciscoipphone** keyword is only supported on 10/100 and 10/100/1000 Ethernet ports.

The **ciscosoftphone** keyword is supported on all Ethernet ports.

To see the configuration that results in choosing the **ciscodesktop**, **ciscorouter**, or **ciscoswitch** keyword, see to the "Configuring a VoIP Network" chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

When applying user-defined macros, follow these guidelines and restrictions:

- If you attempt to apply a macro on a port and the macro has a variable that is not defined in its definition, the macro is not applied on the port and an appropriate error message is displayed. This does not affect the definition of the macro.
- If you attempt to apply a macro on a port and the macro has some valid and some invalid commands in its definition, the macro is still applied on the port and an appropriate error message is displayed when the invalid command is executed. This does not affect the definition of the macro.
- When you apply a macro, a record of the macro being applied is not stored in the configuration file or NVRAM. However, for each port there is a record of the latest macro that was applied to it.
- Once a macro is applied to a port, you cannot clear the macro. However, one way to cancel a macro on a port is to define another macro that clears the configurations on the port, and then apply the newly created macro on the port.

For more information about user-defined Smartports macros, see the "Configuring a VoIP Network" chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example shows how to execute the Cisco IP Phone configuration macro with an auxiliary VLAN:

```
Console> (enable) set port macro 3/1 ciscoipphone vlan 2 auxvlan 3
Port 3/1 enabled.
Layer 2 protocol tunneling disabled for CDP STP VTP on port(s) 3/1.
Port 3/1 vlan assignment set to static.
Spantree port fast start option set to default for ports 3/1.
Port(s) 3/1 channel mode set to off.

Warning:Connecting Layer 2 devices to a fast start port can cause
temporary spanning tree loops. Use with caution.

Spantree port  3/1 fast start enabled.
Dot1q tunnel feature disabled on port(s)  3/1.
Port(s)  3/1 trunk mode set to off.
VLAN  Mod/Ports
---- -----------------------
```

```
2     2/1
      3/1
      16/1
AuxiliaryVlan Status   Mod/Ports
------------- --------
-------------------------------------------------------
3             inactive 3/1

Vlan 3 is not active.
Inline power for port 3/1 set to auto.

CDP enabled globally
CDP enabled on port 3/1.
CDP version set to v2
........
All ingress and egress QoS scheduling parameters configured on all ports.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps
configured.  Global QoS configured.
Port 3/1 ingress QoS configured for Cisco IP Phone.
Macro completed on port 3/1.
Console> (enable)
```

This example shows the warning message that appears when you do not specify an auxiliary VLAN:

```
Console> (enable) set port macro 3/1 ciscoipphone vlan 2
Warning: All inbound QoS tagging information will be lost as no auxillary
vlan was specified.
Do you want to continue (y/n) [n]?
```

This example shows how to execute the Cisco Softphone configuration macro:

```
Console> (enable) set port macro 3/1 ciscosoftphone vlan 32
Port 3/1 enabled.
Layer 2 protocol tunneling disabled for CDP STP VTP on port(s) 3/1.
Port 3/1 vlan assignment set to static.
Spantree port fast start option set to default for ports 3/1.
Port(s) 3/1 channel mode set to off.

Warning:Connecting Layer 2 devices to a fast start port can cause
temporary spanning tree loops. Use with caution.

Spantree port  3/1 fast start enabled.
Dot1q tunnel feature disabled on port(s)  3/1.
Port(s)  3/1 trunk mode set to off.
Vlan 32 configuration successful
VLAN 32 modified.
VLAN 2 modified.
VLAN  Mod/Ports
---- -----------------------
32    3/1
      16/1
Port 3/1 will not send out CDP packets with AuxiliaryVlan information.
Executing autoqos........
All ingress and egress QoS scheduling parameters configured on all ports.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps
configured.  Global QoS configured.
Port 3/1 ingress QoS configured for Cisco Softphone.
Macro completed on port 3/1.
Console> (enable)
```

8.6 EFT Copy

This example shows how to apply a user-defined macro named “videophone” to port 3/2:

```
Console> (enable) set port macro 3/2 videophone
```

Before the macro is applied, variables are replaced by variables that are specified by entering the **set macro variable** command. The following commands that were included in the user-defined macro then are executed:

```
set port enable 3/2
set vlan 3 3/2
set port auxiliaryvlan 3/2 4
set cdp enable
set cdp version v2
set qos autoqos
Console> (enable)
```

Related Commands

clear macro
set cdp
set macro
set macro ciscosmartports
set port qos autoqos
set qos autoqos
show macro

set port membership

To set the VLAN membership assignment to a port, use the **set port membership** command.

set port membership *mod/port* {**dynamic** | **static**}

Syntax Description

mod/port	Number of the module and the port on the module.
dynamic	Specifies that the port become a member of dynamic VLANs.
static	Specifies that the port become a member of static VLANs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Dynamic VLAN support for VVID includes these restrictions to the following configuration of MVAP on the switch port:

- You can configure any VVID on a dynamic port including dot1p and untagged, except when the VVID is equal to dot1p or untagged. If this is the case, then you must configure VMPS with the MAC address of the IP phone. When you configure the VVID as dot1p or untagged on a dynamic port, this warning message is displayed:

  ```
  VMPS should be configured with the IP phone mac's.
  ```

- You cannot change the VVID of the port equal to PVID assigned by the VMPS for the dynamic port.
- You cannot configure trunk ports as dynamic ports, but you can configure MVAP as a dynamic port.

Examples

This example shows how to set the port membership VLAN assignment to **dynamic**:

```
Console> (enable) set port membership 5/5 dynamic
Port 5/5 vlan assignment set to dynamic.
Spantree port fast start option enabled for ports 5/5.
Console> (enable)
```

This example shows how to set the port membership VLAN assignment to **static**:

```
Console> (enable) set port membership 5/5 static
Port 5/5 vlan assignment set to static.
Console> (enable)
```

Related Commands

set pvlan
set pvlan mapping
set vlan
set vlan mapping

set port name

To configure a name for a port, use the **set port name** command.

set port name *mod/port* [*port_name*]

Syntax Description

mod/port	Number of the module and the port on the module.
port_name	(Optional) Name of the port. See the "Usage Guidelines" section for more information.

Defaults

The default is no port name is configured for any port.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

The *port_name* argument must be fewer than 21 characters.

If you do not specify a *port_name* argument, the port name is cleared.

Examples

This example shows how to set port 1 on module 4 to Snowy:

```
Console> (enable) set port name 4/1 Snowy
Port 4/1 name set.
Console> (enable)
```

Related Commands

set port description
show port
show port description

set port negotiation

To enable or disable the link negotiation protocol on the specified port, use the **set port negotiation** command.

set port negotiation *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables the link negotiation protocol.
disable	Disables the link negotiation protocol.

Defaults

The default is link negotiation protocol is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You cannot configure port negotiation on 1000BASE-T (copper) Gigabit Ethernet ports in this release. If a 1000BASE-T GBIC is inserted in the port that was previously configured as a negotiation-disabled port, the negotiation-disabled setting is ignored, and the port operates in negotiation-enabled mode.

The **set port negotiation** command is supported on Gigabit Ethernet ports only, except on WS-X6316-GE-TX and on WS-X6516-GE-TX.

If the port does not support this command, this message appears:

```
Feature not supported on Port N/N.
```

where N/N is the module and port number.

In most cases, when you enable link negotiation, the system autonegotiates flow control, duplex mode, and remote fault information. The exception applies to 16-port 10/100/1000BASE-T Ethernet modules; when you enable link negotiation on these Ethernet modules, the system autonegotiates flow control only.

You must either enable or disable link negotiation on both ends of the link. Both ends of the link must be set to the same value or the link cannot connect.

Examples

This example shows how to disable link negotiation protocol on port 1, module 4:

```
Console> (enable) set port negotiation 4/1 disable
Link negotiation protocol disabled on port 4/1.
Console> (enable)
```

Related Commands

show port negotiation

set port protocol

To enable or disable protocol membership of ports, use the **set port protocol** command.

set port protocol *mod/port* {**ip** | **ipx** | **group**} {**on** | **off** | **auto**}

Syntax Description

mod/port	Number of the module and the port on the module.
ip	Specifies IP.
ipx	Specifies IPX.
group	Specifies VINES, AppleTalk, and DECnet protocols.
on	Indicates the port will receive all the flood traffic for that protocol.
off	Indicates the port will not receive any flood traffic for that protocol.
auto	Specifies that the port is added to the group only after packets of the specific protocol are received on that port.

Defaults

The default is that the ports are configured to **on** for the IP protocol groups and **auto** for IPX and group protocols.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Protocol filtering is supported only on nontrunking EtherChannel ports. Trunking ports are always members of all the protocol groups.

If the port configuration is set to **auto**, the port initially does not receive any flood packets for that protocol. When the corresponding protocol packets are received on that port, the supervisor engine detects this and adds the port to the protocol group.

Ports configured as **auto** are removed from the protocol group if no packets are received for that protocol within a certain period of time. This aging time is set to 60 minutes. They are also removed from the protocol group on detection of a link down.

Examples

This example shows how to disable IPX protocol membership of port 1 on module 2:

```
Console> (enable) set port protocol 2/1 ipx off
IPX protocol disabled on port 2/1.
Console> (enable)
```

This example shows how to enable automatic IP membership of port 1 on module 5:

```
Console> (enable) set port protocol 5/1 ip auto
IP protocol set to auto mode on module 5/1.
Console> (enable)
```

Related Commands show port protocol

8.6 EFT Copy

set port qos

To specify whether an interface is interpreted as a physical port or as a VLAN, use the **set port qos** command.

set port qos *mod/ports...* **port-based** | **vlan-based**

Syntax Description

mod/ports...	Number of the module and the ports on the module.
port-based	Interprets the interface as a physical port.
vlan-based	Interprets the interface as part of a VLAN.

Defaults

The default is ports are port-based if QoS is enabled and VLAN-based if QoS is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

When you change a port from port-based QoS to VLAN-based QoS, all ACLs are detached from the port. Any ACLs attached to the VLAN apply to the port immediately.

When you set a port to VLAN-based QoS using the **set port qos** command with RSVP or COPS QoS enabled on that port, the QoS policy source is COPS, or DSBM-election is enabled. The VLAN-based setting is saved in NVRAM only.

Examples

This example shows how to specify an interface as a physical port:

```
Console> (enable) set port qos 1/1-2 port-based
Updating configuration ...
QoS interface is set to port-based for ports 1/1-2.
Console> (enable)
```

This example shows how to specify an interface as a VLAN:

```
Console> (enable) set port qos 3/1-48 vlan-based
Updating configuration ...
QoS interface is set to VLAN-based for ports 3/1-48.
Console> (enable)
```

This example shows the output if you change from port-based QoS to VLAN-based QoS with either RSVP or COPS enabled on the port:

```
Console> (enable) set port qos 3/1-48 vlan
Qos interface is set to vlan-based for ports 3/1-48
Port(s) 3/1-48 - QoS policy-source is Cops or DSBM-election is enabled.
Vlan-based setting has been saved in NVRAM only.
Console> (enable)
```

Related Commands

set port qos cos
set port qos trust
show port qos
show qos info

8.6 EFT Copy

set port qos autoqos

To apply the automatic QoS feature on a per-port basis, use the **set port qos autoqos** command.

set port qos *mod/port* **autoqos trust** {**cos** | **dscp**}

set port qos *mod/port* **autoqos voip** {**ciscoipphone** | **ciscosoftphone**}

Syntax Description

mod/port	Number of the module and ports on the module.
trust	Specifies AutoQoS for ports trusting all traffic markings.
cos	Trusts CoS-based markings of all inbound traffic.
dscp	Trusts DSCP-based markings of all inbound traffic.
voip	Specifies AutoQoS for voice applications.
ciscoipphone	Specifies AutoQoS for Cisco 79xx IP phones.
ciscosoftphone	Specifies AutoQoS for Cisco IP SoftPhones.

Defaults

The per-port AutoQos feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to trust CoS-based markings of inbound traffic on module 4, port 1:

```
Console> (enable) set port qos 4/1 autoqos trust cos
Port 4/1 ingress QoS configured for trust cos.
Trusting all incoming CoS marking on port 4/1.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

This example shows how to apply AutoQoS settings for Cisco 79xx IP phones on module 4, port 1:

```
Console> (enable) set port qos 4/1 autoqos voip ciscoipphone
Port 4/1 ingress QoS configured for ciscoipphone.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

This example shows how to apply AutoQoS settings for Cisco IP SoftPhones on module 4, port 1:

```
Console> (enable) set port qos 4/1 autoqos voip ciscosoftphone
Port 4/1 ingress QoS configured for ciscosoftphone.  Policing configured on 4/1.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

Related Commands

clear port qos autoqos
clear qos autoqos
set qos autoqos
show port qos
show qos acl info

set port qos cos

To set the default value for all packets that have arrived through an untrusted port, use the **set port qos cos** command.

set port qos *mod/ports* **cos** *cos_value*

set port qos *mod/ports* **cos-ext** *cos_value*

Syntax Description

mod/ports	Number of the module and ports.
cos *cos_value*	Specifies the CoS value for a port; valid values are from 0 to 7.
cos-ext *cos_value*	Specifies the CoS extension for a phone port; valid values are from 0 to 8.

Defaults

The default is CoS 0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is only supported on Ethernet modules.

This command has no effect when QoS is disabled. The port CoS setting takes effect when QoS is enabled.

Examples

This example shows how to set the CoS default value on a port:

```
Console> (enable) set port qos 2/1 cos 3
Port 2/1 qos cos set to 3.
Console> (enable)
```

This example shows how to set the CoS-ext default value on a port:

```
Console> (enable) set port qos 2/1 cos-ext 3
Port 2/1 qos cos-ext set to 3.
Console> (enable)
```

Related Commands

clear port qos cos
set port qos
set port qos trust
show port qos
show qos info

set port qos policy-source

To set the QoS policy source for all ports in the specified module, use the **set port qos policy-source** command.

set port qos policy-source *mod/ports...* **local** | **cops**

Syntax Description

mod/ports...	Number of the module and the ports on the module.
local	Sets the policy source to local NVRAM configuration.
cops	Sets the policy source to COPS configuration.

Defaults

The default is all ports are set to local.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you set the policy source to **local**, the QoS policy is taken from local configuration stored in NVRAM. If you set the policy source to local after it was set to COPS, the QoS policy reverts back to the local configuration stored in NVRAM.

Examples

This example shows how to set the policy source to local NVRAM:

```
Console> (enable) set port qos 5/5 policy-source local
QoS policy source set to local on port(s) 5/1-48.
Console> (enable)
```

This example shows the output if you attempt to set the policy source to COPS and no COPS servers are available:

```
Console> (enable) set port qos 5/5 policy-source cops
QoS policy source for the switch set to COPS.
Warning: No COPS servers configured. Use the 'set cops server' command
to configure COPS servers.
Console> (enable)
```

This example shows the output if you set the policy source to COPS and the switch is set to local configuration (using the **set qos policy-source** command):

```
Console> (enable) set port qos 5/5 policy-source cops
QoS policy source set to COPS on port(s) 5/1-48.
Warning: QoS policy source for the switch set to use local configuration.
Console> (enable)
```

Related Commands

clear qos config
show port qos

set port qos trust

To set the trusted state of a port, use the **set port qos trust** command; for example, whether or not the packets arriving at a port are trusted to carry the correct classification.

set port qos *mod/ports...* **trust** {**untrusted** | **trust-cos** | **trust-ipprec** | **trust-dscp**}

Syntax Description

mod/ports...	Number of the module and the ports on the module.
untrusted	Specifies that packets need to be reclassified from the matching access control entry (ACE).
trust-cos	Specifies that although the CoS bits in the incoming packets are trusted, the ToS is invalid and a valid value needs to be derived from the CoS bits.
trust-ipprec	Specifies that although the ToS and CoS bits in the incoming packets are trusted, the ToS is invalid and the ToS is set as IP precedence.
trust-dscp	Specifies that the ToS and CoS bits in the incoming packets can be accepted as is with no change.

Defaults

The default is **untrusted**; when you disable QoS, the default is **trust-cos** on Layer 2 switches and **trust-dscp** on Layer 3 switches.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you disable QoS, the default is **trust-cos** on Layer 2 switches and **trust-dscp** on Layer 3 switches.

This command is not supported by the NAM.

On 10/100 ports, you can use only the **set port qos trust** command to activate the receive-drop thresholds. To configure a trusted state, you have to convert the port to port-based QoS, define an ACL that defines all (or the desired subset) of ACEs to be trusted, and attach the ACL to that port.

Examples

This example shows how to set the port to a trusted state:

```
Console> (enable) set port qos 3/7 trust trust-cos
Port 3/7 qos set to trust-cos.
Console> (enable)
```

This example shows the output if you try to set the trust state on a 10/100 port:

```
Console> (enable) set port qos 3/28 trust trust-cos
Trust type trust-cos not supported on this port.
Receive thresholds are enabled on port 3/28.
Port  3/28 qos set to untrusted.
Console> (enable)
```

Related Commands

set port qos
set port qos cos
show port qos
show qos info

set port qos trust-device

To configure the trust mode on a port on a specific device or module, use the **set port qos trust-device** command.

set port qos *mod/ports...* **trust-device** {**none** | **ciscoipphone**}

Syntax Description

mod/ports...	Number of the module and the ports on the module.
none	Sets the device trust mode to disable.
ciscoipphone	Trusts only Cisco IP phones.

Defaults

By default, the device trust mode for each port is set to **none**.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to trust only Cisco IP phones on port 4/1:

```
Console> (enable) set port qos 4/1 trust-device ciscoipphone
Port 4/1 set to only trust device of type ciscoIPPhone.
Console> (enable)
```

This example shows how to disable the device trust on port 4/1:

```
Console> (enable) set port qos 4/1 trust-device none
Port 4/1 trust device feature disabled.
Console> (enable)
```

Related Commands

show port qos

set port qos trust-ext

To configure the access port on a Cisco IP phone connected to the switch port, use the **set port qos trust-ext** command.

set port qos *mod/ports...* **trust-ext** {**trusted** | **untrusted**}

Syntax Description

mod/ports...	Number of the module and the ports on the module.
trusted	Specifies that all traffic received through the access port passes through the phone switch unchanged.
untrusted	Specifies that all traffic in 802.1Q or 802.1p frames received through the access port is marked with a configured Layer 2 CoS value.

Defaults

The default when the phone is connected to a Cisco LAN switch is untrusted mode; trusted mode is the default when the phone is not connected to a Cisco LAN switch.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Traffic in frame types other than 802.1Q or 802.1p passes through the phone switch unchanged, regardless of the access port trust state.

Examples

This example shows how to set the trust extension on ports on the connected phone to a trusted state:

```
Console> (enable) set port qos 3/7 trust-ext trusted
Port in the phone device connected to port 3/7 is configured to be trusted.
Console> (enable)
```

Related Commands

set port qos
set port qos cos
show qos info
show port qos

set port rsvp dsbm-election

To specify whether or not the switch participates in the Designated Subnet Bandwidth Manager (DSBM) election on that particular segment, use the **set port rsvp dsbm-election** command.

set port rsvp *mod/port* **dsbm-election enable** | **disable** [*dsbm_priority*]

Syntax Description

mod/port	Number of the module and the port.
enable	Enables participation in the DSBM election.
disable	Disables participation in the DSBM election.
dsbm_priority	(Optional) DSBM priority; valid values are from 128 to 255.

Defaults

The default is DSBM is disabled; the default *dsbm_priority* is 128.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to enable participation in the DSBM election:

```
Console> (enable) set port rsvp 2/1,3/2 dsbm-election enable 232
DSBM election enabled for ports 2/1,3/2.
DSBM priority set to 232 for ports 2/1,3/2.
This DSBM priority will be used during the next election process.
Console> (enable)
```

This example shows how to disable participation in the DSBM election:

```
Console> (enable) set port rsvp 2/1 dsbm-election disable
DSBM election disabled for ports(s)  2/1.
Console> (enable)
```

This example shows the output when you enable participation in the DSBM election on a port that is not forwarding:

```
Console> (enable) set port rsvp 2/1,3/2 dsbm-election enable 232
DSBM enabled and priority set to 232 for ports 2/1,3/2.
Warning: Port 2/1 not forwarding. DSBM negotiation will start after port starts forwarding
on the native vlan.
Console> (enable)
```

Related Commands

show port rsvp

set port security

To configure port security on a port or range of ports, use the **set port security** command.

set port security *mod*[*/port...*] [**enable** | **disable**] [*mac_addr*] [**age** {*age_time*}] [**maximum** {*num_ of_mac*}] [**shutdown** {*shutdown_time*}] [**unicast-flood** {**enable** | **disable**}] [**violation** {**shutdown** | **restrict**}]

set port security *mod/port* **timer-type** {**absolute** | **inactivity**}

set port security auto-configure {**enable** | **disable**}

set port security *mod/port mac_addr* [*vlan_list*]

Syntax Description

mod[*/port...*]	Number of the module and optionally, the port on the module.
enable	(Optional) Enables port security or unicast flooding.
disable	(Optional) Disables port security or unicast flooding.
mac_addr	(Optional) Secure MAC address of the enabled port.
age *age_time*	(Optional) Specifies the duration for which addresses on the port will be secured; valid values are **0** (to disable) and from 1 to 1440 (minutes).
maximum *num_of_mac*	(Optional) Specifies the maximum number of MAC addresses to secure on the port; valid values are from 1 to 4097.
shutdown *shutdown_time*	(Optional) Specifies the duration for which a port will remain disabled in case of a security violation; valid values are **0** (to disable) and from 1 to 1440 (minutes).
unicast-flood	(Optional) Specifies unicast flooding.
violation	(Optional) Specifies the action to be taken in the event of a security violation.
shutdown	(Optional) Shuts down the port in the event of a security violation.
restrict	(Optional) Restricts packets from unsecure hosts.
mod/port	Number of the module and the port on the module.
timer-type	Specifies the type of aging to be applied to the autoconfigured addresses on a per-port basis.
absolute	Specifies absolute aging. See the "Usage Guidelines" section for more information.
inactivity	Specifies inactivity aging. See the "Usage Guidelines" section for more information.
auto-configure	Automatically configures all learned MAC addresses on a secure port. See the "Usage Guidelines" section for more information.
enable	Enables the automatic configuration feature.
disable	Disables the automatic configuration feature.
mac_addr	MAC address. See the "Usage Guidelines" section for more information.
vlan_list	(Optional) VLAN or list of VLANs. See the "Usage Guidelines" section for more information.

Defaults

The default port security configuration is as follows:

- Port security is disabled.
- Number of secure addresses per port is one.
- Violation action is shutdown.
- Age is permanent. (Addresses are not aged out.)
- Shutdown time is indefinite.
- Timer type is set to absolute aging.
- Unicast flooding is enabled.
- The automatic configuration feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

If you enter the **set port security enable** command but do not specify a MAC address, the first MAC address seen on the port becomes the secure MAC address.

You can specify the number of MAC addresses to secure on a port. You can add MAC addresses to this list of secure addresses. If you change the number of addresses to a value that is less than the current value, some configured addresses might be cleared. A warning message displays when you attempt to reduce the number of addresses.

The **set port security violation** command allows you to specify whether you want the port to shut down or to restrict access to insecure MAC addresses only. The shutdown time allows you to specify the duration of shutdown in the event of a security violation.

We recommend that you configure the age timer and the shutdown timer if you want to move a host from one port to another when port security is enabled on those ports. If the *age_time* value is less than or equal to the *shutdown_time* value, the moved host will function again in an amount of time equal to the *shutdown_time* value. The age timer begins upon learning the first MAC address, and the disable timer begins when there is a security violation.

If you disable unicast flooding on a port, the port will drop unicast flood packets when it reaches the maximum number of MAC addresses allowed.

You can secure only unicast MAC addresses through the CLI. Unicast MAC addresses can also be learned dynamically. Multicast MAC addresses cannot be secured.

You can apply one of two types of aging for automatically learned addresses on a secure port:

- Absolute aging times out the MAC address after the *age_time* has been exceeded, regardless of the traffic pattern. This is the default for any secured port, and the *age_time* is set to 0.
- Inactivity aging times out the MAC address only after the *age_time* of inactivity from the corresponding host has been exceeded.

Enabling the automatic configuration feature automatically configures learned MAC addresses on secure ports. If a secure port shuts down because of a violation, if the port is disabled, or if port security is disabled, all learned MAC addresses are converted to configured MAC addresses and retained on the port. If this feature is disabled and the secure port experiences any of the same conditions, all learned MAC addresses are cleared.

When you configure a MAC address on a port, you can associate a VLAN or multiple VLANs to that MAC address by enter the **set port security** *mod/port mac_addr* [*vlan_list*] command. If you do not specify a *vlan_list* argument, the MAC address is configured on the native VLAN of the specified port.

Examples

This example shows how to set port security with a learned MAC address:

```
Console> (enable) set port security 3/1 enable
Port 3/1 port security enabled with the learned mac address.
Console> (enable)
```

This example shows how to set port security with a specific MAC address:

```
Console> (enable) set port security 3/1 enable 00-02-03-04-05-06
Port 3/1 port security enabled with 00-02-03-04-05-06 as the secure mac address.
Console> (enable)
```

This example shows how to set the maximum MAC address limit to 10:

```
Console> (enable) set port security 3/37 max 10
Setting the Maximum Addresses Limit to a value lesser than the
current value might result in configured addresses getting cleared
Do you want to continue (y/n) [n]?y
Port 3/37 security maximum address 10.
Console> (enable)
```

This example shows how to set the shutdown time to 600 minutes on port 7/7:

```
Console> (enable) set port security 7/7 shutdown 600
Secure address shutdown time set to 600 minutes for port 7/7.
Console> (enable)
```

This example shows how to configure the port to drop all packets that are coming in on the port from insecure hosts:

```
Console> (enable) set port security 7/7 violation restrict
Port security violation on port 7/7 will cause insecure packets to be dropped.
Console> (enable)
```

This example shows how to enable unicast flooding on port 4/1:

```
Console> (enable) set port security 4/1 unicast-flood enable
Port 4/1 security flood mode set to enable.
Console> (enable)
```

This example shows how to disable unicast flooding on port 4/1:

```
Console> (enable) set port security 4/1 unicast-flood disable
WARNING: Trunking & Channelling will be disabled on the port.
Port 4/1 security flood mode set to disable.
Console> (enable)
```

This example shows how to set the aging type on a port to absolute aging:

```
Console> (enable) set port security 5/1 timer-type absolute
Port 5/1 security timer type absolute.
Console> (enable)
```

This example shows how to set the aging type on a port to inactivity aging:

```
Console> (enable) set port security 5/1 timer-type inactivity
Port 5/1 security timer type inactive.
Console> (enable)
```

This example shows how to enable the automatic configuration feature:

```
Console> (enable) set port security auto-configure enable
Automatic configuration of secure learnt addresses enabled.
Console> (enable)
```

This example shows how to associate a MAC address with a list of VLANs:

```
Console> (enable) set port security 3/37 00-00-aa-00-00-aa 20,30
Mac address 00-00-aa-00-00-aa set for port 3/37 on vlan 20.
Mac address 00-00-aa-00-00-aa set for port 3/37 on vlan 30.
Console> (enable)
```

This example shows what happens if you configure a secure MAC address without specifying the *vlan_list* argument. Note that the MAC address is automatically configured on the native VLAN:

```
Console> (enable) set port security 3/38 00-00-aa-00-00-aa
Mac address 00-00-aa-00-00-aa set for port 3/38 on vlan 1
Console> (enable)
```

If a specified VLAN is not the native VLAN of the port (in the case of an access port) or if it is not an allowed VLAN on a trunk port, the command results in these messages:

```
Console> (enable) set port security 3/38 00-00-aa-00-00-aa 20
Vlan 20 is not the native vlan for access port 3/38.
Console> (enable)

Console> (enable) set port security 3/37 00-00-aa-00-00-aa 20,30,100
Vlan 100 is not a configured vlan on trunk/vvid port 3/37
Console> (enable)
```

Related Commands

clear port security
show config
show port security

set port security-acl

To specify the port access control list (PACL) mode, use the **set port security-acl** command.

set port security-acl *mod/ports...* {**port-based** | **vlan-based** | **merge**}

Syntax Description

mod/ports...	Number of the module and the ports on the module.
port-based	Specifies the mode in which the PACL overrides the VACL and RACL.
vlan-based	Specifies the mode in which the VACL and RACL override the PACL.
merge	Specifies the mode in which the ingress PACL, VACL, and RACL merge.

Defaults

The port security ACL mode is **vlan-based** to keep the existing VACL configuration active.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configuring port access control lists is only available on PFC3-based forwarding engines.

For more information about PACLs, refer to the "Configuring Access Control" chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example shows how to set the PACL mode to port-based mode on port 3/1:

```
Console> (enable) set port security-acl 3/1 port-based
Warning: Vlan-based ACL features will be disabled on port(s) 3/1.
ACL interface is set to port-based mode for port(s) 3/1.
Console> (enable)
```

This example shows how to set the PACL mode to VLAN-based mode on port 3/1:

```
Console> (enable) set port security-acl 3/1 vlan-based
ACL interface is set to vlan-based mode for port(s) 3/1.
Console> (enable)
```

This example shows how to set the PACL mode to merge mode on port 3/1:

```
Console> (enable) set port security-acl 3/1 merge
ACL interface is set to merge mode for port(s) 3/1.
Console> (enable)
```

This example shows the message that displays when merge mode cannot work because a port is a trunk port:

```
Console> (enable) set port security-acl 3/1-4 merge
ACL interface cannot be in merge mode on multi-vlan access port 3/1.
ACL interface is set to merge mode for port(s) 3/2.
ACL interface is set to merge mode for port(s) 3/3.
ACL interface is set to merge mode for port(s) 3/4.
Console> (enable)
```

Related Commands

show port security-acl

set port speed

To configure the speed of a port interface, use the **set port speed** command.

set port speed *mod/port* {**10** | **100** | **1000** | **auto** | **auto-10-100**}

Syntax Description

mod/port	Number of the module and the port on the module.
10 | **100** | **1000**	Sets a port speed for 10BASE-T, 100BASE-T, or 1000BASE-T ports.
auto	Specifies autonegotiation for transmission speed and duplex mode on 10/100 Fast Ethernet ports.
auto-10-100	Specifies autonegotiation for speed and duplex mode on 10/100/1000 Fast Ethernet ports. Only 10-Mbps and 100-Mbps Fast Ethernet ports are negotiated; 1000-Mbps Fast Ethernet ports are not negotiated.

Defaults

The default is **auto**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

In most cases, autonegotiation manages transmission speed, duplex mode, the master link, and the slave link. The exception applies to 16-port 10/100/1000BASE-T Ethernet modules, where autonegotiation manages transmission speed only.

You can configure Fast Ethernet interfaces on the 10/100-Mbps Fast Ethernet switching module to either 10, 100, or 1000 Mbps, or to autosensing mode, allowing the interfaces to sense and distinguish between 10- and 100-Mbps port transmission speeds and full-duplex or half-duplex port transmission types at a remote port connection. If you set the interfaces to autosensing, they configure themselves automatically to operate at the proper speed and transmission type.

Examples

This example shows how to configure port 1, module 2 to **auto**:

```
Console> (enable) set port speed 2/1 auto
Port 2/1 speed set to auto-sensing mode.
Console> (enable)
```

This example shows how to configure the port speed on port 2, module 2 to **10** Mbps:

```
Console> (enable) set port speed 2/2 10
Port 2/2 speed set to 10 Mbps.
Console> (enable)
```

Related Commands

show port

set port sync-restart-delay

To specify the synchronization restart delay of a port, use the **set port sync-restart-delay** command.

set port sync-restart-delay *mod/port delay*

Syntax Description

mod/port	Number of the module and the port on the module.
delay	Delay time in milliseconds; the delay range is 200 to 60000 milliseconds (60 seconds).

Defaults

The default delay time is 210 milliseconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The more dense wavelength division multiplexing (DWDM) equipment you have in the network, usually the longer the synchronization delay should be.

The **set port sync-restart-delay** and **show port sync-restart-delay** commands are available in both binary mode and text configuration mode.

Use the **clear config** command to reset the synchronization delay to 210 milliseconds.

Related Commands

clear config
show port sync-restart-delay

set port trap

To enable or disable the operation of the standard Simple Network Management Protocol (SNMP) link trap (up or down) for a port or range of ports, use the **set port trap** command.

set port trap *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Activates the SNMP link trap.
disable	Deactivates the SNMP link trap.

Defaults

The default is all port traps are disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

To set SNMP traps, enter the **set snmp trap** command.

Examples

This example shows how to enable the SNMP link trap for module 1, port 2:

```
Console> (enable) set port trap 1/2 enable
Port 1/2 up/down trap enabled.
Console> (enable)
```

Related Commands

show port trap

set port unicast-flood

To configure the switch to drop Unicast Flood traffic on an Ethernet port, use the **set port unicast-flood** command.

set port unicast-flood *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables unicast flood and disables unicast flood blocking.
disable	Disables unicast flood and enables unicast flood blocking.

Defaults

Unicast flood blocking is disabled on all ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Only Ethernet ports can block unicast flood traffic.

You must have a static CAM entry associated with the Ethernet port before you disable unicast flood on the port, or you will lose network connectivity when you disable unicast flood. You can verify a static CAM entry exists by entering the **show cam static** command.

You cannot configure a port channel on a unicast flood disabled port, and you cannot disable unicast flood on a port channel.

You cannot disable unicast flood on a SPAN destination port, and you cannot configure a SPAN destination on a unicast flood disabled port.

You cannot disable unicast flood on a trunk port. If you do, an error message will be displayed.

If you disable unicast flood on an Ethernet port that has port security enabled on it, the switch stops sending Unicast Flood packets to the port once the switch has learned the allowed maximum number of MAC addresses. When the learned MAC address count drops below the maximum number allowed, unicast flooding is automatically reenabled.

Unicast flood blocking and GARP VLAN Registration Protocol (GVRP) are mutually exclusive. You cannot disable unicast flood and exchange VLAN configuration information with GVRP switches at the same time.

Examples

This example shows how to enable unicast flood traffic on module 4, port 1 of a switch:

```
Console> (enable) set port unicast-flood 4/1 disable
WARNING: Trunking & Channelling will be disabled on the port.
Unicast Flooding is successfully disabled on the port 4/1.
Console> (enable)
```

This example shows how to disable unicast flood traffic on module 4, port 1 of a switch:

```
Console> (enable) set port unicast-flood 4/1 enable
Unicast Flooding is successfully enabled on the port 4/1.
Console> (enable)
```

Related Commands

show port unicast-flood

set port vlan-mapping

To configure VLAN mapping on a per-port basis, use the **set port vlan-mapping** command.

set port vlan-mapping *mod/port* {**enable** | **disable**}

set port vlan-mapping *mod/port source_vlan_id translated_vlan_id*

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables VLAN mapping.
disable	Disables VLAN mapping.
source_vlan_id	Number of the source VLAN; valid values are from 1 to 4094.
translated_vlan_id	Number of the VLAN that is mapped to the source VLAN; valid values are from 1 to 4094.

Defaults

VLAN mapping is disabled on all ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

VLAN mapping occurs only if you enter the **set port vlan-mapping** *mod/port* **enable** command and only if the port is operationally trunking. The **set port vlan-mapping** *mod/port source_vlan_id translated_vlan_id* command takes effect only after VLAN mapping is enabled.

When you enable VLAN mapping and specify a *source_vlan_id* value and a *translated_vlan_id* value, traffic coming in on a trunk port with the *source_vlan_id* value is translated to the VLAN with the *translated_vlan_id* value. Also, any traffic internally tagged with the *translated_vlan_id* value is tagged with the *source_vlan_id* value before leaving the port.

Some port ASICs support VLAN mapping only on a per-ASIC basis, but VLAN mapping is enabled or disabled on a per-port basis. With these types of ASICs, the **set port vlan-mapping** *mod/port* {**enable** | **disable**} command is applied only to the port configuration and not to the ASIC.

You cannot enable global VLAN mapping and per-port/per-ASIC VLAN mapping simultaneously.

Examples

This example shows how to enable VLAN mapping on a specified port:

```
Console> (enable) set port vlan-mapping 7/1 enable
VLAN mapping enabled on port 7/1.
Console> (enable)
```

8.6 EFT Copy

This example shows how to enable port VLAN mapping and to configure VLAN mapping on an individual port. In this example, module 7 is the 48-port 10/100/1000 switching module (WS-X6748-GE-TX). This module supports per-ASIC VLAN mapping; 1 ASIC supports 12 ports.

```
Console> (enable) set port vlan-mapping 7/1 enable
VLAN mapping enabled on port 7/1.
Console> (enable) set port vlan-mapping 7/1 2002 3003
VLAN 2002 mapped to VLAN 3003 on ports 7/1-12.
Console> (eanble)
```

In this example, module 5 is the 1-port 10GBASE-E serial 10-Gigabit Ethernet module (WS-X6502-10GE). This module supports per-port VLAN mapping.

```
Console> (enable) set port vlan-mapping 5/1 2002 3003
VLAN 2002 mapped to VLAN 3003 on port 5/1.
Console> (enable)
```

In this example, module 7 is the 48-port 10/100/1000 switching module (WS-X6748-GE-TX). This module supports per-ASIC VLAN mapping; 1 ASIC supports 12 ports. In this example, ports 7/1-4 are part of an EtherChannel.

```
Console>(enable) set port vlan-mapping 7/1 2002 3003
VLAN 2002 mapped to VLAN 3003 on ports 7/1-12.
Console>(enable)
```

Related Commands

clear port vlan-mapping
show port vlan-mapping

set port voice interface dhcp

To set the port voice interface for the DHCP, TFTP, and DNS servers, use the **set port voice interface dhcp** command.

set port voice interface *mod/port* **dhcp enable** [**vlan** *vlan*]

set port voice interface *mod/port* **dhcp disable** {*ipaddrspec*} {**tftp** *ipaddr*} [**vlan** *vlan*] [**gateway** *ipaddr*] [**dns** [*ipaddr*] [*domain_name*]]

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Activates the SNMP link trap.
vlan *vlan*	(Optional) Specifies a VLAN interface; valid values are from 1 to 4094.
disable	Deactivates the SNMP link trap.
ipaddrspec	IP address and mask; see the “Usage Guidelines” section for format instructions.
tftp *ipaddr*	Specifies the number of the TFTP server IP address or IP alias in dot notation a.b.c.d.
gateway *ipaddr*	(Optional) Specifies the number of the gateway server IP address or IP alias in dot notation a.b.c.d.
dns	(Optional) Specifies the DNS server.
ipaddr	(Optional) Number of the DNS IP address or IP alias in dot notation a.b.c.d.
domain_name	(Optional) Name of the domain.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The *ipaddrspec* format is {*ipaddr*} {*mask*} or {*ipaddr*}/{*mask*} {*mask*}. The *mask* is a dotted format (255.255.255.0) or number of bits (0 to 31).

You can specify a single port only when setting the IP address.

If you enable DHCP on a port, the port obtains all other configuration information from the TFTP server. When you disable DHCP on a port, the following mandatory parameters must be specified:

- If you do not specify DNS parameters, the software uses the system DNS configuration on the supervisor engine to configure the port.
- You cannot specify more than one port at a time because a unique IP address must be set for each port.

Examples

This example shows how to enable the port voice interface for the DHCP server:

```
Console> (enable) set port voice interface 7/4-8 dhcp enable
Port 7/4 DHCP enabled.
Console> (enable)
```

This example shows how to disable the set port voice interface DHCP server:

```
Console> (enable) set port voice interface 7/3 dhcp disable 171.68.111.41/24 tftp
173.32.43.11 dns 172.20.34.204 cisco.com
Port 7/3 dhcp disabled.
System DNS configurations applied.
Console> (enable)
```

This example shows how to enable the port voice interface for the DHCP server with a specified VLAN:

```
Console> (enable) set port voice interface 7/4-6 dhcp enable vlan 3
Vlan 3 configuration successful
Ports 7/4-6 DHCP enabled.
Console> (enable)
```

This example shows how to enable the port voice interface for the TFTP, DHCP, and DNS servers:

```
Console> (enable) set port voice interface dhcp enable 4/2 171.68.111.41 tftp 173.32.43.11
dhcp 198.98.4.1 dns 189.69.24.192
Port 4/2 interface set.
IP address: 171.68.111.41 netmask 255.255.0.0
TFTP server: 173.32.43.11
DHCP server: 198.98.4.1
DNS server: 189.69.24.192
Console> (enable)
```

This example shows how to enable a single port voice interface:

```
Console> (enable) set port voice interface 4/2-9 dhcp 123.23.32.1/24
Single port must be used when setting the IP address.
Console> (enable)
```

Related Commands

show port voice interface

set port vtp

To enable or disable VLAN Trunk Protocol (VTP) on a per-port basis, use the **set port vtp** command.

set port vtp *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Activates VTP.
disable	Deactivates VTP.

Defaults

VTP is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set port vtp** command allows you to enable or disable any kind of VTP interaction on a per-port basis, which may be useful on trunks leading to non-trusted hosts. When a port is disabled, no VTP packet is sent on the port, and any VTP packet received on the port is dropped.

Examples

This example shows how to disable VTP on ports 1 and 2 on module 1:

```
Console> (enable) set port vtp 1/1-2 disable
Port(s) 1/1-2 will no longer participate in VTP.
Console> (enable)
```

Related Commands

set vtp
show port vtp
show vtp

set port web-auth

To enable or disable web-based proxy authentication on a port or to specify an AAA fail policy for web-based proxy authentication, use the **set port web-auth** command.

set port web-auth *mod/port* {**disable** | **enable**}

set port web-auth *mod/port* **aaa-fail-policy** *policy-name*

Syntax Description

mod/port	Module and port number.
disable	Disables web-based proxy authentication on a port.
enable	Enables web-based proxy authentication on a port.
aaa-fail-policy	Maps an AAA fail policy for web-based proxy authentication to a specified port.
policy-name	Policy name to be mapped to the port.

Defaults

Disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Note If you have disabled web-based proxy authentication globally, web-based proxy authentication on a port may not start but will be stored in the configuration.

You must enable web-based proxy authentication globally before entering the **set port web-auth** command. To enable web-based proxy authentication globally, use the **set web-auth** command.

Before you can use the **set port web-auth** *mod/port* **aaa-fail-policy** *policy-name* command, the template for the policy must be created.

After you have specified a policy template for a port, any changes to the policy template affect only those hosts that have been moved to AAA fail state after the policy template was changed. Hosts in already existing sessions use the policy template as it was before any changes were made.

When you specify a different policy for a port, hosts in already existing sessions maintain the previously specified policy. The newly specified policy affects only new hosts entering AAA fail state.

Examples

This example shows how to enable web-based proxy authentication on a port:

```
Console> (enable) set port web-auth 1/1 enable
web-authentication successfully enabled on Interface 1/1.
Console> (enable)
```

8.6 EFT Copy

This example shows how to disable web-based proxy authentication on a port:

```
Console> (enable) set port web-auth 1/1 disable
web-authentication successfully disabled on Interface 1/1.
Console> (enable)
```

Related Commands

clear web-auth
set port critical
set port web-auth initialize
set web-auth
set web-auth login-attempts
set web-auth login-fail-page
set web-auth login-page
set web-auth quiet-timeout
set web-auth session-timeout
show port web-auth
show web-auth summary

set port web-auth initialize

To initialize a web-based proxy authentication port for authentication again, use the **set port web-auth initialize** command.

set port web-auth *mod/port* **initialize** [*ip_addr*]

Syntax Description

mod/port	Module and port number.
ip_addr	(Optional) Host IP address.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you initialize the port by entering the **set port web-auth initialize** command, you are returning the port to the first state. In this state, the IP address of the host is registered with URL redirection for redirecting any HTTP packet from this host to the supervisor engine.

If you specify the *ip_addr* argument, web-based proxy authentication is initialized for that host only. If you do not specify the *ip_addr* argument, web-based proxy authentication is initialized for all hosts.

You must enable web-based proxy authentication globally and the individual port before you can initialize a web-based proxy authentication port for authentication again. To enable web-based proxy authentication globally, use the **set web-auth** command. To enable web-based proxy authentication for an individual port, use the **set port web-auth** command.

Examples

This example shows how to initialize web-based proxy authentication again for all hosts on a port:

```
Console> (enable) set port web-auth 2/1 initialize
Initialized web-authentication for all hosts on port 2/1.
Console> (enable)
```

This example shows how to initialize web-based proxy authentication again for a specific host on a port:

```
Console> (enable) set port web-auth 2/1 initialize 10.76.34.45
Initialized web authentication for 10.76.34.45 on port 2/1
Console> (enable)
```

Related Commands

clear web-auth
set port web-auth
set web-auth
set web-auth login-attempts
set web-auth login-fail-page
set web-auth login-page
set web-auth quiet-timeout
set web-auth session-timeout
show port web-auth
show web-auth summary

set power redundancy

To turn redundancy between the power supplies on or off, use the **set power redundancy** command.

set power redundancy {**enable** | **disable**}

Syntax Description

enable	Activates redundancy between the power supplies.
disable	Deactivates redundancy between the power supplies.

Defaults

The default is power redundancy is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

In a system with dual power supplies, this command turns redundancy on or off between the power supplies. In a redundant configuration, the power available to the system is the maximum power capability of the weakest power supply.

In a nonredundant configuration, the power available to the system is the sum of the power capability of both power supplies.

Examples

This example shows how to activate redundancy between power supplies:

```
Console> (enable) set power redundancy enable
Power supply redundancy enabled.
Console> (enable)
```

This example shows how to deactivate redundancy between power supplies:

```
Console> (enable) set power redundancy disable
Power supply redundancy disabled.
Console> (enable)
```

Related Commands

show environment
show system

set prompt

To change the prompt for the CLI, use the **set prompt** command.

set prompt *prompt_string*

Syntax Description

prompt_string	String to use as the command prompt.

Defaults

The default is the prompt is set to Console>.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use the **set system name** command to assign a name to the switch, the switch name is used as the prompt string. However, if you specify a different prompt string using the **set prompt** command, that string is used for the prompt.

Examples

This example shows how to set the prompt to system100>:

```
Console> (enable) set prompt system100>
system100> (enable)
```

Related Commands

set system name

set protocolfilter

To activate or deactivate protocol filtering on Ethernet VLANs and on nontrunking Ethernet, Fast Ethernet, and Gigabit Ethernet ports, use the **set protocolfilter** command.

set protocolfilter {**enable** | **disable**}

Syntax Description

enable	Activates protocol filtering.
disable	Deactivates protocol filtering.

Defaults

The default is protocol filtering is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Protocol filtering is supported only on Ethernet VLANs and on nontrunking EtherChannel ports.

This feature is not supported on the Supervisor Engine 720 with PFC3.

Examples

This example shows how to activate protocol filtering:

```
Console> (enable) set protocolfilter enable
Protocol filtering enabled on this switch.
Console> (enable)
```

This example shows how to deactivate protocol filtering:

```
Console> (enable) set protocolfilter disable
Protocol filtering disabled on this switch.
Console> (enable)
```

Related Commands

show protocolfilter

set pvlan

To bind the isolated or community VLAN to the primary VLAN and assign the isolated or community ports to the private VLAN, use the **set pvlan** command.

set pvlan *primary_vlan* {*isolated_vlan* | *community_vlan* | *twoway_community_vlan*}
[*mod/port* | **sc0**]

Caution We recommend that you read and understand the "Configuring VLANs" chapter in the *Catalyst 6500 Series Software Configuration Guide* before using this command.

Syntax Description

primary_vlan	Number of the primary VLAN.
isolated_vlan	Number of the isolated VLAN.
community_vlan	Number of the community VLAN.
twoway_community_vlan	Number of the two-way community VLAN.
mod/port	(Optional) Module and port numbers of the isolated or community ports.
sc0	(Optional) Specifies the inband port sc0.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must set the primary VLAN, isolated VLAN, and community VLANs using the **set vlan pvlan-type** *pvlan_type* command before making the association with the **set pvlan** command.

Each isolated or community VLAN can have only one primary VLAN associated with it. A primary VLAN may have one isolated or multiple community VLANs associated to it.

Although you can configure sc0 as a private port, you cannot configure sc0 as a promiscuous port.

Examples

This example shows how to map VLANs 901, 902, and 903 (isolated or community VLANs) to VLAN 7 (the primary VLAN):

```
Console> (enable) set pvlan 7 901 4/3
Port 4/3 is successfully assigned to vlan 7, 901 and is made an isolated port.
Console> (enable) set pvlan 7 902 4/4-5
Ports 4/4-5 are successfully assigned to vlan 7, 902 and are made community ports.
Console> (enable) set pvlan 7 903 4/6-7
Ports 4/6-7 are successfully assigned to vlan 7, 903 and are made community ports.
Console> (enable) set pvlan 300 301 sc0
Successfully set the following ports to Private Vlan 300, 301:
sc0
Console> (enable)
```

This example shows the message that appears when VLAN port-provisioning verification is enabled:

```
Console> (enable) set pvlan 20 30 2/2
Port Provisioning Verification is enabled on the switch.
To move port(s) into the VLAN
Use 'set pvlan <primary_vlan> <secondary_vlan> <port> <pri_vlan_name> <sec_vlan_name>'
command.
Console> (enable)
```

Related Commands

clear config pvlan
clear pvlan mapping
clear vlan
set pvlan mapping
set vlan
set vlan verify-port-provisioning
show pvlan
show pvlan capability
show pvlan mapping
show vlan
show vlan verify-port-provisioning

set pvlan mapping

To map isolated or community VLANs to the primary VLAN on the promiscuous port, use the **set pvlan mapping** command.

set pvlan mapping *primary_vlan* {*isolated_vlan* | *community_vlan* | *twoway_community_vlan*} *mod/port*

Syntax Description

primary_vlan	Number of the primary VLAN.
isolated_vlan	Number of the isolated VLAN.
community_vlan	Number of the community VLAN.
twoway_community_vlan	Number of the two-way community VLAN.
mod/port	Module and port number of the promiscuous port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must set the primary VLAN, isolated VLANs, and community VLANs using the **set vlan pvlan-type** command combined with the **set pvlan** command before you can apply the VLANs on any of the promiscuous ports with the **set pvlan mapping** command.

You should connect the promiscuous port to an external device for the ports in the private VLAN to communicate with any other device outside the private VLAN.

You should apply this command for each primary or isolated (community) association in the private VLAN.

Examples

This example shows how to remap community VLAN 903 to the primary VLAN 901 on ports 3 through 5 on module 8:

```
Console> (enable) set pvlan mapping 901 903 8/3-5
Successfully set mapping between 901 and 903 on 8/3-5.
Console> (enable)
```

Related Commands

clear pvlan mapping
clear vlan
set pvlan
set vlan
show pvlan
show pvlan mapping
show vlan

set qos

To turn on or turn off QoS functionality on the switch, use the **set qos** command.

set qos enable | disable

Syntax Description

enable	Activates QoS functionality.
disable	Deactivates QoS functionality.

Defaults

The default is QoS functionality is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Refer to the *Catalyst 6500 Series Switch Software Configuration Guide* for information on how to change the QoS default configurations.

When you enable and disable QoS in quick succession, a bus timeout might occur.

If you enable or disable QoS on channel ports with different port types, channels might break or form.

Examples

This example shows how to enable QoS:

```
Console> (enable) set qos enable
QoS is enabled.
Console> (enable)Console> (enable)
```

This example shows how to disable QoS:

```
Console> (enable) set qos disable
QoS is disabled.
Console> (enable)
```

Related Commands

show qos info

set qos acl default-action

To set the ACL default actions, use the **set qos acl default-action** command.

set qos acl default-action ip {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [{**microflow** *microflow_name*}] [{**aggregate** *aggregate_name*}] [**input** | **output**]

set qos acl default-action ipx {{**dscp** *dscp*} | **trust-cos**} [{**microflow** *microflow_name*}] [{**aggregate** *aggregate_name*}]

set qos acl default-action {**ipx** | **mac**} {{**dscp** *dscp*} | **trust-cos**} [{**aggregate** *aggregate_name*}] [**input** | **output**]

set qos acl default-action trust-override {**enable** | **disable**}

Syntax Description

ip	Specifies the IP ACL default actions.
dscp *dscp*	Sets the DSCP to be associated with packets matching this stream.
trust-cos	Specifies DSCP is derived from the packet CoS.
trust-ipprec	Specifies DSCP is derived from the packet IP precedence.
trust-dscp	Specifies DSCP is contained in the packet already.
microflow *microflow_name*	(Optional) Specifies the name of the microflow policing rule to be applied to packets matching the ACE.
aggregate *aggregate_name*	(Optional) Specifies the name of the aggregate policing rule to be applied to packets matching the ACE.
input	(Optional) Specifies the receive side.
output	(Optional) Specifies the transmit side.
ipx	Specifies the IPX ACL default actions.
mac	Specifies the MAC ACL default actions.
trust-override	Specifies the overriding of the QoS classification ACL trust.
enable	Enables the overriding of the QoS classification ACL trust.
disable	Disables the overriding of the QoS classification ACL trust.

Defaults

The default is no ACL is set up. When you enable QoS, the default-action is to classify everything to best effort and to do no policing. When you disable QoS, the default-action is **trust-dscp** on all packets and no policing.

The overriding of the QoS classification ACL trust is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering this command are saved to NVRAM and the switch and do not require that you enter the **commit** command.

Only PFC3 supports the **input** and **output** keywords.

Examples

This example shows how to set up the IP ACL default actions:

```
Console> (enable) set qos acl default-action ip dscp 5 microflow micro aggregate agg
QoS default-action for IP ACL is set successfully.
Console> (enable)
```

This example shows how to set up the IPX ACL default actions:

```
Console> (enable) set qos acl default-action ipx dscp 5 microflow micro aggregate agg
QoS default-action for IPX ACL is set successfully.
Console> (enable)
```

This example shows how to set up the MAC ACL default actions:

```
Console> (enable) set qos acl default-action mac dscp 5 microflow micro aggregate agg
QoS default-action for MAC ACL is set successfully.
Console> (enable)
```

Related Commands

clear qos acl
show qos acl info

set qos acl ip

To create or add IP access lists, use the **set qos acl ip** command.

set qos acl ip {*acl_name*} {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] {*src_ip_spec*} [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set qos acl ip {*acl_name*} {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] {*protocol*} {*src_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set qos acl ip {*acl_name*} {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **icmp** {*src_ip_spec*} {*dest_ip_spec*} [*icmp_type* [*icmp_code*] | *icmp_message*] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set qos acl ip {*acl_name*} {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **tcp** {*src_ip_spec*} [{*operator*} {*port*} [*port*]] {*dest_ip_spec*} [{*operator*} {*port*} [*port*]] [**established**] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set qos acl ip {*acl_name*} {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **udp** {*src_ip_spec*} [{*operator*} {*port*} [*port*]] {*dest_ip_spec*} [{*operator*} {*port*} [*port*]] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set qos acl ip {*acl_name*} {{**dscp** *dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **igmp** {*src_ip_spec*} {*dest_ip_spec*} [*igmp_type*] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
dscp *dscp*	Sets CoS and DSCP from configured DSCP values; valid values are from 0 to 63.
trust-cos	Specifies DSCP is derived from the packet CoS.
trust-ipprec	Specifies DSCP is derived from the packet IP precedence.
trust-dscp	Specifies DSCP is contained in the packet already.
microflow *microflow_name*	(Optional) Specifies the name of the microflow policing rule to be applied to packets matching the ACE.
aggregate *aggregate_name*	(Optional) Specifies the name of the aggregate policing rule to be applied to packets matching the ACE.
src_ip_spec	Source IP address and the source mask. See the “Usage Guidelines” section for the format.
precedence *precedence*	(Optional) Specifies the precedence level to compare with an incoming packet; valid values are from 0 to 7 or by name. See the “Usage Guidelines” section for a list of valid names.
dscp-field *dscp*	(Optional) Specifies the DSCP field level to compare with an incoming packet. Valid values are from 0 to 63.

8.6 EFT Copy

before *editbuffer_index*	(Optional) Inserts the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Replaces an ACE with the new ACE.
protocol	Keyword or number of an IP protocol; valid numbers are from 0 to 255 representing an IP protocol number. See the "Usage Guidelines" section for the list of valid keywords and corresponding numbers.
dest_ip_spec	Destination IP address and the destination mask. See the "Usage Guidelines" section for the format.
icmp	Specifies ICMP.
icmp-type	(Optional) ICMP message type; valid values are from 0 to 255.
icmp-code	(Optional) ICMP message code; valid values are from 0 to 255.
icmp-message	(Optional) ICMP message type name or ICMP message type and code name. See the "Usage Guidelines" section for a list of valid names.
tcp	Specifies TCP.
operator	(Optional) Operands; valid values include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).
port	(Optional) TCP or UDP port number or name; valid port numbers are from 0 to 65535. See the "Usage Guidelines" section for a list of valid names.
established	(Optional) For TCP protocol only; specifies an established connection.
udp	Specifies UDP.
igmp	Specifies IGMP.
igmp_type	(Optional) IGMP message type; valid values are from 0 to 15.

Defaults

The default is there are no ACLs.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering any of these commands are saved to NVRAM and the switch only after you enter the **commit** command. Enter ACEs in batches and then enter the **commit** command to save them in NVRAM and the switch.

Use the **show qos acl info** command to view the edit buffer.

The **dscp** *dscp*, **trust-cos**, **trust-ipprec**, and **trust-dscp** keywords and variables are used to select a marking rule. Refer to the *Catalyst 6500 Series Switch Software Configuration Guide* for additional marking rule information.

The optional **microflow** *microflow_name* and **aggregate** *aggregate_name* keywords and variables are used to configure policing in the ACE. Refer to the *Catalyst 6500 Series Switch Software Configuration Guide* for additional policing rule information.

The *src_ip_spec*, optional **precedence** *precedence*, or **dscp-field** *dscp* keywords and variables are used to configure filtering.

When you enter the ACL name, follow these naming conventions:

- Maximum of 31 characters long and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types
- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer

When you specify the source IP address and the source mask, use the form *source_ip_address source_mask* and follow these guidelines:

- The *source_mask* is required; 0 indicates a "care" bit, and 1 indicates a "don't-care" bit.
- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0.

When you enter a destination IP address and the destination mask, use the form *destination_ip_address destination_mask*. The destination mask is required.

- Use a 32-bit quantity in a four-part dotted-decimal format
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255
- Use **host**/source as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0

Valid names for *precedence* are critical, flash, flash-override, immediate, internet, network, priority, and routine.

Valid names for *tos* are max-reliability, max-throughput, min-delay, min-monetary-cost, and normal.

Valid *protocol* keywords include **icmp** (1), **ip**, **ipinip** (4), **tcp** (6), **udp** (17), **igrp** (9), **eigrp** (88), **gre** (47), **nos** (94), **ospf** (89), **ahp** (51), **esp** (50), **pcp** (108), and **pim** (103). The IP protocol number is displayed in parentheses. Use the keyword **ip** to match any Internet Protocol.

ICMP packets that are matched by ICMP message type can also be matched by the ICMP message code.

Valid names for *icmp_type* and *icmp_code* are administratively-prohibited, alternate-address, conversion-error, dod-host-prohibited, dod-net-prohibited, echo, echo-reply, general-parameter-problem, host-isolated, host-precedence-unreachable, host-redirect, host-tos-redirect, host-tos-unreachable, host-unknown, host-unreachable, information-reply, information-request, mask-reply, mask-request, mobile-redirect, net-redirect, net-tos-redirect, net-tos-unreachable, net-unreachable, network-unknown, no-room-for-option, option-missing, packet-too-big, parameter-problem, port-unreachable, precedence-unreachable, protocol-unreachable, reassembly-timeout, redirect, router-advertisement, router-solicitation, source-quench, source-route-failed, time-exceeded, timestamp-reply, timestamp-request, traceroute, ttl-exceeded, and unreachable.

If the *operator* is positioned after the source and source-wildcard, it must match the source port. If the *operator* is positioned after the destination and destination-wildcard, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number only.

TCP port names can be used only when filtering TCP. Valid names for TCP ports are bgp, chargen, daytime, discard, domain, echo, finger, ftp, ftp-data, gopher, hostname, irc, klogin, kshell, lpd, nntp, pop2, pop3, smtp, sunrpc, syslog, tacacs-ds, talk, telnet, time, uucp, whois, and www.

UDP port names can be used only when filtering UDP. Valid names for UDP ports are biff, bootpc, bootps, discard, dns, dnsix, echo, mobile-ip, nameserver, netbios-dgm, netbios-ns, ntp, rip, snmp, snmptrap, sunrpc, syslog, tacacs-ds, talk, tftp, time, who, and xdmcp.

If no layer protocol number is entered, you can use this syntax:

set qos acl ip {*acl_name*} {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] {*src_ip_spec*} [**before** *editbuffer_index* | **modify** *editbuffer_index*]

If a Layer 4 protocol is specified, you can use this syntax:

set qos acl ip {*acl_name*} {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] {*protocol*} {*src_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

If ICMP is used, you can use this syntax:

set qos acl ip {*acl_name*} {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **icmp** {*src_ip_spec*} {*dest_ip_spec*} [*icmp_type* [*icmp_code*] | *icmp_message*] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

If TCP is used, you can use this syntax:

set qos acl ip {*acl_name*} {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **tcp** {*src_ip_spec*} [{*operator*} {*port*} [*port*]] {*dest_ip_spec*} [{*operator*} {*port*} [*port*]] [**established**] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

If UDP is used, you can use this syntax:

set qos acl ip {*acl_name*} {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [[**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **udp** {*src_ip_spec*} [{*operator*} {*port*} [*port*]] {*dest_ip_spec*} [{*operator* {*port*} [*port*]] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Examples

This example shows how to define a TCP access list:

```
Console> (enable) set qos acl ip my_acl trust-dscp microflow my-micro tcp 1.2.3.4
255.0.0.0 eq port 21 172.20.20.1 255.255.255.0
my_acl editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

This example shows how to define an ICMP access list:

```
Console> (enable) set qos acl ip icmp_acl trust-dscp my-micro icmp 1.2.3.4 255.255.0.0
172.20.20.1 255.255.255.0 precedence 3
my_acl editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

Related Commands

clear qos acl
commit
rollback
show qos acl info

8.6 EFT Copy

set qos acl ipx

To define IPX access lists, use the **set qos acl ipx** command.

set qos acl ipx {*acl_name*} {**dscp** *dscp* | **trust-cos**} [**aggregate** *aggregate_name*] {*protocol*} {*src_net*} [*dest_net*.[*dest_node*] [[*dest_net_mask*.]*dest_node_mask*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
dscp *dscp*	Sets CoS and DSCP from configured DSCP values.
trust-cos	Specifies that the DSCP is derived from the packet CoS.
aggregate *aggregate_name*	(Optional) Specifies the name of the aggregate policing rule to be applied to packets matching the ACE.
protocol	Keyword or number of an IPX protocol; valid values are from 0 to 255 representing an IPX protocol number. See the "Usage Guidelines" section for a list of valid keywords and corresponding numbers.
src_net	Number of the network from which the packet is being sent. See the "Usage Guidelines" section for format guidelines.
dest_net.	(Optional) Mask to be applied to destination-node. See the "Usage Guidelines" section for format guidelines.
dest_node	(Optional) Node on destination-network of the packet being sent.
dest_net_mask.	(Optional) Mask to be applied to the destination network. See the "Usage Guidelines" section for format guidelines.
dest_node_mask	(Optional) Mask to be applied to destination-node. See the "Usage Guidelines" section for format guidelines.
before *editbuffer_index*	(Optional) Inserts the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Replaces an ACE with the new ACE.

Defaults

There are no default ACL mappings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **dscp** *dscp* and **trust-cos** keywords and variables are used to select a marking rule. Refer to the *Catalyst 6500 Series Switch Software Configuration Guide* for additional marking rule information.

The **dscp** *dscp* and **trust-cos** keywords and variables are not supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2).

8.6 EFT Copy

The optional **aggregate** *aggregate_name* keyword and variable are used to configure policing in the ACE. Refer to the *Catalyst 6500 Series Switch Software Configuration Guide* for additional policing rule information.

Use the **show security acl** command to display the list.

The *src_ip_spec*, optional **precedence** *precedence*, or **dscp-field** *dscp* keywords and variables, are used to configure filtering.

When you enter the ACL name, follow these naming conventions:

- Maximum of 31 characters long and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types
- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer

Valid *protocol* keywords include **ncp** (17), **rip** (1), **sap** (4), and **spx** (5). The IP network number is listed in parentheses.

The *src_net* and *dest_net* variables are eight-digit hexadecimal numbers that uniquely identify network cable segments. When you specify the *src_net* or *dest_net*, use the following guidelines:

- It can be a number in the range 0 to FFFFFFFF. A network number of -1 or **any** matches all networks.
- You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.

The *dest_node* is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (xxxx.xxxx.xxxx).

The *destination_mask* is of the form N.H.H.H or H.H.H where N is the destination network mask and H is the node mask. It can be specified only when the destination node is also specified for the destination address.

The *dest_net_mask* is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must be immediately followed by a period, which must in turn be immediately followed by destination-node-mask. You can enter this value only when *dest_node* is specified.

The *dest_node_mask* is a 48-bit value represented as a dotted triplet of 4-digit hexadecimal numbers (xxxx.xxxx.xxxx). Place ones in the bit positions you want to mask. You can enter this value only when *dest_node* is specified.

The *dest_net_mask* is an eight-digit hexadecimal number that uniquely identifies the network cable segment. It can be a number in the range 0 to FFFFFFFF. A network number of -1 or **any** matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA. Following are *dest_net_mask* examples:

- 123A
- 123A.1.2.3
- 123A.1.2.3 ffff.ffff.ffff
- 1.2.3.4 ffff.ffff.ffff.ffff

Note The PFC3 does not provide QoS support for IPX traffic.

Examples

This example shows how to create an IPX ACE:

```
Console> (enable) set qos acl ipx my_IPXacl trust-cos aggregate my-agg -1
my_IPXacl editbuffer modified. Use `commit' command to apply changes.
Console> (enable)
```

Related Commands

clear qos acl
commit
rollback
show qos acl info

set qos acl mac

To define MAC access lists, use the **set qos acl mac** command.

set qos acl mac {*acl_name*} {**dscp** *dscp* | **trust-cos**} [**aggregate** *aggregate_name*] {*src_mac_addr_spec*} {*dest_mac_addr_spec*} [*ethertype*] [**cos** *cos_value*] [**vlan** *vlan*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
dscp *dscp*	Sets CoS and DSCP from configured DSCP values.
trust-cos	Specifies that the DSCP is derived from the packet CoS.
aggregate *aggregate_name*	(Optional) Specifies the name of the aggregate policing rule to be applied to packets matching the ACE.
src_mac_addr_spec	Number of the source MAC address in the form *source_mac_address source_mac_address_mask*.
dest_mac_addr_spec	Number of the destination MAC address.
ethertype	(Optional) Name or number that matches the Ethertype for Ethernet-encapsulated packets. See the "Usage Guidelines" section for a list of valid names and numbers.
cos *cos_value*	(Optional) Specifies the CoS value; valid values are from 0 to 7.
vlan *vlan*	(Optional) Specifies a VLAN; valid values are from 1 to 4094.
before *editbuffer_index*	(Optional) Inserts the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Replaces an ACE with the new ACE.

Defaults

There are no default ACL mappings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **dscp** *dscp* and **trust-cos** keywords and variables are used to select a marking rule. Refer to the *Catalyst 6500 Series Switch Software Configuration Guide* for additional marking rule information.

The **dscp** *dscp* and **trust-cos** keywords and variables are not supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2).

The optional **aggregate** *aggregate_name* keyword and variable are used to configure policing in the ACE. Refer to the *Catalyst 6500 Series Switch Software Configuration Guide* for additional policing rule information.

When you enter the ACL name, follow these naming conventions:

- Maximum of 31 characters long and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types
- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer

The *src_mac_addr_spec* is a 48-bit source MAC address and mask and entered in the form of *source_mac_address source_mac_address_mask* (for example, 08-11-22-33-44-55 ff-ff-ff-ff-ff-ff). Place ones in the bit positions you want to mask. When you specify the *src_mac_addr_spec*, follow these guidelines:

- The *source_mask* is required; 0 indicates a “care” bit, and 1 indicates a “don’t-care” bit.
- Use a 32-bit quantity in 4-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0.

The *dest_mac_spec* is a 48-bit destination MAC address and mask and entered in the form of *dest_mac_address dest_mac_address_mask* (for example, 08-00-00-00-02-00/ff-ff-ff-00-00-00). Place ones in the bit positions you want to mask. The destination mask is mandatory. When you specify the *dest_mac_spec*, use the following guidelines:

- Use a 48-bit quantity in 6-part dotted-hexadecimal format for the source address and mask.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 ff-ff-ff-ff-ff-ff.
- Use **host** source as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0.

Valid names for Ethertypes (and corresponding numbers) are Ethertalk (0x809B), AARP (0x8053), dec-mop-dump (0x6001), dec-mop-remote-console (0x6002), dec-phase-iv (0x6003), dec-lat (0x6004), dec-diagnostic-protocol (0x6005), dec-lavc-sca (0x6007), dec-amber (0x6008), dec-mumps (0x6009), dec-lanbridge (0x8038), dec-dsm (0x8039), dec-netbios (0x8040), dec-msdos (0x8041), banyan-vines-echo (0x0baf), xerox-ns-idp (0x0600), and xerox-address-translation (0x0601).

The *ether-type* is a 16-bit hexadecimal number written with a leading 0x.

Use the **show security acl** command to display the list.

Note The PFC3 does not provide QoS support for IPX traffic.

Examples

This example shows how to create a MAC access list:

```
Console> (enable) set qos acl mac my_MACacl trust-cos aggregate my-agg any any

my_MACacl editbuffer modified. Use `commit' command to apply changes.
Console> (enable)
```

Related Commands

clear qos acl
commit
rollback
show qos acl info

set qos acl map

To attach an ACL to a specified port or VLAN, use the **set qos acl map** command.

set qos acl map *acl_name* {*mod/port* | *vlan*} [**input**]

set qos acl map *acl_name vlan* **output**

Syntax Description

acl_name	Name of the list to which the entry belongs.
mod/port	Number of the module and the port on the module.
vlan	Number of the VLAN; valid values are from 1 to 4094.
input	(Optional) Attaches the ACL to the ingress interface. See the "Usage Guidelines" section for more information.
output	Attaches the ACL to the egress interface.

Defaults

There are no default ACL mappings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Caution This command may fail if you try to map an ACL to a VLAN and the NVRAM is full.

Caution Use the **copy** command to save the ACL configuration to Flash memory.

If you try to configure an ACL feature that is not supported on the input or the output interface, the **set qos acl map** command fails with an error message.

Only PFC3 supports the **input** and **output** keywords. If you do not specify a direction keyword (**input** or **output**), the system automatically specifies **input**.

Examples

This example shows how to attach an ACL to a port:

```
Console> (enable) set qos acl map my_acl 2/1
ACL my_acl is attached to port 2/1.
Console> (enable)
```

This example shows how to attach an ACL to a VLAN:

```
Console> (enable) set qos acl map ftp_acl 4
ACL ftp_acl is attached to vlan 4.
Console> (enable)
```

This example shows what happens if you try to attach an ACL that has not been committed:

```
Console> (enable) set qos acl map new_acl 4
Commit ACL new_acl before mapping.
Console> (enable)
```

This example shows how to attach an ACL named "test" to the VLAN 1 ingress interface:

```
Console> (enable) set qos acl map test 1
ACL test is successfully mapped to vlan 1 on input side.
Console> (enable)
```

This example shows how to attach an ACL named "test2" to the VLAN 1 egress interface:

```
Console> (enable) set qos acl map test2 1 output
ACL test2 is successfully mapped to vlan 1 on output side.
Console> (enable)
```

Related Commands

clear qos acl
commit
rollback
show qos acl map

set qos autoqos

To apply automatic QoS settings to all ports on the switch, use the **set qos autoqos** command.

set qos autoqos

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When the switch has applied all global QoS settings successfully, the switch displays a prompt that shows the CLI for port-based AutoQoS commands that are currently supported.

Examples

This example shows how to apply all global QoS settings to all ports on the switch:

```
Console> (enable) set qos autoqos
........
All ingress and egress QoS scheduling parameters configured on all ports.
CoS to DSCP, DSCP to COS and IP Precedence to DSCP maps configured.
Global QoS configured, port specific autoqos recommended:
    set port qos <mod/ports..> autoqos trust [cos|dscp]
    set port qos <mod/ports..> autoqos voip [ciscoipphone|ciscosoftphone]
Console> (enable)
```

Related Commands

clear port qos autoqos
clear qos autoqos
set port qos autoqos
show port qos
show qos info

set qos bridged-microflow-policing

To enable or disable microflow policing of bridged packets on a per-VLAN basis, use the **set qos bridged-microflow-policing** command.

set qos bridged-microflow-policing {**enable** | **disable**} *vlanlist*

Syntax Description

enable	Activates microflow policing functionality.
disable	Deactivates microflow policing functionality.
vlanlist	List of VLANs; valid values are from 1 to 4094.

Defaults

The default is intraVLAN QoS is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Layer 3 switching engine-based systems do not create NetFlow entries for bridged packets. Without a NetFlow entry, these packets cannot be policed at the microflow level. You must enter the **set qos bridged-microflow-policing enable** command if you want the bridged packets to be microflow policed.

This command is supported on systems configured with a Layer 3 switching engine only.

Examples

This example shows how to enable microflow policing:

```
Console> (enable) set qos bridged-microflow-policing enable 1-1000
QoS microflow policing is enabled for bridged packets on vlans 1-1000.
Console> (enable)
```

This example shows how to disable microflow policing:

```
Console> (enable) set qos bridged-microflow-policing disable 10
QoS microflow policing is disabled for bridged packets on VLAN 10.
Console> (enable)
```

Related Commands

show qos bridged-microflow-policing

set qos cos-cos-map

To set the CoS-to-CoS mapping on a global basis, use the **set qos cos-cos-map** command.

set qos cos-cos-map *cos1 cos2 ... cos8*

Syntax Description

cos#	CoS value; valid values are from 0 to 7.

Defaults

The default CoS-to-CoS configuration is listed in Table 2-19.

Table 2-19 CoS-to-CoS Mapping

CoS	0	1	2	3	4	5	6	7
CoS	0	1	2	3	4	5	6	7

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If QoS is disabled, this message displays when you attempt to define a CoS-to-CoS mapping:

```
QoS is disabled, changes will take effect after QoS is enabled.
```

Examples

This example shows how to set the CoS-to-CoS mapping:

```
Console> (enable) set qos cos-cos-map 0 1 2 3 4 4 6 7
QoS cos-cos-map set successfully.
Console> (enable)
```

Related Commands

clear qos cos-cos-map
show qos maps

set qos cos-dscp-map

To set the CoS-to-DSCP mapping, use the **set qos cos-dscp-map** command.

set qos cos-dscp-map *dscp1 dscp2... dscp8*

Syntax Description

dscp#	Number of the differentiated services code point (DSCP); valid values are from 0 to 63.

Defaults

The default CoS-to-DSCP configuration is listed in Table 2-20.

Table 2-20 CoS-to-DSCP Mapping

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The CoS-to-DSCP map is used to map the CoS of packets arriving on trusted ports (or flows) to a DSCP where the trust type is **trust-cos**. This map is a table of eight CoS values (0 through 7) and their corresponding DSCP values. The switch has one map.

This command is supported on systems configured with a Layer 3 switching engine only.

Examples

This example shows how to set the CoS-to-DSCP mapping:

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
QoS cos-dscp-map set successfully.
Console> (enable)
```

Related Commands

clear qos cos-dscp-map
show qos maps

set qos drop-threshold

To program the transmit-queue and receive-queue drop thresholds on all ports in the system, use the **set qos drop-threshold** command.

set qos drop-threshold 2q2t tx queue *q# thr1 thr2*

set qos drop-threshold {**1q2t** | **1q4t** | **1p1q4t**} **rx queue** *q# thr1 thr2 thr3 thr4*

Syntax Description

2q2t tx	Specifies the transmit-queue drop threshold.
1q2t | **1q4t** | **1p1q4t rx**	Specifies the receive-queue drop threshold.
queue *q#*	Specifies the queue; valid values are **1** and **2**.
thr1, thr2, thr3, thr4	Threshold percentage; valid values are from 1 to 100.

Defaults

If you enable QoS, the following defaults apply:

- Transmit-queue drop thresholds:
  - Queue 1—80%, 100%
  - Queue 2—80%, 100%
- Receive-queue drop thresholds:
  - Queue 1—50%, 60%, 80%, 100% if the port is trusted
  - Queue 2—100%, 100%, 100%, 100% if the port is untrusted

If you disable QoS, the following defaults apply:

- Transmit-queue drop thresholds:
  - Queue 1—100%, 100%
  - Queue 2—100%, 100%
- Receive-queue drop thresholds: queue 1—100%, 100%, 100%, 100%

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The number preceding the **t** letter in the port type (**2q2t**, **1q2t**, **1q4t**, or **1p1q4t**) determines the number of threshold values the hardware supports. For example, with **2q2t** and **1q2t**, the number of thresholds specified is two; with **1q4t** and **1p1q4t**, the number of thresholds specified is four. Due to the granularity of programming the hardware, the values set in hardware will be close approximations of the values provided.

The number preceding the **q** letter in the port type determines the number of the queues that the hardware supports. For example, with **2q2t**, the number of queues specified is two; with **1q2t**, **1q4t** and **1p1q4t**, the number of queues specified is one. The system defaults for the transmit queues attempt to keep the maximum latency through a port at a maximum of 10 milliseconds.

The number preceding the **p** letter in the **1p1q4t** port types determines the threshold in the priority queue.

When you configure the drop threshold for **1p1q4t**, the drop threshold for the second queue is 100 percent and is not configurable.

The thresholds are all specified as percentages; 10 indicates a threshold when the buffer is 10 percent full.

The single-port ATM OC-12 module does not support transmit-queue drop thresholds.

Examples

This example shows how to assign the transmit-queue drop threshold:

```
Console> (enable) set qos drop-threshold 2q2t tx queue 1 40 80
Transmit drop thresholds for queue 1 set at 40% and 80%
Console> (enable)
```

These examples show how to assign the receive-queue drop threshold:

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 40 50 60 100
Receive drop thresholds for queue 1 set at 40% 50% 60% 100%
Console> (enable)

Console> (enable) set qos drop-threshold 1p1q4t rx queue 1 40 50 60 100
Receive drop thresholds for queue 1 set at 40% 50% 60% 100%
Console> (enable)
```

Related Commands

show qos info

set qos dscp-cos-map

To set the DSCP-to-CoS mapping, use the **set qos dscp-cos-map** command.

set qos dscp-cos-map *dscp_list:cos_value* ...

Syntax Description

dscp_list	Number of the DSCP; valid values are from 0 to 63.
cos_value...	Number of the CoS; valid values are from 0 to 7.

Defaults

The default DSCP-to-CoS configuration is listed in Table 2-21.

Table 2-21 DSCP-to-CoS Mapping

DSCP	0 to 7	8 to 15	16 to 23	24 to 31	32 to 39	40 to 47	48 to 55	56 to 63
CoS	0	1	2	3	4	5	6	7

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The DSCP-to-CoS map is used to map the final DSCP classification to a final CoS. This final map determines the output queue and threshold to which the packet is assigned. The CoS map is written into the ISL header or 802.1Q tag of the transmitted packet on trunk ports and contains a table of 64 DSCP values and their corresponding CoS values. The switch has one map.

This command is supported on systems configured with a Layer 3 switching engine only.

Examples

This example shows how to set the DSCP-to-CoS mapping:

```
Console> (enable) set qos dscp-cos-map 20-25:7 33-38:3
QoS dscp-cos-map set successfully.
Console> (enable)
```

Related Commands

clear qos map
show qos maps

set qos dscp-mutation-map

To configure a DSCP mutation map, use the **set qos dscp-mutation-map** command.

set qos dscp-mutation-map *mutation_table_id old_dscp_list:new_dscp...*

Syntax Description

mutation_table_id	Number of the mutation table; valid values are from 1 to 15.
old_dscp_list:new dscp...	Number of the DSCP mapping and number of the mutated DSCP mapping; valid values are from 0 to 63. See the "Usage Guidelines" section for more information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The PFC3 supports 16 DSCP mutation maps. QoS uses one mutation map for the default mapping. You can configure 15 mutation maps.

You can specify of range of old DSCP mappings. Enter the range as integers separated by a hyphen and a comma (for example, 1-3,7 specifies mappings 1, 2, 3 and 7).

Examples

This example shows how to configure a DSCP mutation map:

```
Console> (enable) set qos dscp-mutation-map 1 30:2
QoS dscp-mutation-map with mutation-table-id 1 has been set correctly.
Console> (enable)
```

Related Commands

clear qos dscp-mutation-map
clear qos dscp-mutation-table-map
set qos dscp-mutation-table-map
show qos maps

set qos dscp-mutation-table-map

To configure the DSCP mutation table map, use the **set qos dscp-mutation-table-map** command.

set qos dscp-mutation-table-map *mutation_table_id vlan_list*

Syntax Description

mutation_table_id	Number of the mutation table; valid values are from 1 to 15.
vlan_list	VLAN numbers that form a VLAN list; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The PFC3 supports 16 DSCP mutation maps. QoS uses one mutation map for the default mapping. You can configure 15 mutation maps.

Examples

This example shows how to set DSCP mutation table map 1 for VLANs 1 through 10:

```
Console> (enable) set qos dscp-mutation-table-map 1 1-10
VLANs 1-10 mapped to mutation-table-id 1.
Console> (enable)
```

Related Commands

clear qos dscp-mutation-map
clear qos dscp-mutation-table-map
set qos dscp-mutation-map
show qos maps

set qos dscp-rewrite

To globally enable or disable rewriting the differentiated services code point (DSCP) values of packets as they go through the switch, use the **set qos dscp-rewrite** command.

set qos dscp-rewrite {**enable** | **disable**}

Syntax Description

enable	Rewrites the DSCP values of packets.
disable	Maintains the DSCP values of packets so that the values are the same as when the packets came to the switch.

Defaults

The DSCP rewrite feature is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to globally disable the DSCP rewrite feature:

```
Console> (enable) set qos dscp-rewrite disable
DSCP rewrite has been globally disabled.
Console> (enable)
```

This example shows how to globally enable the DSCP rewrite feature:

```
Console> (enable) set qos dscp-rewrite enable
DSCP rewrite has been globally enabled.
Console> (enable)
```

Related Commands

show qos status

set qos ipprec-dscp-map

To set the IP precedence-to-DSCP map, use the **set qos ipprec-dscp-map** command. This command applies to all packets and all ports.

set qos ipprec-dscp-map *dscp1* ... *dscp8*

Syntax Description

dscp1#	Number of the IP precedence value; up to eight values can be specified.

Defaults

The default IP precedence-to-DSCP configuration is listed in Table 2-22.

Table 2-22 IP Precedence-to-DSCP Mapping

IPPREC	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use this command to map the IP precedence of IP packets arriving on trusted ports (or flows) to a DSCP when the trust type is **trust-ipprec**. This map is a table of eight precedence values (0 through 7) and their corresponding DSCP values. The switch has one map. The IP precedence values are as follows:

- network 7
- internet 6
- critical 5
- flash-override 4
- flash 3
- immediate 2
- priority 1
- routine 0

This command is supported on systems configured with a Layer 3 switching engine only.

Examples

This example shows how to assign IP precedence-to-DSCP mapping and return to the default:

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
QoS ipprec-dscp-map set successfully.
Console> (enable)
```

Related Commands

clear qos ipprec-dscp-map
show qos maps

set qos mac-cos

To set the CoS value to the MAC address and VLAN pair, use the **set qos mac-cos** command.

set qos mac-cos *dest_mac vlan cos*

Syntax Description

dest_mac	MAC address of the destination host.
vlan	Number of the VLAN; valid values are from 1 to 4094.
cos	CoS value; valid values are from 0 to 7, higher numbers represent higher priority.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command has no effect on a switch configured with a PFC since the Layer 3 switching engine's result always overrides the Layer 2 result. Instead, use the **set qos acl** command.

The **set qos mac-cos** command creates a permanent CAM entry in the CAM table until you reset the active supervisor engine.

The port associated with the MAC address is learned when the first packet with this source MAC address is received. These entries do not age out.

The CoS for a packet going to the specified MAC address is overwritten even if it is coming from a trusted port.

If you enter the **show cam** command, entries made with the **set qos mac-cos** command display as dynamic because QoS considers them to be dynamic, but they do not age out.

Examples

This example shows how to assign the CoS value 3 to VLAN 2:

```
Console> (enable) set qos mac-cos 0f-ab-12-12-00-13 2 3
CoS 3 is assigned to 0f-ab-12-12-00-13 vlan 2.
Console> (enable)
```

Related Commands

clear qos mac-cos
show qos mac-cos

set qos map

To map a specific CoS value to the transmit- or receive-priority queues and the thresholds per available priority queue for all ports, use the **set qos map** command.

set qos map *port_type* **tx** | **rx** *q#* *thr#* **cos** *coslist*

set qos map *port_type* **tx** | **rx** *q#* **cos** *coslist*

Syntax Description

port_type	Port type; valid values are **2q2t**, **1p2q2t**, **1p3q1t**, and **1p2q1t** for transmit. Valid values are **1q2t**, **1p1q4t**, **1p1q0t**, and **1p1q8t**, **2q8t** for receive. See the "Usage Guidelines" section for additional information.
tx	Specifies the transmit queue.
rx	Specifies the receive queue.
q#	Value determined by the number of priority queues provided at the transmit or receive end; valid values are **1** and **2**, with the higher value indicating a higher priority queue.
thr#	Value determined by the number of drop thresholds available at a port; valid values are **1** and **2**, with the higher value indicating lower chances of being dropped.
cos *coslist*	Specifies CoS values; valid values are from **0** through **7**, with the higher numbers representing a higher priority.

Defaults

The default mappings for all ports are shown in Table 2-23 and Table 2-24.

Table 2-23 CoS-to-Queue-to-Threshold Mapping (TX)

Queue	Threshold	Cos Values[1]
QoS enabled		
1	1	0, 1
2	1	2, 3, 4
3	1	6, 7
4	0	5
QoS disabled		
1	0	0, 1, 2, 3, 4, 5, 6, 7

[1] All CoS values, except CoS 5, are mapped to WRED. CoS 5, which is mapped to queue 4, does not have an associated WRED threshold.

Table 2-24 CoS-to-Queue Mapping (RX)

Queue	COS Values
QoS enabled	
1	0, 1, 2, 3, 4, 6, 7
2	5
QoS disabled	
1	0, 1, 2, 3, 4, 5, 6, 7

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter the **set qos map** *port_type* **tx** | **rx** *q#* **cos** *coslist* command, the following is a list of possible port types available:

- **tx** *port_type* = **1p3q1t** and **1p2q1t**
- **rx** *port_type* = **1p1q0t** and **2q8t**

You can enter the *cos_list* variable as a single CoS value, multiple noncontiguous CoS values, a range of CoS values, or a mix of values. For example, you can enter any of the following: **0**, or **0,2,3**, or **0-3,7**.

The priority queue number is 4 for transmit and queue number 2 for receive.

When specifying the priority queue for the **1p2q2t** port type, the priority queue number is 3 and the threshold number is 1.

The receive- and transmit-drop thresholds have this relationship:

- Receive-queue 1 (standard) threshold 1 = transmit-queue 1 (standard low priority) threshold 1
- Receive-queue 1 (standard) threshold 2 = transmit-queue 1 (standard low priority) threshold 2
- Receive-queue 1 (standard) threshold 3 = transmit-queue 2 (standard high priority) threshold 1
- Receive-queue 1 (standard) threshold 4 = transmit-queue 2 (standard high priority) threshold 2

Refer to the *Catalyst 6500 Series Switch Software Configuration Guide* for additional usage guidelines.

Examples

This example shows how to assign the CoS values 1, 2, and 5 to the first queue and the first drop threshold in that queue:

```
Console> (enable) set qos map 2q2t tx 1 1 cos 1,2,5
Qos tx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

This example shows how to assign the CoS values to queue 1 and threshold 2 in that queue:

```
Console> (enable) set qos map 2q2t tx 1 2 cos 3-4,7
Qos tx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

This example shows how to map the CoS value 5 to strict-priority transmit-queue 3/drop-threshold 1:

```
Console> (enable) set qos map 1p2q2t tx 3 1 cos 5

Qos tx strict queue and threshold mapped to cos successfully.
Console> (enable)
```

Related Commands

clear qos map
show qos info

set qos policed-dscp-map

To set the mapping of policed in-profile DSCPs, use the **set qos policed-dscp-map** command.

set qos policed-dscp-map [**normal-rate** | **excess-rate**] *in_profile_dscp***:***policed_dscp...*

Syntax Description

normal-rate	(Optional) Specifies normal rate policers.
excess-rate	(Optional) Specifies excess rate policers.
in_profile_dscp	Number of the in-profile DSCP; valid values are from 0 through 63.
:*policed_dscp*	Number of the policed DSCP; valid values are 0 through 63.

Defaults

The default map is no markdown.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can enter *in_profile_dscp* as a single DSCP, multiple DSCPs, or a range of DSCPs (for example, 1 or 1,2,3 or 1-3,7).

The colon between *in_profile_dscp* and *policed_dscp* is required.

This command is supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

If you do not specify a rate, the system automatically specifies the normal rate.

Examples

This example shows how to set the mapping of policed in-profile DSCPs:

```
Console> (enable) set qos policed-dscp-map 33:30
QoS normal-rate policed-dscp-map set successfully.
Console> (enable)
```

This example shows how to set the mapping of policed in-profile DSCPs for the excess rate:

```
Console> (enable) set qos policed-dscp-map excess-rate 33:30
QoS excess-rate policed-dscp-map set successfully.
Console> (enable)
```

Related Commands

clear qos policed-dscp-map
show qos maps
show qos policer

set qos policer

To create a policing rule for ACL, use the **set qos policer** command.

set qos policer {**microflow** *microflow_name*} {**rate** *rate*} {**burst** *burst*} {**drop** | **policed-dscp**}

set qos policer {**aggregate** *aggregate_name*} {**rate** *rate*} {**burst** *burst*} {**drop** | **policed-dscp**}

set qos policer {**aggregate** *aggregate_name*} {**rate** *rate*} **policed-dscp** {**erate** *erate*} {**drop** | **policed-dscp**} **burst** *burst* [**eburst** *eburst*]

Syntax Description

microflow *microflow_name*	Specifies the name of the microflow policing rule.
rate *rate*	Specifies the average rate; valid values are **0** and from 32 kilobits per second to 32 gigabits per second.
burst *burst*	Specifies the burst size; valid values are 1 to 256000 kilobits.
drop	Specifies drop traffic.
policed-dscp	Specifies policed DSCP.
aggregate *aggregate_name*	Specifies the name of the aggregate policing rule.
erate *erate*	Specifies the excess rate value; valid values are **0** and from 32 kilobits per second to 8 gigabits per second.
eburst *eburst*	(Optional) Specifies the excess burst size; valid values are 1 to 256000 kilobits.

Defaults

The default is no policing rules or aggregates are configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Before microflow policing can occur, you must define a microflow policing rule. Policing allows the switch to limit the bandwidth consumed by a flow of traffic.

The Catalyst 6500 series switch supports up to 63 microflow policing rules. When a microflow policer is used in any ACL that is attached to any port or VLAN, the NetFlow flow mask is increased to full flow.

Before aggregate policing can occur, you must create an aggregate and a policing rule for that aggregate. The Catalyst 6500 series switch supports up to 1023 aggregates and 1023 policing rules.

When both normal and excess rates are zero, you can specify any burst size. If the normal rates and excess rates are zero, the value is ignored and set internally by hardware.

The excess rate must be greater than or equal to the normal rate.

The **set qos policer aggregate** command allows you to configure an aggregate flow and a policing rule for that aggregate. When you enter the **microflow** *microflow_name* **rate** *rate* **burst** *burst*, the range for the average rate is 32 kilobits per second to 8 gigabits per second, and the range for the burst size is 1 kilobit (entered as 1) to 32 megabits (entered as 32000). The burst can be set lower, higher, or equal to the rate. Modifying an existing aggregate rate limit entry causes that entry to be modified in NVRAM and in the switch if that entry is currently being used.

Note We recommend a 32-kilobit minimum value burst size. Due to the nature of the traffic at different customer sites, along with the hardware configuration, smaller values occasionally result in lower rates than the specified rate. If you experiment with smaller values but problems occur, increase the burst rate to this minimum recommended value.

When you modify an existing microflow or aggregate rate limit, that entry in NVRAM is modified, as well as in the switch if it is currently being used.

When you enter the policing name, follow these naming conventions:

- Maximum of 31 characters long and may include a through z, A through Z, 0 through 9, the dash character (-), the underscore character (_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types
- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer

The **burst** keyword and the *burst* value and the optional **eburst** keyword and the *eburst* value set the token bucket sizes. To sustain a specific rate, set the token bucket size to be at least the rate divided by 4000, because tokens are removed from the bucket every 1/4000th of a second (0.25 milliseconds) and the bucket needs to be at least as large as the burst size to sustain the specified rate.

If you do not enter the **eburst** keyword and the *eburst* value, QoS sets both token buckets to the size configured with the **burst** keyword and the *burst* value.

Examples

This example shows how to create a microflow policing rule for ACL:

```
Console> (enable) set qos policer microflow my-micro rate 1000 burst 10000 policed-dscp
QoS policer for microflow my-micro set successfully.
Console> (enable)
```

These examples show how to create an aggregate policing rule for ACL:

```
Console> (enable) set qos policer aggregate my-agg rate 1000 burst 2000 drop
QoS policer for aggregate my-aggset successfully.
Console> (enable)

Console> (enable) set qos policer aggregate test3 rate 64 policed-dscp erate 128 drop burst 96
QoS policer for aggregate test3 created successfully.
Console> (enable)
```

Related Commands

clear qos policer
show qos policer

set qos policy-source

To set the QoS policy source, use the **set qos policy-source** command.

set qos policy-source local | cops

Syntax Description

local	Sets the policy source to local NVRAM configuration.
cops	Sets the policy source to COPS-PR configuration.

Defaults

The default is all ports are set to local.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you set the policy source to **local**, the QoS policy is taken from local configuration stored in NVRAM. If you set the policy source to **local** after it was set to **cops**, the QoS policy reverts back to the local configuration stored in NVRAM.

When you set the policy source to **cops**, all global configurations to the device, such as the DSCP-to-marked-down DSCP, is taken from policy downloaded to the policy enforcement point (PEP) by the policy decision point (PDP). Configuration of each physical port, however, is taken from COPS-PR only if the policy source for that port has been set to **cops**.

Examples

This example shows how to set the policy source to COPS-PR:

```
Console> (enable) set qos policy-source cops
QoS policy source for the switch set to COPS.
Console> (enable)
```

This example shows how to set the policy source to local NVRAM:

```
Console> (enable) set qos policy-source local
QoS policy source for the switch set to local.
Console> (enable)
```

This example shows the output if you attempt to set the policy source to COPS-PR and no COPS-PR servers are available:

```
Console> (enable) set qos policy-source cops
QoS policy source for the switch set to COPS.
Warning: No COPS servers configured. Use the 'set cops server' command
to configure COPS servers.
Console> (enable)
```

Related Commands

clear qos config
show qos policy-source

8.6 EFT Copy

set qos rsvp

To turn on or turn off the RSVP feature on the switch, to set the time in minutes after which the RSVP databases get flushed (when the policy server dies), and to set the local policy, use the **set qos rsvp** command.

set qos rsvp enable | disable

set qos rsvp policy-timeout *timeout*

set qos rsvp local-policy forward | reject

Syntax Description

enable	Activates the RSVP feature.
disable	Deactivates the RSVP feature.
policy-timeout *timeout*	Specifies the time in minutes after which the RSVP databases get flushed; valid values are from 1 to 65535 minutes.
local-policy forward | reject	Specifies the policy configuration local to the network device to either accept existing flows and forward them or not accept new flows.

Defaults

The default is the RSVP feature is disabled, policy-timeout is 30 minutes, and local policy is forward.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The local policy guidelines are as follows:

- There is no connection with the policy server.
- New flows that come up after connection with the policy server have been lost.
- Old flows that come up after the PDP policy times out.

Examples

This example shows how to enable RSVP:

```
Console> (enable) set qos rsvp enable
RSVP enabled. Only RSVP qualitative service supported.
QoS must be enabled for RSVP.
Console> (enable)
```

This example shows how to disable RSVP:

```
Console> (enable) set qos rsvp disable
RSVP disabled on the switch.
Console> (enable)
```

This example shows how to set the policy timeout interval:

```
Console> (enable) set qos rsvp policy-timeout 45
RSVP database policy timeout set to 45 minutes.
Console> (enable)
```

This example shows how to set the policy timeout interval:

```
Console> (enable) set qos rsvp local-policy forward
RSVP local policy set to forward.
Console> (enable)
```

Related Commands

show qos rsvp

set qos rxq-ratio

To set the amount of packet buffer memory allocated to high-priority incoming traffic and low-priority incoming traffic, use the **set qos rxq-ratio** command.

set qos rxq-ratio *port_type queue1_val queue2_val... queueN_val*

Syntax Description

port_type	Port type; valid value is **1p1q0t** and **1p1q8t**.
queue1_val	Percentage of low-priority traffic; valid values are from 1 to 99 and must total 100 with the *queue2_val* value.
queue2_val	Percentage of high-priority traffic; valid values are from 1 to 99 and must total 100 with the *queue1_val* value.
queueN_val	Percentage of strict-priority traffic; valid values are from 1 to 99 and must total 100 with the *queue1_val* and *queue1_val* values.

Defaults

The default is 80:20 (queue 1 and queue 2) if you enable QoS and 100:0 (queue 1 and queue 2) if you disable QoS.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Caution Use caution when using this command. When entering the **set qos rxq-ratio** command, all ports go through a link up and link down condition.

The values set in hardware are close approximations of the values provided. For example, if you specify 0 percent, the actual value programmed is not necessarily 0.

The **rxq** ratio is determined by the traffic mix in the network. High-priority traffic is typically a smaller fraction of the traffic. Because the high-priority queue gets more service, you should set the high-priority queue lower than the low-priority queue.

The strict-priority queue requires no configuration.

For the strict-priority queue on 1p1q8t ingress ports, the minimum valid value is 3 percent.

Examples

This example shows how to set the receive-queue size ratio:

```
Console> (enable) set qos rxq-ratio 1p1q0t 80 20
QoS rxq-ratio is set successfully.
Console> (enable)
```

Related Commands

show qos info

set qos statistics export

To globally enable or disable statistics data gathering from hardware, use the **set qos statistics export** command.

set qos statistics export {**enable** | **disable**}

Syntax Description

enable	Enables statistics data gathering.
disable	Disables statistics data gathering.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Statistics polling does not occur if statistics are disabled, regardless of any other settings.

You must designate an export destination prior to entering this command. If an export destination is not set, this message is displayed:

```
Warning: Export destination not set. Use the ‘set qos statistics export destination’
command to configure the export destination.
```

Examples

This example shows how to enable statistics polling:

```
Console> (enable) set qos statistics export enable
QoS statistics export enabled.
Export destination: Stargate, port 9996
Console> (enable)
```

Related Commands

show qos statistics export info

set qos statistics export aggregate

To enable or disable statistics data export on an aggregate policer, use the **set qos statistics export aggregate** command.

set qos statistics export aggregate *name* {**enable** | **disable**}

Syntax Description

name	(Optional) Name of the policer.
enable	Enables statistics data export for the named aggregate policer.
disable	Disables statistics data export for the named aggregate policer.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To export data, you need to enable statistics on the port. You also must globally enable statistics and data export. (See the set qos statistics export command.)

This command is supported on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to enable statistics export:

```
Console> (enable) set qos statistics export aggregate ipagg_3 enable
Statistics data export enabled for aggregate policer ipagg_3.
Export destination: 172.20.15.1 (Stargate), port 9996
Console> (enable)
```

Related Commands

set qos statistics export
show mac
show qos statistics export info

8.6 EFT Copy

set qos statistics export destination

To specify the statistics data export destination address, use the **set qos statistics export destination** command.

set qos statistics export destination {*host_name* | *host_ip*} [*port*]

set qos statistics export destination {*host_name* | *host_ip*} [**syslog** [{*facility severity*}]]

Syntax Description

host_name	Host name.
host_ip	Host IP address.
port	(Optional) UDP port number.
syslog	(Optional) Specifies the syslog port.
facility	(Optional) Value to specify the type of facility to export; see the "Usage Guidelines" section for a list of valid values.
severity	(Optional) Value to specify the severity level to export; see the "Usage Guidelines" section for a list of valid values.

Defaults

The default is none unless **syslog** is specified. If **syslog** is specified, the defaults are as follows:

- *port* is 514
- *facility* is local6
- *severity* is debug

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Valid *facility* values are **kern**, **user**, **mail**, **daemon**, **auth**, **lpr**, **news**, **uucp**, **cron**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, and **local7**.

Valid *severity* levels are **emerg**, **alert**, **crit**, **err**, **warning**, **notice**, **info**, and **debug**.

Examples

This example shows how to specify the statistics data export destination address:

```
Console> (enable) set qos statistics export destination stargate 9996
Statistics data export destination set to stargate port 9996.
Console> (enable)
```

Related Commands

set qos statistics export
show qos statistics export info

set qos statistics export interval

To specify how often a port or aggregate policer statistics data is read and exported, use the **set qos statistics export interval** command.

set qos statistics export interval *interval*

Syntax Description

interval	Export time interval; valid values are from 30 seconds to 65535 seconds.

Defaults

The default is 30 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the export interval:

```
Console> (enable) set qos statistics export interval 35
Statistics export interval set to 35 seconds.
Console> (enable)
```

Related Commands

show qos statistics export info

set qos statistics export port

To enable or disable statistics data export on a port, use the **set qos statistics export port** command.

set qos statistics export port *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	(Optional) Number of the module and the port on the module.
enable	Enables statistics data export.
disable	Disables statistics data export.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

For data export to be performed, you should enable statistics on the aggregate policer as well. You must globally enable statistics and data export (see the **set qos statistics export** command).

Examples

This example shows how to enable statistics export on a port:

```
Console> (enable) set qos statistics export port 2/5 enable
Statistics data export enabled on port 2/5.
Console> (enable)
```

Related Commands

show qos statistics export info

8.6 EFT Copy

set qos txq-ratio

To set the amount of packet buffer memory allocated to high-priority traffic and low-priority traffic, use the **set qos txq-ratio** command.

set qos txq-ratio *port_type queue1_val queue2_val... queueN_val*

Syntax Description

port_type	Port type; valid values are **2q2t**, **1p2q2t**, and **1p2q1t**.
queue1_val	Percentage of low-priority traffic; valid values are from 1 to 99 and must total 100 with the *queue2_val* value.
queue2_val	Percentage of high-priority traffic; valid values are from 1 to 99 and must total 100 with the *queue1_val* value.
queueN_val	Percentage of strict-priority traffic; valid values are from 1 to 99 and must total 100.

Defaults

The default for **2q2t** is 80:20 if you enable QoS and 100:0 if you disable QoS. The default for **1p2q2t** is 70:15:15 if you enable QoS and 100:0:0 if you disable QoS.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Caution Use caution when using this command. When entering the **set qos txq-ratio** command, all ports go through a link up and down condition.

The values set in hardware will be close approximations of the values provided. For example, even if you specify 0 percent, the actual value programmed will not necessarily be 0.

The **txq** ratio is determined by the traffic mix in the network. Because high-priority traffic is typically a smaller fraction of the traffic and because the high-priority queue gets more service, you should set the high-priority queue lower than the low-priority queue.

The strict-priority queue requires no configuration. For the strict-priority queue on 1p2q1t egress ports, the minimum valid value is 5 percent.

Examples

This example shows how to set the transmit-queue size ratio:

```
Console> (enable) set qos txq-ratio 2q2t 75 25
QoS txq-ratio is set successfully.
Console> (enable)
```

Related Commands

show qos info

set qos wred

To configure the WRED threshold parameters for the specified port type, use the **set qos wred** command.

set qos wred *port_type* [**tx**] **queue** *q#* {[*thr1Lo*:]*thr1Hi*} {[*thr2Lo*:]*thr2Hi*}...

Syntax Description

port_type	Port type; valid values are **1p2q2t**, **1p2q1t**, **1p3q1t**, and **1p1q8t**.
tx	(Optional) Specifies the parameters for output queuing.
queue *q#*	Keyword and variable to specify the queue to which the arguments apply; valid values are 1 through 3.
thr1Lo	(Optional) Percentage of the lower threshold size for the first WRED curve; valid values are from 1 to 100.
thr1Hi	Percentage of the upper threshold size for the first WRED curve; valid values are from 1 to 100.
thr2Lo	(Optional) Percentage of the lower threshold size for the second WRED curve; valid values are from 1 to 100.
thr2Hi	Percentage of the upper threshold size for the second WRED curve; valid values are from 1 to 100.

Defaults

The default thresholds are as follows:

- For **1p2q2t** = 40:70 (threshold1) and 70:100 (threshold2) (low:high percentage)/queue
- For **1p3q1t** = 70:100 (low:high)

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The queue values range from 1 to 3. Queue 4 is the strict-priority queue and does not have an associated WRED threshold. The thresholds are all specified as percentages ranging from 1 to 100. A value of 10 indicates a threshold when the buffer is 10 percent full.

The colon between the low and high threshold values is required.

Examples

This example shows how to configure lower and upper threshold values for queue 1:

```
Console> (enable) set qos wred 1p2q2t queue 1 20:60 40:90
WRED thresholds for queue 1 set to 20:60 and 40:90 on all WRED-capable 1p2q2t ports.
Console> (enable)
```

This example shows how to configure the upper threshold value for queue 1:

```
Console> (enable) set qos wred 1p3q1t tx queue 1 20
WRED thresholds for queue 1 set to 0:20 on all WRED-capable 1p3q1t ports.
Console> (enable)
```

Related Commands

clear qos config
show qos info

set qos wrr

To specify the weights that determine how many packets will transmit out of one queue before switching to the other queue, use the **set qos wrr** command.

set qos wrr *port_type queue1_val queue2_val*... [**srr**]

Syntax Description

port_type	Port type; valid values are **2q2t**, **1p2q2t**, **1p3q1t**, **1p2q1t**, **1p3q8t**,**1p7q8t**, **2q2t**
queue#_val	Number of weights for queues 1, 2, or 3; valid values are from 1 to 255.
srr	(Optional) Specifies Shaped Round Robin (SRR).

Defaults

The default WRR with QoS enabled for port type **1p3q1t** is as follows:

- Queue 1 = 100
- Queue 2 = 150
- Queue 3 = 200

With QoS disabled, the default is 255 for all three queues.

The default WRR for port types **2q2t** and **1p2q2t** is 4:255.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The WRR weights are used to partition the bandwidth between the queues in the event all queues are not empty. For example, weights of 1:3 mean that one queue gets 25 percent of the bandwidth and the other gets 75 percent as long as both queues have data.

Weights of 1:3 do not necessarily lead to the same results as when the weights are 10:30. In the latter case, more data is serviced from each queue and the latency of packets serviced from the other queue goes up. For best results, set the weights so that at least one packet (maximum size) can be serviced from the lower priority queue at a time. For the higher priority queue, set the weights so that multiple packets are serviced at any one time.

The values set in hardware will be close approximations of the values provided. For example, even if you specify 0 percent, the actual value programmed will not necessarily be 0. Whatever weights you choose, make sure that the resulting byte values programmed (see the **show qos info** command with the **runtime** keyword) are at least equal to the MTU size.

The ratio achieved is only an approximation of what you specify since the cutoff is on a packet and midway through a packet. For example, if you specify that the ratio services 1000 bytes out of the low-priority queue, and there is a 1500-byte packet in the low-priority queue, the entire 1500-byte packet is transmitted because the hardware services an entire packet.

For **1p2q2t** and **2q2t**, only two queues can be set; the third queue is strict priority.

For **1p3q1t**, three queues can be set; a fourth queue is strict priority.

SRR is only supported on switches with a PFC3. SRR is only supported with **1p3q8t**.

Examples

This example shows how to specify the weights for queue 1 and queue 2 to 30 and 70:

```
Console> (enable) set qos wrr 2q2t 30 70
QoS wrr ratio is set successfully.
Console> (enable)
```

This example shows how to specify the SRR link scheduling algorithm:

```
Console> (enable) set qos wrr 1p3q8t 80 100 20 srr
QoS wrr and srr ratio is set successfully.
WRR/SRR absolute values are affected by hardware granularity.
Config> (enable)
```

Related Commands

show qos info
show qos statistics

set radius attribute

To set attributes to the RADIUS ACCESS_REQUEST packet, use the **set radius attribute** command.

set radius attribute {*number* | *name*} **include-in-access-req** {**enable** | **disable**}

Syntax Description

number	Attribute number; valid value is 8.
name	Attribute name; valid value is framed-ip-address.
include-in-access-req	Sets attributes to the ACCESS_REQUEST packet.
enable | **disable**	Enables or disables the attribute.

Defaults

All RADIUS attributes are disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set radius attribute** command allows you to specify the transmission of optional attributes such as Framed-IP address, NAS-Port, Called-Station-Id, and Calling-Station-Id. You can set attribute transmission by either the attribute number or the attribute name.

Examples

This example shows how to specify and enable the Framed-IP address attribute by number:

```
Console> (enable) set radius attribute 8 include-in-access-req enable
Transmission of Framed-ip address in access-request packet is enabled.
Console> (enable)
```

This example shows how to specify and disable the Framed-IP address attribute by name:

```
Console> (enable) set radius attribute framed-ip-address include-in-access-req disable
Transmission of Framed-ip address in access-request packet is disabled.
Console> (enable)
```

Related Commands

show radius

set radius auto-initialize

To enable or disable the automatic initialization of all ports in AAA fail state when a RADIUS server becomes active, use the **set radius auto-initialize** command.

set radius auto-initialize {**enable** | **disable**}

Syntax Description

enable	Enables automatic initialization.
disable	Disables automatic initialization.

Defaults

Automatic initialization is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

With automatic initializatioin enabled, when AAA modules detect that at least one RADIUS server is active, all modules are notified of the AAA up event. When notified, the EoU policy reviews the list of all ports in AAA fail state and begins to revalidate them without changing the existing fail policy. If rate limiting is enabled, sessions are rate limited. If rate limiting is disabled, all ports attempt to authenticate when a RADIUS server becomes active. When authentications are successful, the new authenticated policy replaces the existing fail policy.

Examples

This example shows how to enable automatic initialization of all ports in AAA fail state when a RADIUS server become active:

```
Console> (enable) set radius auto-initialize enable
Radius Auto-initialize enabled.
Console> (enable)
```

Related Commands

set radius deadtime

To set the time to skip RADIUS servers that do not reply to an authentication request, use the **set radius deadtime** command.

set radius deadtime *minutes*

Syntax Description

minutes	Length of time a RADIUS server does not respond to an authentication request; valid values are from 0 to 1440 minutes.

Defaults

The default is 0 minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If only one RADIUS server is configured or if all the configured servers are marked dead, deadtime will be ignored since no alternate servers are available. By default, the deadtime is 0 minutes; the RADIUS servers are not marked dead if they do not respond.

Examples

This example shows how to set the RADIUS deadtime to 10 minutes:

```
Console> (enable) set radius deadtime 10
Radius deadtime set to 10 minutes.
Console> (enable)
```

Related Commands

show radius

set radius keepalive

To enable or disable the RADIUS keepalive timer and to configure the keepalive timer to check that status of configured RADIUS servers, use the set radius keepalive command.

set radius keepalive {**enable** | **disable**}

set radius keepalive time *minutes*

Syntax Description

enable	Enables the RADIUS keepalive timer.
disable	Disables the RADIUS keepalive timer.
time	Specifies the RADIUS keepalive timer interval.
minutes	Number of minutes between checks of configured RADIUS servers; valid values are from 1 to 65535 minutes.

Defaults

The timer is enabled and set to 5 minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

For every RADIUS keepalive timer interval, a test RADIUS request with username azbycx is sent to all configured RADIUS servers. If the server sends a response, the server is marked “Active.” If no response is received during the timer interval and the server was already “Dead,” the RADIUS server remains in the “Dead” state.

If the RADIUS server was previously “Active” but now does not send a response, the server is in the “Checkup” state. During the “Checkup” state interval, the test RADIUS request is resent. To specify the number of times that the request is sent, enter the **set radius retransmit** *count* command.

Examples

This example shows how to disable the RADIUS keepalive timer:

```
Console> (enable) set radius keepalive disable
Radius Keepalive disabled.
Console> (enable)
```

This example show how to set the RADIUS keepalive timer interval to 60 minutes:

```
Console> (enable) set radius keepalive time 60
Radius keepalive time set to 60 minutes.
Console> (enable)
```

Related Commands

set radius auto-initialize
set radius retransmit
show radius

8.6 EFT Copy

set radius key

To set the encryption and authentication for all communication between the RADIUS client and the server, use the **set radius key** command.

set radius key *key*

Syntax Description

key	Name of the key to authenticate the transactions between the RADIUS client and the server.

Defaults

The default of the key is set to null.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The key you set must be the same one as configured in the RADIUS server. All leading spaces are ignored; spaces within and at the end of the key are not ignored. Double quotes are not required even if there are spaces in the key, unless the quotes themselves are part of the key. The length of the key is limited to 65 characters; it can include any printable ASCII characters except tabs.

If you configure a RADIUS key on the switch, make sure you configure an identical key on the RADIUS server.

Examples

This example shows how to set the RADIUS encryption and authentication key to Make my day:

```
Console> (enable) set radius key Make my day
Radius key set to Make my day.
Console> (enable)
```

Related Commands

show radius

set radius retransmit

To specify the number of times the RADIUS servers are tried before giving up on the server, use the **set radius retransmit** command.

set radius retransmit *count*

Syntax Description

count	Number of times the RADIUS servers are tried before giving up on the server; valid values are from 1 to 100.

Defaults

The default is two times.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the retransmit attempts to 3:

```
Console> (enable) set radius retransmit 3
Radius retransmit count set to 3.
Console> (enable)
```

Related Commands

set radius keepalive
show radius

set radius server

To set up the RADIUS server, use the **set radius server** command.

set radius server *ipaddr* [**auth-port** *port*] [**acct-port** *port*] [**primary**]

Syntax Description

ipaddr	Number of the IP address or IP alias in dot notation a.b.c.d.
auth-port *port*	(Optional) Specifies a destination User Datagram Protocol (UDP) port for RADIUS authentication messages.
acct-port *port*	(Optional) Specifies a destination UDP port for RADIUS accounting messages.
primary	(Optional) Specifies that this server be contacted first.

Defaults

The default **auth-port** is 181, and the default **acct-port** is 1813.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you configure multiple RADIUS servers, the first server configured is the primary. Authentication requests are sent to this server first. You can specify a particular server as primary by using the **primary** keyword. You can add up to three RADIUS servers.

The *ipaddr* value can be entered as an IP alias or an IP address in dot notation a.b.c.d.

If you set the **auth-port** *port* to 0, the RADIUS server will not be used for authentication. If you set the **acct-port** *port* to 0, the RADIUS server will not be used for accounting.

If you configure a RADIUS key on the switch, make sure you configure an identical key on the RADIUS server.

You must specify a RADIUS server before enabling RADIUS on the switch.

Examples

This example shows how to add a primary server using an IP alias:

```
Console> (enable) set radius server everquest.com auth-port 0 acct-port 1646 primary
everquest.com added to RADIUS server table as primary server.
Console> (enable)
```

This example shows how to add a primary server using an IP address:

```
Console> (enable) set radius server 172.22.11.12 auth-port 0 acct-port 1722 primary
172.22.11.12 added to RADIUS server table as primary server
Console> (enable)
```

Related Commands

show radius

set radius timeout

To set the time between retransmissions to the RADIUS server, use the **set radius timeout** command.

set radius timeout *seconds*

Syntax Description

seconds	Number of seconds to wait for a reply; valid values are from 1 to 1000 seconds.

Defaults

The default timeout is 5 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the time between retransmissions to 7 seconds:

```
Console> (enable) set radius timeout 7
Radius timeout set to 7 seconds.
Console> (enable)
```

Related Commands

show radius

8.6 EFT Copy

set rate-limit

To enable, disable, or set the Layer 2 rate limiters, use the **set rate-limit** command.

set rate-limit {**l2pdu** | **l2port-security** | **l2protocol-tunnel**} {**enable** | **disable**}

set rate-limit {**l2pdu** | **l2port-security** | **l2protocol-tunnel**} **rate** *rate*

Syntax Description

l2pdu	Specifies rate limiting for the spanning-tree BPDUs—IEEE and SSTP, CDP, UDLD, VTP, and PAgP.
l2port-security	Specifies rate limiting for port security.
l2protocol-tunnel	Specifies rate limiting for the protocol tunnel-encapsulated PDUs.
enable	Enables Layer 2 rate limiting.
disable	Disables Layer 2 rate limiting.
rate *rate*	Specifies the rate-limiting threshold in packets per seconds; valid values are from 10 to 1000000.

Defaults

The defaults are as follows:

- Rate limiting is disabled.
- If enabled, the default *rate* is 1000 packets per second.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure a maximum of four rate limiters.

The following restrictions apply if you want to enable rate limiting:

- Hardware-based rate limiters are supported on Catalyst 6500 series switches that are configured with a Distributed Forwarding Card 3A (DFC3A) or the Policy Feature Card 3 (PFC3) only.
- The Catalyst 6500 series switch cannot be in truncated mode. If you attempt to enable rate limiting and you are in truncated mode, a message is displayed.

If the rate limiter is enabled and some events cause the system to go from nontruncated mode to truncated mode, rate limiting is disabled and a message is displayed.

Rate limiters control packets as follows:

- The frames are classified as Layer 2 control frames by the destination MAC address. The destination MAC address used are as follows:
  - 0180.C200.0000 for IEEE BPDU
  - 0100.0CCC.CCCC for CDP
  - 0100.0CCC.CCCD for PVST/SSTP BPDU

- The software allocates an LTL index for the frames.
- The LTL index is submitted to the forwarding engine for aggregate rate limiting of all the associated frames.

The Layer 2 control packets are as follows:

- GVRP/GMRP
- 802.1X
- BPDUs
- CDP/DTP/PAgP/UDLD/LACP/VTP PDUs
- PVST/SSTP PDUs

Examples

This example shows how to enable Layer 2 rate limiting for PDUs:

```
Console>(enable) set rate-limit l2pdu enable
Layer 2 rate limiter for PDUs enabled on the switch.
Console>(enable)
```

This example shows how to enable Layer 2 rate limiting for port security:

```
Console> (enable) set rate-limit l2port-security enable
l2port-security rate limiter enabled.
Console> (enable)
```

This example shows how to disable Layer 2 rate limiting for protocol tunnel-encapsulated PDUs:

```
Console>(enable) set rate-limit l2protocol-tunnel disable
Layer 2 rate limiter for l2protocol-tunnel disabled on the switch.
Console>(enable)
```

This example shows how to set the Layer 2 rate limiter value for PDUs:

```
Console>(enable) set rate-limit l2pdu rate 1000
Layer 2 rate limiter for PDU rate set to 1000.
Console>(enable)
```

This example shows how to set the Layer 2 rate limiter value for port security:

```
Console> (enable) set rate-limit l2port-security rate 10000
l2port-security rate limiter rate set to 10000 pps.
Console> (enable)
```

Related Commands

show rate-limit

set rcp username

To specify your username for rcp file transfers, use the **set rcp username** command.

set rcp username *username*

Syntax Description

username	Username up to 14 characters long.

Defaults

There are no default settings for this command.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The username can be a maximum of 40 characters, must be different from “root,” and not a null string.

The only case where you cannot configure the rcp username is for the VMPS database where you will use an rcp VMPS username. Use the **set vmps downloadmethod** command to specify the rcp VMPS username.

Examples

This example shows how to set the username for rcp:

```
Console> (enable) set rcp username jdoe
Console> (enable)
```

Related Commands

clear rcp
set vmps downloadmethod
show rcp

set rgmp

To enable or disable the Router-Ports Group Management Protocol (RGMP) feature on the switch, use the **set rgmp** command.

set rgmp {**enable** | **disable**}

Syntax Description

enable	Enables RGMP on the switch.
disable	Disables RGMP on the switch.

Defaults

The default is RGMP is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set rgmp** command affects the entire switch. You cannot enable or disable RGMP on a per-VLAN basis.

The RGMP feature is operational only if IGMP snooping is enabled on the switch. (See the **set igmp** command.)

Examples

This example shows how to enable RGMP on the switch:

```
Console> (enable) set rgmp enable
RGMP is enabled.
Console> (enable)
```

This example shows how to disable RGMP on the switch:

```
Console> (enable) set rgmp disable
RGMP is disabled.
Console> (enable)
```

Related Commands

clear rgmp statistics
set igmp
show rgmp group
show rgmp statistics

set rspan

To create remote Switched Port Analyzer (SPAN) sessions, use the **set rspan** command.

set rspan disable source [*rspan_vlan* | **all**]

set rspan disable session *session_number*

set rpsan disable destination [*mod/port* | **all**]

set rspan disable destination session *session_number*

set rspan source {*src_mod/src_ports...* | *vlans...* | **sc0**} {*rspan_vlan*} [**rx** | **tx** | **both**] **session** *session_number* [**multicast** {**enable** | **disable**}] [**filter** *vlans...*] [**create**]

set rspan destination *mod/port* {*rspan_vlan*} **session** *session_number* [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}] [**create**]

Syntax Description

disable source	Disables remote SPAN source information.
rspan_vlan	(Optional) Remote SPAN VLAN.
all	(Optional) Disables all remote SPAN source or destination sessions.
session *session_number*	Specifies a unique SPAN session across all types of SPAN sessions.
disable destination	Disables remote SPAN destination information.
mod/port	(Optional) Remote SPAN destination port.
src_mod/src_ports...	Monitored ports (remote SPAN source).
vlans...	Monitored VLANs (remote SPAN source).
sc0	Specifies the inband port is a valid source.
rx	(Optional) Specifies that information received at the source (ingress SPAN) is monitored.
tx	(Optional) Specifies that information transmitted from the source (egress SPAN) is monitored.
both	(Optional) Specifies that information both transmitted from the source (ingress SPAN) and received (egress SPAN) at the source are monitored.
multicast enable	(Optional) Enables monitoring multicast traffic (egress traffic only).
multicast disable	(Optional) Disables monitoring multicast traffic (egress traffic only).
filter *vlans*	(Optional) Monitors traffic on selected VLANs on source trunk ports.
create	(Optional) Creates a new remote SPAN session instead of overwriting the previous SPAN session.
inpkts enable	(Optional) Allows the remote SPAN destination port to receive normal ingress traffic (from the network to the bus) while forwarding the remote SPAN traffic.
inpkts disable	(Optional) Disables the receiving of normal inbound traffic on the remote SPAN destination port.
learning enable	(Optional) Enables learning for the remote SPAN destination port.
learning disable	(Optional) Disables learning for the remote SPAN destination port.

Defaults

The defaults are as follows:

- Remote SPAN is disabled.
- No VLAN filtering.
- Monitoring multicast traffic is enabled.
- Learning is enabled.
- inpkts is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

The *rspan_vlan* variable is optional in the **set rspan disable source** command and required in the **set rspan source** and **set rspan destination** command set.

After you enable SPAN, system defaults are used if no parameters were ever set. If you changed parameters, these are stored in NVRAM, and the new parameters are used.

Use a network analyzer to monitor ports.

Use the **inpkts** keyword with the **enable** option to allow the remote SPAN destination port to receive normal incoming traffic in addition to the traffic mirrored from the remote SPAN source. Use the **disable** option to prevent the remote SPAN destination port from receiving normal incoming traffic.

You can specify an Multilayer Switch Module (MSM) port as the remote SPAN source port. However, you cannot specify an MSM port as the remote SPAN destination port.

When you enable the **inpkts** option, a warning message notifies you that the destination port does not join STP and may cause loops if this option is enabled.

If you do not specify the keyword **create** and you have only one session, the session will be overwritten. If a matching *rspan_vlan* or destination port exists, the particular session will be overwritten (with or without specifying **create**). If you specify the keyword **create** and there is no matching *rspan_vlan* or destination port, the session will be created.

Each switch can source only one remote SPAN session (ingress, egress, or both). When you configure a remote ingress or bidirectional SPAN session in a source switch, the limit for local ingress or bidirectional SPAN session is reduced to one. There are no limits on the number of remote SPAN sessions carried across the network within the remote SPAN session limits.

You can configure any VLAN as a remote SPAN VLAN as long as these conditions are met:

- The same remote SPAN VLAN is used for a remote SPAN session in the switches.
- All the participating switches have appropriate hardware and software.
- No unwanted access port is configured in the remote SPAN VLAN.

If you do not specify a SPAN session number, one is provided by the software. The software provides a session number only if the basic check for the SPAN session limits and sanity is successful.

8.6 EFT Copy

If you provide a session number, but the same session number for the same session type is present in the SPAN database already, the session number that you enter overwrites the SPAN session with the same number. If the same session number is already present in the database, but that session number is for a different session type, the session number that you enter is rejected.

If you provide a session number that does not exist in the SPAN database, the number is regarded as a new SPAN session request and is subject to SPAN session limits.

Examples

This example shows how to disable all enabled source sessions:

```
Console> (enable) set rspan disable source all
This command will disable all remote span source session(s).
Do you want to continue (y/n) [n]? y
Disabled monitoring of all source(s) on the switch for remote span.
Console> (enable)
```

This example shows how to disable one source session to a specific VLAN:

```
Console> (enable) set rspan disable source 903
Disabled monitoring of all source(s) on the switch for rspan_vlan 903.
Console> (enable)
```

This example shows how to disable all enabled destination sessions:

```
Console> (enable) set rspan disable destination all
This command will disable all remote span destination session(s).
Do you want to continue (y/n) [n]? y
Disabled monitoring of remote span traffic on ports 9/1,9/2,9/3,9/4,9/5,9/6.
Console> (enable)
```

This example shows how to disable one destination session to a specific port:

```
Console> (enable) set rspan disable destination 4/1
Disabled monitoring of remote span traffic on port 4/1.
Console> (enable)
```

Related Commands

show rspan

set security acl adjacency

To set an entry for the adjacency table, use the **set security acl adjacency** command.

set security acl adjacency *adjacency_name dest_vlan dest_mac* [*source_mac* [**mtu** *mtu_size*] | **mtu** *mtu_size*]

Syntax Description

adjacency_name	Name of the adjacency table entry.
dest_vlan	Name of the destination VLAN.
dest_mac	Destination MAC address.
source_mac	(Optional) Source MAC address.
mtu *mtu_size*	(Optional) Specifies packet size in bytes.

Defaults

The default size for the MTU is 9600 bytes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The order of ACEs in a policy-based forwarding (PBF) VACL is important. The adjacency table entry has to be defined in the VACL before the redirect ACE because the redirect ACE uses it to redirect traffic. Refer to the *Catalyst 6500 Series Switch Software Configuration Guide* for detailed information on configuring PBF VACLs.

You can set the MTU when jumbo frames are sent using PBF.

Examples

This example shows how to set an entry for the adjacency table:

```
Console> (enable) set security acl adjacency ADJ1 11 0-0-0-0-0-B 0-0-0-0-0-A
Console> (enable)
```

This example shows how to set an entry for the adjacency table with a specific MTU size:

```
Console> (enable) set security acl adjacency a_1 2 0-0a-0a-0a-0a-0a 9000
Console> (enable)
```

Related Commands

clear security acl
commit
show security acl

set security acl arp-inspection

To configure Address Resolution Protocol (ARP) inspection features, use the **set security acl arp-inspection** command.

set security acl arp-inspection {**match-mac** | **address-validation**} {**enable** | [**drop** [**log**]] | **disable**}

set security acl arp-inspection dynamic {**enable** | **disable**} {*vlanlist* | **port** *mod/port*}

set security acl arp-inspection dynamic log {**enable** | **disable**}

Syntax Description

match-mac	Specifies the MAC address matching feature.
address-validation	Specifies the address validation feature.
enable	Enables the specified ARP inspection feature.
drop	(Optional) Indicates to drop **match-mac** or **address-validation** packets.
log	(Optional) Enables logging of **match-mac** or **address-validation** packets that are dropped.
disable	Disables the specified ARP inspection feature.
dynamic	Specifies the Dynamic ARP Inspection (DAI) bindings feature for a list of VLANs.
vlanlist	VLANs included in DAI.
port	Specifies a port to be included in DAI.
mod/port	Number of the module and the port on module.
log	Specifies logging for DAI.

Defaults

The MAC address matching, address validation, DAI, and the DAI logging features are disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enter the **set security acl arp-inspection match-mac enable** command, the system drops packets in which the source Ethernet address in the Ethernet header is not the same as the source MAC address in the ARP header.

When you enter the **set security acl arp-inspection address-validation enable** command, the system drops packets that have illegal IP or MAC addresses.

The following IP addresses are illegal:

- 0.0.0.0
- 255.255.255.255

- Class D multicast IP addresses

The following MAC addresses are illegal:

- 00-00-00-00-00-00
- Multicast MAC addresses
- ff-ff-ff-ff-ff-ff

Note If you do not enter the **drop** keyword, the system only generates a syslog message.

The **set security acl arp-inspection dynamic** {**enable** | **disable**} *vlanlist* command enables or disables DAI bindings for specified VLANs. The command does not affect any static ARP inspection rules that are specified as part of the security ACL framework.

Do not enable DAI on a VLAN unless DHCP Snooping is also enabled on the VLAN. You cannot enable DAI on management VLANs.

Do not enable DAI on VLANs that have ports with static IP addresses unless the ports are trusted.

If DAI is enabled for a VLAN that is untrusted for ARP inspection, the port should be untrusted for DHCP snooping. Otherwise, all ARP packets from that port will be dropped because bindings are not kept for ports trusted by DHCP snooping.

The **set security acl arp-inspection dynamic log** {**enable** | **disable**} command enables or disables the logging of packets that have been denied because of dynamic bindings. If logging is enabled, all packets dropped because of dynamic bindings are logged. If logging is disabled, these packets are not logged. DAI logging is configured on a global basis and does not affect per-ACE logging that is specified for static bindings.

Examples

This example shows how to enable the MAC address matching feature:

```
Console> (enable) set security acl arp-inspection match-mac enable
ARP Inspection match-mac feature enabled.
Console> (enable)
```

This example shows how to enable the address validation feature:

```
Console> (enable) set security acl arp-inspection address-validation enable
ARP Inspection address-validation feature enabled.
Console> (enable)
```

This example shows how to enable the dynamic ARP inspection feature:

```
Console> (enable) set security acl arp-inspection dynamic enable 100
Dynamic ARP Inspection is enabled for vlan(s) 100.
Console> (enable)
```

This example shows how to enable the dynamic ARP inspection logging feature:

```
Console> (enable) set security acl arp-inspection dynamic log enable
Dynamic ARP Inspection logging enabled.
Console> (enable)
```

Related Commands

set port arp-inspection
set security acl ip

set security acl capture-ports

To set the ports (specified with the **capture** option in the **set security acl ip**, **set security acl ipx**, and **set security acl mac** commands) to show traffic captured on these ports, use the **set security acl capture-ports** command.

set security acl capture-ports {*mod/ports...*}

Syntax Description

mod/ports...	Module and port number.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering this command are saved in NVRAM. This command *does not* require that you enter the **commit** command.

The module and port specified in this command are added to the current ports configuration list.

This command works with Ethernet ports only; you cannot set ATM ports.

The ACL capture will not work unless the capture port is in the spanning tree forwarding state for the VLAN.

Examples

This example shows how to set a port to capture traffic:

```
Console> (enable) set security acl capture-ports 3/1
Successfully set 3/1 to capture ACL traffic.
Console> (enable)
```

This example shows how to set multiple ports to capture traffic:

```
Console> (enable) set security acl capture-ports 1/1-10
Successfully set the following ports to capture ACL traffic: 1/1-2.
Console> (enable)
```

Related Commands

clear security acl capture-ports
show security acl capture-ports

set security acl cram

To enable a test run of the compression and reordering of ACL masks (CRAM) feature or to enable the CRAM feature, use the **set security acl cram** command.

set security acl cram testrun

set security acl cram {**run** | {**auto** [*nsec*]}}

Syntax Description

testrun	Tests ACL mask usage if CRAM was executed.
run	Manually executes the CRAM feature.
auto	Automatically executes the CRAM feature at specified interval.
nsec	(Optional) CRAM timer; valid values are 60 to 3600 seconds.

Defaults

The default time for the CRAM timer is 300 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When the CRAM feature is executed, the new mask ordering is computed and the ACL hardware is programmed accordingly.

The CRAM feature can be run in two modes. To manually execute the CRAM feature, enter the **set security acl cram run** command. To automatically execute the CRAM feature whenever the TCAM is full, enter the **set security acl cram auto** command.

The CRAM timer runs CRAM at an interval that you specify even if the TCAM is not full.

Note With software release 8.4(1), the CRAM feature is only supported for security ACLs. The CRAM feature works for QoS ACLs but you cannot specifically run the feature on QoS ACLs.

Examples

This example shows how to execute a test run of the CRAM feature:

```
Console> (enable) set security acl cram testrun
CRAM execution in progress.

CRAM execution complete.
Current ACL storage mask usage 60.0%
ACL storage mask usage if CRAM is run is 41.0%
Console> (enable)
```

This example shows how to manually execute the CRAM feature:

```
Console> (enable) set security acl cram run
Traffic may be disrupted for some time while programming hardware. Agree (y/n)[n] ? y
CRAM execution in progress.

CRAM execution complete.
Previous ACL storage mask usage 60.0%
Current ACL storage mask usage 41.0%
Console> (enable)
```

This example shows how to enable the automatic execution of the CRAM feature:

```
Console> (enable) set security acl cram auto
Cram auto mode enabled. Timer is default =  300 seconds
Console> (enable)
```

This example shows how to change the CRAM timer interval:

```
Console> (enable) set security acl cram auto 1000
Cram auto mode enabled. Timer is 1000 seconds
Console> (enable)
```

Related Commands

clear security acl cram
show security acl cram

set security acl feature ratelimit

To specify a rate limit in packets per second for ARP inspection, DHCP snooping, and 802.1X DHCP features, use the **set security acl feature ratelimit** command.

set security acl feature ratelimit *rate*

Syntax Description

rate	Number of packets; valid values are **0** and from 500 to 2000 packets per second. See the “Usage Guidelines” section for more information.

Defaults

The *rate* is 1000 pps.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set security acl feature ratelimit** command sets the rate at which packets are sent to the supervisor engine for processing by the ARP inspection, DHCP snooping, and 802.1X DHCP features.

If you want to disable rate limiting, enter a *rate* value of 0. We strongly recommend, however, that you do not disable rate limiting because traffic that is redirected by various security features might flood the supervisor engine and diminish system performance.

The rate limit is shared by multiple features. To display the features sharing rate limiting, enter the **show security acl feature ratelimit** command.

The rate limit is available on the PFC2 or later.

To specify the rate limit for the number of ARP inspection packets that are sent to the CPU on a per-port basis, use the **set port arp-inspection** command.

Examples

This example shows how to set the global rate limit to 600:

```
Console> (enable) set security acl feature ratelimit 600
ARP Inspection, DHCP Snooping, and Dot1x DHCP global rate limit set to 600 pps.
Console> (enable)
```

This example shows how to disable rate limiting:

```
Console> (enable) set security acl feature ratelimit 0
CAUTION:ARP Inspection, DHCP Snooping, and Dot1x DHCP global rate limit is disabled.
Console> (enable) 2004 Feb 04 16:17:17 %ACL-4-ARPINSPECTRATELIMITDISABLED:ARP Inspection,
DHCP Snooping, and Dot1x DHCP global rate is disabled
Console> (enable)
```

Related Commands

set port arp-inspection
show security acl feature ratelimit

set security acl ip

To create a new entry in a standard IP VACL and append the new entry at the end of the VACL, use the **set security acl ip** command.

set security acl ip {*acl_name*} {**permit** | **deny**} {*src_ip_spec*} [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**]

set security acl ip {*acl_name*} [**permit** | **deny**] **arp**

set security acl ip {*acl_name*} **permit dot1x-dhcp** [**before** *edit_buffer* | **modify** *edit_buffer*]

set security acl ip {*acl_name*} **permit dhcp-snooping** {**before** *editbuffer_index* | **modify** *editbuffer_index*}

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*adj_name* | *mod_num/port_num*}} {*protocol*} {*src_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**ip**] {*src_ip_spec* | **group** *group_name*} {*dest_ip_spec* | **group** *group_name*} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**icmp** | **1**] {*src_ip_spec*} {*dest_ip_spec*} [*icmp_type*] [*icmp_code*] | [*icmp_message*] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**tcp** | **6**] {*src_ip_spec*} [*operator port* [*port*]] {*dest_ip_spec*} [*operator port* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**udp** | **17**] {*src_ip_spec*} [*operator port* [*port*]] {*dest_ip_spec*} [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**]

set security acl ip {*acl_name*} {**permit** | **deny**} **arp-inspection** {**host** *ip_addr*} {*mac_addr* | **any** [**log**]}

set security acl ip {*acl_name*} {**permit** | **deny**} **arp-inspection any any** [**log**] [**before** *edit_buffer* | **modify** *edit_buffer*]

set security acl ip {*acl_name*} {**permit** | **deny**} **arp-inspection** {**host** *ip_addr*} {*ip_mask*} **any** [**log**]

set security acl ip {*acl_name*} **permit any**

set security acl ip {*acl_name*} [**permit**] **eapoudp** [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set security acl ip {*acl_name*} **include** {**downloaded-acl** | **ip-phone**} {*feature*}

Syntax Description

acl_name	Unique name that identifies the lists to which the entry belongs.
permit	Allows traffic from the source IP address.
deny	Blocks traffic from the source IP address.
src_ip_spec	Source IP address and the source mask. See the “Usage Guidelines” section for the format.
before *editbuffer_index*	(Optional) Inserts the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Replaces an ACE with the new ACE.
log	(Optional) Logs denied packets.
arp	Specifies ARP.
dot1x-dhcp	Specifies 802.1X authentication for the DHCP Relay Agent.
dhcp-snooping	Specifies DHCP snooping.
redirect	Specifies to which switched ports the packet is redirected.
adj_name	Name of the adjacency table entry.
mod_num/port_num	Number of the module and port.
protocol	Keyword or number of an IP protocol; valid numbers are from 0 to 255 representing an IP protocol number. See the “Usage Guidelines” section for the list of valid keywords.
dest_ip_spec	Destination IP address and the destination mask. See the “Usage Guidelines” section for the format.
precedence *precedence*	(Optional) Specifies the precedence level; valid values are from 0 to 7 or by name. See the “Usage Guidelines” section for a list of valid names.
tos *tos*	(Optional) Specifies the type of service level; valid values are from 0 to 15 or by name. See the “Usage Guidelines” section for a list of valid names.
fragment	(Optional) Filters IP traffic that carries fragments.
capture	(Optional) Specifies packets are switched normally and captured; **permit** must also be enabled.
ip	(Optional) Matches any Internet Protocol packet.
icmp | **1**	(Optional) Matches ICMP packets.
icmp-type	(Optional) ICMP message type name or a number; valid values are from 0 to 255. See the “Usage Guidelines” section for a list of valid names.
icmp-code	(Optional) ICMP message code name or a number; valid values are from 0 to 255. See the “Usage Guidelines” section for a list of valid names.
icmp-message	(Optional) ICMP message type name or ICMP message type and code name. See the “Usage Guidelines” section for a list of valid names.
tcp | **6**	(Optional) Matches TCP packets.
operator	(Optional) Operands; valid values include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).
port	(Optional) Number or name of a TCP or UDP port; valid port numbers are from 0 to 65535. See the “Usage Guidelines” section for a list of valid names.
established	(Optional) Specifies an established connection; used only for TCP protocol.
udp | **17**	(Optional) Matches UDP packets.
arp-inspection	Specifies ARP inspection.

host *ip_addr*	Specifies the host and host's IP address.
mac_addr	Specifies the MAC address.
any	Matches any IP address or MAC address.
ip_mask	Specifies the IP mask.
eapoudp	Redirects all LPIP contol packets (EAPoUDP) to the supervisor engine.
include	Creates a place holder for an ACE.
downloaded-acl | ip-phone	Specifies either a downloaded ACL or an IP phone ACE.
feature	Specifies the feature type and applies only to downloaded ACLs. This can be dot1x, webauth, macauth-bypass, or eou.

Defaults

There are no default ACLs and no default ACL-VLAN mappings. By default, ARP is enabled. By default, DHCP snooping is disabled on all VLANs.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering this command are saved to NVRAM and the switch hardware only after you enter the **commit** command. Enter ACEs in batches, and then enter the **commit** command to save them in NVRAM and in the hardware.

The **arp** keyword is supported on switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2). The **arp** keyword is supported on a per-ACL basis only; either ARP is allowed or ARP is denied.

If you use the **fragment** keyword in an ACE, this ACE applies to nonfragmented traffic and to the fragment with offset equal to zero in a fragmented flow.

A fragmented ACE that permits Layer 4 traffic from host A to host B also permits fragmented traffic from host A to host B regardless of the Layer 4 port.

If you use the **capture** keyword, the ports that capture the traffic and transmit out are specified by entering the **set security acl capture-ports** command.

802.1X and DHCP Snooping cannot coexist on a VLAN. If both features are configured on a VLAN, the feature that resides higher up in the ACL will override the other.

The position of the DHCP-Snooping Access Control Entry (ACE) in the VACL is important, as it can be used to restrict specific types of DHCP packets. The position of the DHCP Snooping ACE is determined by the policy for DHCP Snooping packets. For example, if you want to deny DHCP Snooping packets from a certain host and perform DHCP Snooping on other packets, then the deny ACE should come before the DHCP Snooping ACE.

When you enter the ACL name, follow these naming conventions:

- Maximum of 32 characters long and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types

- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are **all**, **default-action**, **map**, **help**, and **editbuffer**

When you specify the source IP address and the source mask, use the form *source_ip_address source_mask* and follow these guidelines:

- The *source_mask* is required; 0 indicates a care bit, 1 indicates a don't-care bit.
- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0.

When you enter a destination IP address and the destination mask, use the form *destination_ip_address destination_mask*. The destination mask is required.

- Use a 32-bit quantity in a four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host**/source as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0.

The **log** keyword is an option of **deny** only. If you want to change an existing VACL configuration to **deny** with **log**, you must first clear the VACL and then set it again.

The **log** keyword is supported on systems configured with Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Valid names for *precedence* are critical, flash, flash-override, immediate, internet, network, priority, and routine.

Valid names for *tos* are max-reliability, max-throughput, min-delay, min-monetary-cost, and normal.

Valid *protocol* keywords include **icmp** (1), **ip**, **ipinip** (4), **tcp** (6), **udp** (17), **igrp** (9), **eigrp** (88), **gre** (47), **nos** (94), **ospf** (89), **ahp** (51), **esp** (50), **pcp** (108), and **pim** (103). The IP number is displayed in parentheses. Use the keyword **ip** to match any Internet Protocol.

ICMP packets that are matched by ICMP message type can also be matched by the ICMP message code.

Valid names for *icmp_type* and *icmp_code* are administratively-prohibited, alternate-address, conversion-error, dod-host-prohibited, dod-net-prohibited, echo, echo-reply, general-parameter-problem, host-isolated, host-precedence-unreachable, host-redirect, host-tos-redirect, host-tos-unreachable, host-unknown, host-unreachable, information-reply, information-request, mask-reply, mask-request, mobile-redirect, net-redirect, net-tos-redirect, net-tos-unreachable, net-unreachable, network-unknown, no-room-for-option, option-missing, packet-too-big, parameter-problem, port-unreachable, precedence-unreachable, protocol-unreachable, reassembly-timeout, redirect, router-advertisement, router-solicitation, source-quench, source-route-failed, time-exceeded, timestamp-reply, timestamp-request, traceroute, ttl-exceeded, and unreachable.

If the operator is positioned after the source and source-wildcard, it must match the source port. If the operator is positioned after the destination and destination-wildcard, it must match the destination port. The range operator requires two port numbers. All other operators require one port number.

TCP port names can be used only when filtering TCP. Valid names for TCP ports are bgp, chargen, daytime, discard, domain, echo, finger, ftp, ftp-data, gopher, hostname, irc, klogin, kshell, lpd, nntp, pop2, pop3, smtp, sunrpc, syslog, tacacs-ds, talk, telnet, time, uucp, whois, and www.

UDP port names can be used only when filtering UDP. Valid names for UDP ports are biff, bootpc, bootps, discard, dns, dnsix, echo, mobile-ip, nameserver, netbios-dgm, netbios-ns, ntp, rip, snmp, snmptrap, sunrpc, syslog, tacacs-ds, talk, tftp, time, who, and xdmcp.

The number listed with the protocol type is the layer protocol number (for example, **udp** | **17**).

If no layer protocol number is entered, you can enter the following syntax:

set security acl ip {*acl_name*} {**permit** | **deny**} {*src_ip_spec*} [**before** *editbuffer_index* | **modify** *editbuffer_index*]

If a Layer 4 protocol is specified, you can enter the following syntax:

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** *mod_num/port_num*} {*protocol*} {*src_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

For IP, you can enter the following syntax:

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**ip**] {*src_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

For ICMP, you can enter the following syntax:

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**icmp** | **1**] {*src_ip_spec*} {*dest_ip_spec*} [*icmp_type*] [*icmp_code*] | [*icmp_message*] [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

For TCP, you can enter the following syntax:

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**tcp** | **6**] {*src_ip_spec*} [*operator port* [*port*]] {*dest_ip_spec*} [*operator port* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

For UDP, you can enter the following syntax:

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**udp** | **17**] {*src_ip_spec*} [*operator port* [*port*]] {*dest_ip_spec*} [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Note With PFC2, the counters report if a particular ACE was hit during a 300 ms window, but the counters do not indicate how much traffic hit the entry. For example, if you have two flows where one flow is 1000 packets per second and the second flow is 10 packets per second, both flows return the same result with a PFC2. PFC3 and later PFCs do not have this limitation.

Examples

These examples show different ways to use the **set security acl ip** commands to configure IP security ACLs:

```
Console> (enable) set security acl ip IPACL1 deny 1.2.3.4 0.0.0.0
IPACL1 editbuffer modified.  Use 'commit' command to apply changes.
```

```
Console> (enable)

Console> (enable) set security acl ip IPACL1 deny host 171.3.8.2 before 2
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)

Console> (enable) set security acl ip IPACL1 permit any any
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)

Console> (enable) set security acl ip IPACL1 redirect 3/1 ip 3.7.1.2 0.0.0.255 host
255.255.255.255 precedence 1 tos min-delay
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)

Console> (enable) set security acl ip IPACL1 permit ip host 60.1.1.1 host 60.1.1.98
capture
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

This example shows how to create a placeholder for a downloaded ACL:

```
Console> set security acl ip test include downloaded-acl dot1x
Console> Successfully configured placeholder download ACL test. Use
  'commit' command to save changes.
Console> show security acl info test
set security acl ip test
--------------------------------------------------
1. permit arp-inspection
2. permit eapoudp
3. include downloaded-acl dot1x
4. permit url-redirect
5. deny ip any any
```

Related Commands

clear eou
clear security acl
clear security acl capture-ports
clear security acl map
clear security acl statistics
commit
set eou
set port eou
set security acl map
set security acl capture-ports
show security acl
show security acl capture-ports
show security acl downloaded-acl

set security acl ipx

To create a new entry in a standard IPX VACL and to append the new entry at the end of the VACL, use the **set security acl ipx** command.

set security acl ipx {*acl_name*} {**permit** | **deny** | **redirect** *mod_num/port_num*} {*protocol*} {*src_net*} [*dest_net***.**[*dest_node*] [[*dest_net_mask***.**]*dest_node_mask*]] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
permit	Allows traffic from the specified source IPX address.
deny	Blocks traffic from the specified source IPX address.
redirect	Redirects traffic from the specified source IPX address.
mod_num/port_num	Number of the module and port.
protocol	Keyword or number of an IPX protocol; valid values are from 0 to 255 representing an IPX protocol number. See the “Usage Guidelines” section for a list of valid keywords and corresponding numbers.
src_net	Number of the network from which the packet is being sent. See the “Usage Guidelines” section for format guidelines.
*dest_net***.**	(Optional) Number of the network from which the packet is being sent.
dest_node	(Optional) Node on destination-network to which the packet is being sent.
*dest_net_mask***.**	(Optional) Mask to be applied to the destination network. See the “Usage Guidelines” section for format guidelines.
dest_node_mask	(Optional) Mask to be applied to the destination-node. See the “Usage Guidelines” section for format guidelines.
capture	(Optional) Specifies packets are switched normally and captured.
before *editbuffer_index*	(Optional) Inserts the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Replaces an ACE with the new ACE.

Defaults

There are no default ACLs and no default ACL-VLAN mappings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command. Enter ACEs in batches, and then enter the **commit** command to save all of them in NVRAM and in the hardware.

If you use the **capture** keyword, the ports that capture the traffic and transmit out are specified by entering the **set security acl capture-ports** command.

When you enter the ACL name, follow these naming conventions:

- Maximum of 32 characters long and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types
- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer

Valid *protocol* keywords include **ncp** (17), **netbios** (20), **rip** (1), **sap** (4), and **spx** (5).

The *src_net* and *dest_net* variables are eight-digit hexadecimal numbers that uniquely identify network cable segments. When you specify the *src_net* or *dest_net*, use the following guidelines:

- It can be a number in the range 0 to FFFFFFFF. A network number of -1 or **any** matches all networks.
- You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.

The *dest_node* is a 48-bit value represented by a dotted triplet of 4-digit hexadecimal numbers (xxxx.xxxx.xxxx).

The *dest_net_mask***.** is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must be immediately followed by a period, which must in turn be immediately followed by the destination-node-mask. You can enter this value only when *dest_node* is specified.

The *dest_node_mask* is a 48-bit value represented as a dotted triplet of 4-digit hexadecimal numbers (xxxx.xxxx.xxxx). Place ones in the bit positions you want to mask. You can enter this value only when *dest_node* is specified.

The *dest_net_mask***.** is an eight-digit hexadecimal number that uniquely identifies the network cable segment. It can be a number in the range 0 to FFFFFFFF. A network number of -1 or **any** matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA. Following are *dest_net_mask***.** examples:

- 123A
- 123A.1.2.3
- 123A.1.2.3 ffff.ffff.ffff
- 1.2.3.4 ffff.ffff.ffff.ffff

Use the **show security acl** command to display the list.

Examples

This example shows how to block traffic from a specified source IPX address:

```
Console> (enable) set security acl ipx IPXACL1 deny 1.a
IPXACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

This example shows how to deny traffic from hosts in specific subnet (10.1.2.0/8):

```
Console> (enable) set security acl ipx SERVER deny ip 10.1.2.0 0.0.0.255 host 10.1.1.100
IPXACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

Related Commands

clear security acl
clear security acl capture-ports
clear security acl map
commit
set security acl map
set security acl capture-ports
show security acl
show security acl capture-ports

set security acl log

To configure the security ACL log table, use the **set security acl log** command.

set security acl log maxflow *max_flows*

set security acl log ratelimit *max_rate*

Syntax Description

maxflow *max_flows*	Specifies the maximum flow pattern number in packets per second; valid values are from 256 to 2048.
ratelimit *max_rate*	Specifies the redirect rate in packets per second; valid values are 0 and from 500 to 5000. See the "Usage Guidelines" section for more information.

Defaults

The default *max_number* is 500 packets per second and the default *ratelimit* is 2500 packets per second.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The command is supported on systems configured with Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

The **set security acl log maxflow** command tries to allocate a new log table based on the maximum flow pattern number to store logged packet information. If successful, the new buffer replaces the old one and all flows in the old table are cleared. If either memory is not enough or the maximum number is over the limit, an error message is displayed and the command is dropped.

The **set security acl log ratelimit** command tries to set the redirect rate in packets per second. If the configuration is over the range, the command is discarded and the range is displayed on the console.

If you want to disable rate limiting for VACL logging, enter a *rate* argument of 0.

Examples

This example shows how to set the maximum flow:

```
Console> (enable) set security acl log maxflow 322
Log table size set to 322 flow entries.
Console> (enable)
```

This example shows how to set the rate limit:

```
Console> (enable) set security acl log ratelimit 3444
Max logging eligible packet rate set to 3444pps.
Console> (enable)
```

This example shows how to disable rate limiting:

```
Console> (enable) set security acl log rate-limit 0
CAUTION: Rate limit for logging eligible packet is disabled.
2003 Apr 07 07:13:36 %ACL-4-VACLLOGRATELIMITDISABLED:VACL Logging rate limit disabled
Console> (enable)
```

Related Commands

clear security acl log flow
show security acl log

8.6 EFT Copy

set security acl mac

To create a new entry in a non-IP or non-IPX protocol VACL and to append the new entry at the end of the VACL, use the **set security acl mac** command.

set security acl mac {*acl_name*} {**permit** | **deny**} {*src_mac_addr_spec*} {*dest_mac_addr_spec*} [*ethertype*] [**cos** *cos_value*] [**vlan** *vlan*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
permit	Allows traffic from the specified source MAC address.
deny	Blocks traffic from the specified source MAC address.
src_mac_addr_spec	Source MAC address and mask in the form *source_mac_address source_mac_address_mask*.
dest_mac_addr_spec	Destination MAC address and mask.
ethertype	(Optional) Number or name that matches the Ethertype for Ethernet-encapsulated packets; valid values are **0x0600**, **0x0601**, **0x0BAD**, **0x0BAF**, **0x6000-0x6009**, **0x8038-0x8042**, **0x809b**, and **0x80f3**. See the “Usage Guidelines” section for a list of valid names.
cos *cos_value*	(Optional) Specifies the CoS value; valid values are from 0 to 7.
vlan *vlan*	(Optional) Specifies a VLAN; valid values are from 1 to 4094.
capture	(Optional) Specifies packets are switched normally and captured.
before *editbuffer_index*	(Optional) Inserts the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Replaces an ACE with the new ACE.

Defaults

There are no default ACLs and no default ACL-VLAN mappings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Configurations you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command. Enter ACEs in batches, and then enter the **commit** command to save all of them in NVRAM and in the hardware.

If you use the **capture** keyword, the ports that capture the traffic and transmit out are specified by entering the **set security acl capture-ports** command.

8.6 EFT Copy

When you enter the ACL name, follow these naming conventions:

- Maximum of 32 characters long and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types
- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer

The *src_mac_addr_spec* is a 48-bit source MAC address and mask and entered in the form of *source_mac_address source_mac_address_mask* (for example, 08-11-22-33-44-55 ff-ff-ff-ff-ff-ff). Place ones in the bit positions you want to mask. When you specify the *src_mac_addr_spec*, follow these guidelines:

- The *source_mask* is required; 0 indicates a care bit; 1 indicates a don't-care bit.
- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0.

The *dest_mac_spec* is a 48-bit destination MAC address and mask and entered in the form of *dest_mac_address dest_mac_address_mask* (for example, 08-00-00-00-02-00/ff-ff-ff-00-00-00). Place ones in the bit positions you want to mask. The destination mask is mandatory. When you specify the *dest_mac_spec*, use the following guidelines:

- Use a 48-bit quantity in 6-part dotted-hexadecimal format for a source address and mask.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0-0-0-0-0-0-0 ff-ff-ff-ff-ff-ff.
- Use **host** source as an abbreviation for a *destination* and *destination-wildcard* of destination 0-0-0-0-0-0.

Valid names for Ethertypes (and corresponding numbers) are EtherTalk (0x809B), AARP (0x8053), dec-mop-dump (0x6001), dec-mop-remote-console (0x6002), dec-phase-iv (0x6003), dec-lat (0x6004), dec-diagnostic-protocol (0x6005), dec-lavc-sca (0x6007), dec-amber (0x6008), dec-mumps (0x6009), dec-lanbridge (0x8038), dec-dsm (0x8039), dec-netbios (0x8040), dec-msdos (0x8041), banyan-vines-echo (0x0baf), xerox-ns-idp (0x0600), xerox-address-translation (0x0601), and IPv4 (0x8000).

Use the **show security acl** command to display the list.

Note With PFC2, the counters report if a particular ACE was hit during a 300 ms window, but the counters do not indicate how much traffic hit the entry. For example, if you have two flows where one flow is 1000 packets per second and the second flow is 10 packets per second, both flows return the same result with a PFC2. PFC3 and later PFCs do not have this limitation.

Examples

This example shows how to block traffic to an IP address:

```
Console> (enable) set security acl mac MACACL1 deny 01-02-02-03-04-05
MACACL1 editbuffer modified. User 'commit' command to apply changes.
Console> (enable)
```

Related Commands

clear security acl
clear security acl capture-ports
clear security acl map
commit
set security acl map
set security acl capture-ports
show security acl
show security acl capture-ports

set security acl map

To map an existing ACL to a port or to a VLAN or to enable ACL statistics, use the **set security acl map** command.

set security acl map *acl_name* {*mod/port* | *vlans*} [**statistics** {**enable** | **disable**}]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
mod/port	Number of the module and the port on the module.
vlans	Number of the VLANs to be mapped to the VACL; valid values are from 1 to 4094.
statistics	(Optional) Specifies ACL statistics on a per-VLAN basis.
enable	Enables ACL statistics on a per-VLAN basis.
disable	Disables ACL statistics on a per-VLAN basis.

Defaults

There are no default ACLs and no default ACL-to-VLAN mappings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you use this command, the configurations are saved in NVRAM. This command *does not* require that you enter the **commit** command. Each VLAN can be mapped to only one ACL of each type (IP, IPX, and MAC). An ACL can be mapped to a VLAN only after you have committed the ACL.

When you enter the ACL name, follow these naming conventions:

- Maximum of 32 characters long and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types
- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer

Caution Use the **copy** command to save the ACL configuration to Flash memory.

You can map an ACL to a port even if the port is in VLAN-based PACL mode. In such cases, the configuration is committed to NVRAM and is later restored to the hardware when the port is changed to port-based or merge mode.

Note Mapping an ACL to a port is only available with a Supervisor Engine 720.

If per-VLAN statistics are enabled on a VLAN, subsequent maps configured on the same VLAN will also have per-VLAN statistics enabled. If per-VLAN statistics are disabled on a VLAN, previous maps configured on the same VLAN will also have per-VLAN statistics disabled.

For example, if you enter the **set security acl map ip1 1 statistics enable** command followed by the **set security acl map mac1 1** command, the MAC 1 ACL will also have per-VLAN statistics enabled.

If you enter the **set security acl map ip1 1 statistics enable** command followed by the **set security acl map mac1 1 statistics disable** command, the ip1 ACL will also have per-VLAN statistics disabled.

Note In the per-VLAN mode, label sharing is disabled resulting in more labels being used.

Note With a PFC2, the counters report if a particular ACE was hit during a 300 ms window, but the counters do not indicate how much traffic hit the entry. For example, if you have two flows where one flow is 1000 packets per second and the second flow is 10 packets per second, both flows return the same result on a PFC2. The PFC3 and later PFCs do not have this limitation.

Examples

This example shows how to map an existing ACL to a VLAN:

```
Console> (enable) set security acl map IPACL1 1
ACL IPACL1 mapped to vlan 1
Console> (enable)
```

This example shows the output if you try to map an ACL that has not been committed:

```
Console> (enable) set security acl map IPACL1 1
Commit ACL IPACL1 before mapping.
Console> (enable)
```

This example shows the output if you try to map an ACL that is already mapped to a VLAN for the ACL type (IP, IPX, or MAC):

```
Console> (enable) set security acl map IPACL2 1
Mapping for this type already exists for this VLAN.
Console> (enable)
```

This example shows how to map an ACL to a port:

```
Console> (enable) set security acl map ipacl1 3/1
Mapping in progress.
ACL ipacl1 is successfully mapped to port(s) 3/1.
Console> (enable)
```

This example shows how to enable ACL statistics on a per-VLAN basis:

```
Console> (enable) set security acl map ACL1 1 statistics enable
Mapping in progress.

ACL ACL1 successfully mapped to VLAN 1.
Console> (enable)
```

Related Commands

clear security acl
clear security acl map
commit
set port security-acl
show port security-acl
show security acl
show security acl map

8.6 EFT Copy

set security acl statistics

To enable aggregated ACL statistics on a per-ACL basis, use the **set security acl statistics** command.

set security acl statistics {**all** | *acl_name*}

Syntax Description

all	Enables aggregated ACL statistics on all ACLs.
acl_name	Name of the ACL.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

In aggregated statistics mode, the statistics are enabled for all the ACEs in the specified ACL. This command is effective only after you enter the **commit** command to commit all ACEs to NVRAM.

This command overwrites the per-ACE command, **set security acl ip/mac** *acl_name* … [**statistics**].

The aggregated statistics mode disables the merge optimization and can result in a larger number of ACEs. In some cases, an ACL that was previously installed in the TCAM might not fit in the TCAM after aggregated statistics mode is enabled.

Note With a PFC2, the counters report if a particular ACE was hit during a 300 ms window, but the counters do not indicate how much traffic hit the entry. For example, if you have two flows where one flow is 1000 packets per second and the second flow is 10 packets per second, both flows return the same result on a PFC2. The PFC3 and later PFCs do not have this limitation.

Examples

This example shows how to enable aggregated ACL statistics on a per-ACL basis:

```
Console> (enable) set security acl statistics ACL1
ACL1 editbuffer modified. Use 'commit' command to save changes.
Console> (enable) commit security acl ACL1
ACL commit in progress.

ACL 'ACL1' successfully committed.
Console> (enable)
```

Related Commands

clear security acl counters
clear security acl statistics

set snmp

To enable or disable the processing of SNMP requests to the switch and SNMP traps from the switch, use the **set snmp** command.

set snmp {**enable** | **disable**}

Syntax Description

enable	Enables SNMP processing.
disable	Disables SNMP processing.

Defaults

By default, SNMP processing is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When SNMP processing is enabled, the switch processes SNMP inquiries and sends out SMNP traps if there are no conflicts with other SNMP configurations. When SNMP processing is disabled, the switch ignores SNMP requests and no SNMP traps are sent out regardless of other SNMP configurations.

Whether SNMP processing is enabled or disabled, you can change other SNMP configurations, and RMON-related processes are not affected.

The SNMP ifIndex persistence feature is always enabled. With the ifIndex persistence feature, the ifIndex value of the port and VLAN is always retained and used after the following occurrences:

- Switch reboot
- High-availability switchover
- Software upgrade
- Module reset
- Module removal and insertion of the same type of module

For Fast EtherChannel and Gigabit EtherChannel interfaces, the ifIndex value is only retained and used after a high-availability switchover.

Examples

This example shows how to disable SNMP processing:

```
Console> (enable) set snmp disable
SNMP disabled
Console> (enable)
```

Related Commands

show snmp

set snmp access

To define the access rights of an SNMP group, use the **set snmp access** command.

set snmp access [**-hex**] {*groupname*} {**security-model** {**v1** | **v2c**}} [**read** [**-hex**] {*readview*}] [**write** [**-hex**] {*writeview*}] [**notify** [**-hex**] {*notifyview*}] [**volatile** | **nonvolatile**]

set snmp access [**-hex**] {*groupname*} {**security-model v3** {**noauthentication** | **authentication** | **privacy**}} [**read** [**-hex**] {*readview*}] [**write** [**-hex**] {*writeview*}] [**notify** [**-hex**] {*notifyview*}] [**context** [**-hex**] *contextname* [**exact** | **prefix**]] [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Displays the *groupname, readview, writeview*, *notifyview*, and *contextname* in a hexadecimal format.
groupname	Name of the SNMP group.
security-model v1 | **v2c**	Specifies security-model v1 or v2c.
read *readview*	(Optional) Specifies the name of the view that allows you to see the MIB objects.
write *writeview*	(Optional) Specifies the name of the view that allows you to configure the contents of the agent.
notify *notifyview*	(Optional) Specifies the name of the view that allows you to send a trap about MIB objects.
v3	Specifies security model v3.
noauthentication	Specifies security model is not set to use authentication protocol.
authentication	Specifies the type of authentication protocol.
privacy	Specifies the messages sent on behalf of the user are protected from disclosure.
volatile	(Optional) Specifies that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
context *contextname*	(Optional) Specifies the name of the context string and the way to match the context string; maximum of 32 characters.
exact	(Optional) Specifies that an exact match between the *contextname* and the value of vacmAccessContextPrefix is required to select this entry.
prefix	(Optional) Specifies that only a match between vacmAccessContextPrefix and the starting portion of *contextname* is required to select this entry.

Defaults

The defaults are as follows:

- storage type is **nonvolatile**.
- **read** *readview* is Internet OID space.
- **write** *writeview* is NULL OID.

- **notify** *notifyview* is NULL OID.
- **context** *contextname* is a NULL string.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *groupname, readview, writeview,* and *notifyview* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

readview is assumed to be every object belonging to the Internet (1.3.6.1) OID space; you can use the read option to override this state.

For *writeview*, you must also configure write access.

For *notifyview*, if a view is specified, any notifications in that view are sent to all users associated with the group. (An SNMP server host configuration must exist for the user.)

For *contextname*, the string is treated as either a full context name or the prefix of a context name, depending on whether you enter the **exact** or **prefix** keyword. If you enter the **prefix** keyword, this allows you to enter a simple form of wildcarding. For example, if you enter a *contextname* of vlan, vlan-1 and vlan-100 will be selected.

If you do not enter a context name, a NULL context string is used.

Examples

This example shows how to set the SNMP access rights for a group:

```
Console> (enable) set snmp access cisco-group security-model v3 authentication
SNMP access group was set to cisco-group version v3 level authentication, readview
internet, nonvolatile.
Console> (enable)
```

Related Commands

clear snmp access
show snmp access
show snmp context

set snmp access-list

To specify an access list number for a host or group of hosts, use the **set snmp access-list** command.

set snmp access-list *access_number IP_address* [**ipmask** *maskaddr*]

Syntax Description

access_number	Number that specifies a list of hosts that are pemitted to use a specific community string; valid values are 1 to 65535.
IP_address	IP address that is associated with the access list. See the “Usage Guidelines” section for more information.
ipmask *maskaddr*	(Optional) Sets a mask for the IP address. See the “Usage Guidelines” section for more in information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you want to associate multiple IP addresses to the same access list, you must enter one IP address at a time in the CLI.

If you use an access list number that is already in use, the new IP addresses are appended to the access list. You can clear one or more IP addresses associated with an access list by entering the **clear snmp access-list** command.

The *maskaddr* variable is in the format xxx.xxx.xxx.xxx.

Examples

This example shows how to associate the IP address of a host to access list number 1:

```
Console> (enable) set snmp access-list 1 172.20.60.100
Host 172.20.60.100 is associated with access number 1.
Console> (enable)
```

This example shows how to associate multiple IP addresses to access list number 1:

```
Console> (enable) set snmp access-list 1 10.1.1.1
Console> (enable) set snmp access-list 1 10.1.1.2
Console> (enable) set snmp access-list 1 10.1.1.3
Console> (enable)
```

This example shows how to associate the IP address and subnet mask of a host to access list number 2:

```
Console> (enable) set snmp access-list 2 172.20.60.100 ipmask 255.0.0.0
Access nmber 2 has been created with new IP Address 172.20.60.100 mask 255.0.0.0
Console> (enable)
```

Related Commands

clear snmp access-list
show snmp access-list

set snmp buffer

To set the size of the SNMP UDP socket receive buffer, use the **set snmp buffer** command.

set snmp buffer {*packets*}

Syntax Description

packets	Number of packets allowed in the buffer; valid ranges are from 32 to 95.

Defaults

95 packets.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can adjust the SNMP UDP socket receive buffer up to 95 packets by using the **set snmp buffer** command.

Examples

This example shows how to set the SNMP UDP socket receive buffer to 45:

```
Console> (enable) set snmp buffer 45
SNMP socket receive buffer set to 45 packets.
Console> (enable)
```

This example shows the error message the displays when you try to set the SNMP UDP socket receive buffer above the valid range:

```
Console> (enable)  set snmp buffer 100
Invalid input. Must be an integer between 32 and 95.
Console> (enable)
```

Related Commands

show snmp buffer

set snmp chassis-alias

To set the chassis alias and save it in NVRAM and in the configuration file, use the **set snmp chassis-alias** command.

set snmp chassis-alias [*chassisAlias*]

Syntax Description

chassisAlias	(Optional) Chassis entPhysicalAlias. See the "Usage Guidelines" section for more information about setting the chassis alias.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The *chassisAlias* value must be from 0 to 32 characters.

To clear the current *chassisAlias* value, enter the **set snmp chassis-alias** command without entering a *chassisAlias* value.

Examples

This example shows how to set the chassis alias:

```
Console> (enable) set snmp chassis-alias my chassis
SNMP chassis entPhysicalAlias set to 'my chassis'.
Console> (enable)
```

This example shows how to clear the chassis alias:

```
Console> (enable) set snmp chassis-alias
SNMP chassis entPhysicalAlias cleared.
Console> (enable)
```

This example shows the message that appears when you attempt to set a chassis alias that exceeds 32 characters:

```
Console> (enable) set snmp chassis-alias 123456789123456789123456789123456789
Chassis entPhysicalAlias must be less than 33 characters.
Console> (enable)
```

Related Commands

show snmp

set snmp community

To set SNMP communities and associated access types, use the **set snmp community** command.

set snmp community {**read-only** | **read-write** | **read-write-all**} [*community_string*]

set snmp community index [**-hex**] *index-name* **name** *community_string* **security** [**-hex**] *security-name* [**context** [**-hex**] *context-name*] [**volatile** | **nonvolatile**] [**transporttag** [**-hex**] *tag-value*]

Syntax Description

read-only	Assigns read-only access to the specified SNMP community.
read-write	Assigns read-write access to the specified SNMP community.
read-write-all	Assigns read-write access to the specified SNMP community.
community_string	(Optional) Name of the SNMP community.
index	Sets the SNMP community index
-hex	(Optional) Specifies the SNMP community index in hexadecimal format.
index-name	SNMP community index name.
name	Sets the SNMP community name.
security	Sets the SNMP community security name.
security-name	SNMP community security name.
context	(Optional) Sets the SNMP context name.
context-name	(Optional) SNMP community context name.
volatile	(Optional) Specifies that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
transporttag	(Optional) Specifies SNMP transport endpoints.
tag-value	(Optional) Transport tag value.

Defaults

The default is the following communities and access types are defined:

- public—**read-only**
- private—**read-write**
- secret—**read-write-all**

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

8.6 EFT Copy

There are three configurable SNMP communities, one for each access type. If you do not specify the community string, the community string configured for that access type is cleared.

The *community_string* variable cannot contain the @ symbol.

To support the access types, you also need to configure four MIB tables: vacmContextTable, vacmSecurityToGroupTable, vacmAccessTable, and vacmViewTreeFamilyTable. Use the **clear config snmp** command to reset these tables to the default values.

Examples

This example shows how to set read-write access to the SNMP community called yappledapple:

```
Console> (enable) set snmp community read-write yappledapple
SNMP read-write community string set to yappledapple.
Console> (enable)
```

This example shows how to clear the community string defined for read-only access:

```
Console> (enable) set snmp community read-only
SNMP read-only community string cleared.
Console> (enable)
```

Related Commands

clear config
clear snmp community
show snmp
show snmp community

set snmp community-ext

To set additional community strings, use the **set snmp community-ext** command.

set snmp community-ext *community_string* {**read-only** | **read-write** | **read-write-all**}
[**view** *view_oid*] [**access** *access_number*]

Syntax Description

community_string	Name of the SNMP community.
read-only	Assigns read-only access to the specified SNMP community.
read-write	Assigns read-write access to the specified SNMP community.
read-write-all	Assigns read-write access to the specified SNMP community.
view *view_oid*	(Optional) Restricts the community string to a view. See the "Usage Guidelines" section for more information.
access *access_number*	(Optional) Restricts the community string to an access number; valid values are from 1 to 65335.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Types

Privileged.

Usage Guidelines

Adding a new community string using the **set snmp community-ext** command creates appropriate entries in the vacmAccessTable (if a view is specified), snmpCommunityTable, and vacmSecurityToGroup tables.

An example of the *view_oid* variable is 1.3.6.1.2.1.

Examples

This example shows how to set an additional SNMP community string:

```
Console> (enable) set snmp community-ext public1 read-only
Community string public1 is created with access type as read-only
Console> (enable)
```

This example shows how to restrict the community string to an access number:

```
Console> (enable) set snmp community-ext private1 read-write access 2
Community string private1 is created with access type as read-write access
number 2
Console> (enable)
```

This example shows how to change the access number to the community string:

```
Console> (enable) set snmp community-ext private1 read-write access 3
Community string private1 is updated with access type as read-write access
number 3
Console> (enable)
```

Related Commands

clear snmp community-ext

set snmp extendedrmon netflow

To enable or disable the SNMP extended RMON support for the NAM module, use the **set snmp extendedrmon netflow** command.

set snmp extendedrmon netflow {**enable** | **disable**} {*mod*}

Syntax Description

enable	Enables the extended RMON support.
disable	Disables the extended RMON support.
mod	Module number of the extended RMON NAM.

Defaults

The default is SNMP-extended RMON NetFlow is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable SNMP-extended RMON NetFlow support:

```
Console> (enable) set snmp extendedrmon netflow enable 2
Snmp extended RMON netflow enabled
Console> (enable)
```

This example shows how to disable SNMP-extended RMON NetFlow support:

```
Console> (enable) set snmp extendedrmon netflow disable 2
Snmp extended RMON netflow disabled
Console> (enable)
```

This example shows the response when the SNMP-extended RMON NetFlow feature is not supported:

```
Console> (enable) set snmp extendedrmon enable 4
NAM card is not installed.
Console> (enable)
```

Related Commands

set snmp rmon
show snmp

set snmp group

To establish the relationship between an SNMP group and a user with a specific security model, use the **set snmp group** command.

set snmp group [**-hex**] {*groupname*} **user** [**-hex**] {*username*}
{**security-model** {**v1** | **v2c** | **v3**}} [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Displays the *groupname* and *username* in a hexadecimal format.
groupname	Name of the SNMP group that defines an access control; the maximum length is 32 bytes.
user	Specifies the SNMP group username.
username	Name of the SNMP user that belongs to the SNMP group; the maximum length is 32 bytes.
security-model v1 | v2c | v3	Specifies security-model v1, v2c, or v3.
volatile	(Optional) Specifies that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *groupname* or *username* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to set the SNMP group:

```
Console> (enable) set snmp group cisco-group user joe security-model v3
SNMP group was set to cisco-group user joe and version v3,nonvolatile.
Console> (enable)
```

Related Commands

clear snmp group
show snmp group

set snmp ifalias

To set the SNMP interface alias, use the **set snmp ifalias** command.

set snmp ifalias {*ifIndex*} [*ifAlias*]

Syntax Description

ifIndex	Interface index number.
ifAlias	(Optional) Name of the interface alias. See the “Usage Guidelines” section for more information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The *ifAlias* string can contain 0 to 64 characters.

Examples

This example shows how to set the SNMP interface alias:

```
Console> (enable) set snmp ifalias 1 Inband port
ifIndex 1 alias set
Console> (enable)
```

Related Commands

clear snmp ifalias
show snmp ifalias

set snmp inform

To configure the handling of SNMP inform requests, use the **set snmp inform** command.

set snmp inform *value*

set snmp inform *rcvr_address rcvr_community* [**port** *rcvr_port*] [**index** *rcvr_index*]

Syntax Description

value	Number of SNMP inform requests that are kept in the inform request queue; valid values are from 25 to 65536.
rcvr_address	IP address or IP alias of the SNMP host that will receive the SNMP inform request.
rcvr_community	Community string that will receive the SNMP inform request.
port *rcvr_port*	(Optional) Specifies the UDP port for the SNMP inform request.
index *rcvr_index*	(Optional) Specifies the index for the SNMP inform request; valid values are from 1 to 65535.

Defaults

100 SNMP inform requests are kept in the SNMP inform request queue.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The switch can send notifications to SNMP managers when particular events occur. For example, an SNMP agent switch might send a message to an SNMP manager when the agent switch experiences an error condition.

SNMP notifications can be sent as traps or inform requests. Inform requests are more reliable than traps because the receiver sends a response when it gets an inform request. However, the receiver does not send a response when it gets a trap. The switch discards the trap after it is sent.

With the SNMP inform request feature, the switch sends the inform request to the SNMP manager and waits for a SNMP response PDU from the manager. If the switch never receives a response, it tries to send the inform request again. To configure the period of time that the switch waits to resend the inform request, use the **set snmp targetaddr** command. Use the **set snmp targetaddr** command to configure how long the inform request stays in the queue before it times out.

Sending SNMP inform requests consumes more resources in the switch and in the network than sending SNMP traps. Unlike a trap, an inform request must be held in memory until a response is received or the request times out.

If it is important that the SNMP manager receives every notification, use inform requests.

Setting the inform request queue size restricts the number of inform requests that stay in the inform request queue. If you do not limit the size of the queue, the switch memory will be consumed quickly, especially if the timeout value is too small, if the retry value is too large, and if the SNMP inform request receiver is unreachable.

If the number of inform requests that are pending in the queue exceeds the configured limit, the oldest inform request is removed to free up space for new inform requests.

Examples

This example shows how to configure the number of inform requests that will stay in the queue:

```
Console> (enable) set snmp inform 150
Size of inform queue has been set to 150
Console> (enable)
```

Related Commands

clear snmp inform
set snmp trap
set snmp targetaddr
show snmp inform

8.6 EFT Copy

set snmp notification mapping

To set the notifyname entry in the snmpNotifyTable and the notifytag entry in the snmpTargetAddrTable, use the **set snmp notify** command.

set snmp notify [**-hex**] {*notifyname*} **tag** [**-hex**] {*notifytag*}
[**trap** | **inform**] [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Displays the notifyname and notifytag in a hexadecimal format.
notifyname	Identifier to index the snmpNotifyTable.
tag	Specifies the tag name in the taglist.
notifytag	Name of entries in the snmpTargetAddrTable.
trap	(Optional) Specifies all messages that contain snmpv2-Trap PDUs.
inform	(Optional) Specifies all messages that contain InfoRequest PDUs.
volatile	(Optional) Specifies that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.

Defaults

The defaults are storage type is **volatile** and notify type is **trap**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *notifyname* and *notifytag* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to set the SNMP notify for a specific notifyname:

```
Console> (enable) set snmp notify hello tag world inform
SNMP notify name was set to hello with tag world notifyType inform, and storageType
nonvolatile.
Console> (enable)
```

Related Commands

clear snmp notify
show snmp notify

set snmp notify

To set the notifyname entry in the snmpNotifyTable and the notifytag entry in the snmpTargetAddrTable, use the **set snmp notify** command.

set snmp notify [**-hex**] {*notifyname*} **tag** [**-hex**] {*notifytag*}
[**trap** | **inform**] [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Displays the notifyname and notifytag in a hexadecimal format.
notifyname	Identifier to index the snmpNotifyTable.
tag	Specifies the tag name in the taglist.
notifytag	Name of entries in the snmpTargetAddrTable.
trap	(Optional) Specifies all messages that contain snmpv2-Trap PDUs.
inform	(Optional) Specifies all messages that contain InfoRequest PDUs.
volatile	(Optional) Specifies that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.

Defaults

The defaults are storage type is **volatile** and notify type is **trap**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *notifyname* and *notifytag* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to set the SNMP notify for a specific notifyname:

```
Console> (enable) set snmp notify hello tag world inform
SNMP notify name was set to hello with tag world notifyType inform, and storageType
nonvolatile.
Console> (enable)
```

Related Commands

clear snmp notify
show snmp notify

set snmp rmon

To enable or disable SNMP RMON support, use the **set snmp rmon** command.

set snmp rmon {**enable** | **disable**}

Syntax Description

enable	Activates SNMP RMON support.
disable	Deactivates SNMP RMON support.

Defaults

The default is RMON support is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

RMON statistics are collected on a segment basis.

The RMON feature deinstalls all of the domains for all of the interfaces on an Ethernet module that has been removed from the system.

When you enable RMON, the supported RMON groups for Ethernet ports are Statistics, History, Alarms, and Events as specified in RFC 1757.

Use of this command requires a separate software license.

Examples

This example shows how to enable RMON support:

```
Console> (enable) set snmp rmon enable
SNMP RMON support enabled.
Console> (enable)
```

This example shows how to disable RMON support:

```
Console> (enable) set snmp rmon disable
SNMP RMON support disabled.
Console> (enable)
```

Related Commands

show port counters

set snmp rmonmemory

To set the memory usage limit in percentage, use the **set snmp rmonmemory** command.

set snmp rmonmemory *percentage*

Syntax Description

percentage	Memory usage limit; see the "Usage Guidelines" section for additional information.

Defaults

The default is 85 percent.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

When using this command, setting the percentage value to 85 does not mean that RMON can use 85 percent of memory. It means that you cannot create new RMON entries or restore entries from the NVRAM if the DRAM memory usage exceeds or will exceed 85 percent.

If you expect the device to run other sessions such as Telnet, a lower value should be set to the memory limit. Otherwise, the new Telnet sessions may fail because the available memory is not enough.

Examples

This example shows how to set the memory usage limit:

```
Console> (enable) set snmp rmonmemory 90
Console> (enable)
```

Related Commands

show snmp rmonmemory

set snmp targetaddr

To configure the SNMP target address entries in the snmpTargetAddressTable, use the **set snmp targetaddr** command.

set snmp targetaddr [**-hex**] {*addrname*} **param** [**-hex**] {*paramsname*} {*ipaddr*}
[**udpport** {*port*}] [**timeout** {*value*}] [**retries** {*value*}] [**volatile** | **nonvolatile**]
[**taglist** {[**-hex**] *tag*}] [[**-hex**] **tag** *tagvalue*]

Syntax Description

-hex	(Optional) Displays *addrname, paramsname, tagvalue*, and *tag* in a hexadecimal format.
addrname	Unique identifier to index the snmpTargetAddrTable; the maximum length is 32 bytes.
param	Specifies an entry in the snmpTargetParamsTable that provides parameters to be used when generating a message to the target; the maximum length is 32 bytes.
paramsname	Entry in the snmpTargetParamsTable; the maximum length is 32 bytes.
ipaddr	IP address of the target.
udpport *port*	(Optional) Specifies which UDP port of the target host to use.
timeout *value*	(Optional) Specifies the number of timeouts.
retries *value*	(Optional) Specifies the number of retries.
volatile	(Optional) Specifies that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
taglist *tag*	(Optional) Specifies a tag name in the taglist.
tag *tagvalue*	(Optional) Specifies the tag name.

Defaults

The defaults are as follows:

- storage type is **nonvolatile**.
- **udpport** is 162.
- **timeout** is 1500.
- **retries** is 3.
- **taglist** is NULL.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *addrname, paramsname, tag,* and *tagvalue* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

The maximum *tagvalue* and *taglist* length is 255 bytes.

Examples

This example shows how to set the target address in the snmpTargetAddressTable:

```
Console> (enable) set snmp targetaddr foo param bar 10.1.2.4 udp 160 timeout 10 retries 3
taglist tag1 tag2 tag3
SNMP targetaddr name was set to foo with param bar ipAddr 10.1.2.4, udpport 160, timeout
10, retries 3, storageType nonvolatile with taglist tag1 tag2 tag3.
Console> (enable)
```

Related Commands

clear snmp targetaddr
show snmp targetaddr

set snmp targetparams

To configure the SNMP parameters used in the snmpTargetParamsTable when generating a message to a target, use the **set snmp targetparams** command.

set snmp targetparams [**-hex**] {*paramsname*} **user** [**-hex**] {*username*} {**security-model** {**v1** | **v2c**}} {**message-processing** {**v1** | **v2c** | **v3**}} [**volatile** | **nonvolatile**]

set snmp targetparams [**-hex**] {*paramsname*} **user** [**-hex**] {*username*} {**security-model v3**} {**message-processing v3** {**noauthentication** | **authentication** | **privacy**}} [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Displays the *paramsname* and *username* in a hexadecimal format.
paramsname	Name of the parameter in the snmpTargetParamsTable; the maximum length is 32 bytes.
user	Specifies the SNMP group username.
username	Name of the SNMP user that belongs to the SNMP group; the maximum length is 32 bytes.
security-model v1 | **v2c**	Specifies security-model v1 or v2c.
message-processing v1 | **v2c** | **v3**	Specifies the version number used by the message processing model.
security-model v3	Specifies security-model v3.
message-processing v3	Specifies v3 is used by the message-processing model.
noauthentication	Specifies the security model is not set to use the authentication protocol.
authentication	Specifies the type of authentication protocol.
privacy	Specifies the messages sent on behalf of the user are protected from disclosure.
volatile	(Optional) Specifies that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.

Defaults

The default storage type is **volatile**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for the *paramsname* and *username* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

Examples

This example shows how to set target parameters in the snmpTargetParamsTable:

```
Console> (enable) set snmp targetparams bar user joe security-model v3 message-processing
v3 authentication
SNMP target params was set to bar v3 authentication, message-processing v3, user joe
nonvolatile.
Console> (enable)
```

Related Commands

clear snmp targetparams
show snmp targetparams

8.6 EFT Copy

set snmp trap

To enable or disable the different SNMP traps on the system or to add an entry into the SNMP authentication trap receiver table, use the **set snmp trap** command.

set snmp trap {**enable** | **disable**} [**all** | **auth** | **autoshutdown** | **bridge** | **callhomesmtp** | **chassis** | **config** | **entity** | **entityfru** | **envfan** | **envpower** | **envshutdown** | **envstate** | **envtemp** | **flashinsert** | **flashremove** | **inlinepower** {**module** *mod*} | **ippermit** | **l2tunnel** | **linkerrhigh** | **linkerrlow** | **macmove** | **macnotification** | **macthreshold** | **module** | **redundancy** | **stpx** | **syslog** | **system** | **vlancreation** | **vlandeletion** | **vmps** | **vtp**]

set snmp trap *rcvr_addr rcvr_community* [**port** *rcvr_port*] [**owner** *rcvr_owner*] [**index** *rcvr_index*]

Syntax Description

enable	Enables SNMP traps.
disable	Disables SNMP traps.
all	(Optional) Specifies all trap types and all port traps. See the “Usage Guidelines” section before using this option.
auth	(Optional) Specifies the authenticationFailure trap from RFC 1157.
autoshutdown	(Optional) Specifies the automatic module shutdown traps.
bridge	(Optional) Specifies the newRoot and topologyChange traps from RFC 1493 (the BRIDGE-MIB).
callhomesmtp	(Optional) Specifies the CallHome SMTP server traps.
chassis	(Optional) Specifies the chassisAlarmOn and chassisAlarmOff traps from the CISCO-STACK-MIB.
config	(Optional) Specifies the sysConfigChange trap from the CISCO-STACK-MIB.
entity	(Optional) Specifies the entityMIB trap from the ENTITY-MIB.
entityfru	(Optional) Specifies the entity field replaceable unit (FRU).
envfan	(Optional) Specifies the environmental fan.
envpower	(Optional) Specifies the environmental power.
envshutdown	(Optional) Specifies the environmental shutdown.
envstate	(Optional) Specifies the environmental monitoring status change traps.
envtemp	(Optional) Specifies the environmental monitoring temperature traps.
flashinsert	(Optional) Specifies flash insertion.
flashremove	(Optional) Specifies flash removal.
flexifchange	
inlinepower {**module** ***mod***}	(Optional) Specifies the inline power traps for a specific module; valid values for the *mod* argument are from 1 through 9, 15, and 16.
ippermit	(Optional) Specifies the IP Permit Denied access from the CISCO-STACK-MIB.
l2tunnel	(Optional) Specifies the Layer 2 protocol tunnel threshold traps.
linkerrhigh	(Optional) Specifies the traps for link error monitoring when the high threshold is exceeded.
linkerrlow	(Optional) Specifies the traps for link error monitoring when the low threshold is exceeded.
macmove	(Optional) Specifies MAC address move notification traps.

macnotification	(Optional) Specifies MAC address (CAM) notification traps.
macthreshold	(Optional) Specifies MAC address threshold notification traps.
module	(Optional) Specifies the moduleUp and moduleDown traps from the CISCO-STACK-MIB.
noauthfailvlan	
noguestvlan	
redundancy	(Optional) Specifies the redundancy status traps.
stpx	(Optional) Specifies the spanning tree extension traps.
syslog	(Optional) Specifies the syslog notification traps.
system	(Optional) Specifies the system notification traps.
sysinfolog	
vlancreate	(Optional) Specifies the VLAN creation traps.
vlandelete	(Optional) Specifies the VLAN deletion traps.
vmps	(Optional) Specifies the vmVmpsChange trap from the CISCO-VLAN-MEMBERSHIP-MIB.
vtp	(Optional) Specifies the VTP from the CISCO-VTP-MIB.
rcvr_addr	IP address or IP alias of the system to receive SNMP traps.
rcvr_community	Community string to use when sending authentication traps.
port *rcvr_port*	(Optional) Specifies the UDP port and port number; valid values are from 0 to 65535.
owner *rcvr_owner*	(Optional) Specifies the user who configured the settings for the SNMP trap; the valid value is a character string from 1 to 21 characters in length.
index *rcvr_index*	(Optional) Specifies index entries with the same *rcvr_addr*; valid values are from 0 to 65535.

Defaults

The default is SNMP traps are disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

An IP permit trap is sent when unauthorized access based on the IP permit list is attempted.

Use the **show snmp** command to verify the appropriate traps were configured.

To use this command, you must configure all notification tables: snmpTargetAddrTable, snmpTargetParamsTable, and snmpNotifyTable.

Use the **all** option to enable or disable all trap types and all port traps.

Use the **set port trap command** to enable or disable a single port or a range of ports.

The trap configuration is saved in NVRAM and the configuration file.

Examples

This example shows how to enable SNMP chassis traps:

```
Console> (enable) set snmp trap enable chassis
SNMP chassis alarm traps enabled.
Console> (enable)
```

This example shows how to enable all traps:

```
Console> (enable) set snmp trap enable
All SNMP traps enabled.
Console> (enable)
```

This example shows how to disable SNMP chassis traps:

```
Console> (enable) set snmp trap disable chassis
SNMP chassis alarm traps disabled.
Console> (enable)
```

This example shows how to enable SNMP MAC address notification traps:

```
Console> (enable) set snmp trap enable macnotification
SNMP MAC notification trap enabled.
Console> (enable)
```

This example shows how to add an entry in the SNMP trap receiver table:

```
Console> (enable) set snmp trap 192.122.173.42 public
SNMP trap receiver added.
Console> (enable)
```

This example shows how to enable the SNMP MAC move notification trap:

```
Console> (enable) set snmp trap enable macmove
SNMP MAC move notification trap enabled.
Console> (enable)
```

This example shows how to enable the SNMP MAC threshold notification trap:

```
Console> (enable) set snmp trap enable macthreshold
SNMP MAC threshold notification trap enabled.
Console> (enable)
```

This example shows to enable the automatic module shutdown traps:

```
Console> (enable) set snmp trap enable autoshutdown
SNMP module auto shutdown traps enabled.
Console> (enable)
```

Related Commands

clear snmp trap
set port trap
show snmp
test snmp trap

set snmp user

To configure a new SNMP user, use the **set snmp user** command.

set snmp user [**-hex**] {*username*} {**remote** {*engineid*}} [**authentication** {**md5** | **sha** | *authpassword*}] [**privacy** [**des** | **3des** | **aes** {**128** | **192** | **256**}] *privpassword*] [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Displays *username* in a hexadecimal format.
username	Name of the SNMP user.
remote *engineid*	Specifies the remote SNMP engine ID.
authentication	(Optional) Specifies the authentication protocol.
md5	Specifies HMAC-MD5-96 authentication protocol.
sha	Specifies HMAC-SHA-96 authentication protocol.
authpassword	Password for authentication.
privacy	(Optional) Enables the host to encrypt the contents of the message sent to or from the agent.
des	(Optional) Specifies DES as the privacy protocol.
3des	(Optional) Specifies 3DES as the privacy protocol. This option is only available in k9 images.
aes {**128** | **192** | **256**}	(Optional) Specifies AES as the privacy protocol. When you use the ***aes*** option, you must also specify the key length (128, 192 or 256 bits). This option is only available in k9 images.
privpassword	(Optional) Password that enables the host to encrypt the contents of the message sent to or from the agent; the maximum length is 32 characters.
volatile	(Optional) Specifies that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.

Defaults

The default storage type is **volatile**. If you do not specify **authentication**, the security level default will be **noauthentication**. If you do not specify **privacy**, the default will be no privacy. The privacy protocol is **des**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *username* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

The *authpassword* and *privpassword* values must be hexadecimal characters without delimiters in between.

Examples

This example shows how to set a specific username:

```
Console> (enable) set snmp user joe
Snmp user was set to joe authProt no-auth  privProt no-priv with engineid 00:00.
Console> (enable)
```

This example shows how to set a specific username, authentication, and authpassword:

```
Console> (enable) set snmp user John authentication md5 arizona2
Snmp user was set to John authProt md5 authPasswd arizona2. privProt no-priv wi.
Console> (enable)
```

Related Commands

clear snmp user
show snmp user

8.6 EFT Copy

set snmp view

To configure the SNMP MIB view, use the **set snmp view** command.

set snmp view [**-hex**]{*viewname*}{*subtree*}[**mask**] [**included** | **excluded**] [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Displays the *viewname* value in a hexadecimal format.
viewname	Name of a MIB view.
subtree	MIB subtree.
mask	(Optional) Specifies that the bit mask is used with the subtree. A bit mask can be all ones, all zeros, or any combination; the maximum length is 3 bytes.
included | **excluded**	(Optional) Specifies that the MIB subtree is included or excluded.
volatile	(Optional) Specifies that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies that the storage type is defined as persistent memory and the content remains after the device is turned off and on again.

Defaults

The defaults are as follows:

- Storage type is **volatile**.
- Bit mask is NULL.
- MIB subtree is **included**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *viewname* (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

A MIB subtree with a mask defines a view subtree. The MIB subtree can be in object identifier (OID) format or a text name mapped to a valid OID.

Examples

This example shows how to assign a subtree to the view public:

```
Console> (enable) set snmp view public 1.3.6.1 included
Snmp view name was set to public with subtree 1.3.6.1 included, nonvolatile.
Control> (enable)
```

This example shows the response when the subtree is incorrect:

```
Console> (enable) set snmp view stats statistics excluded
Statistics is not a valid subtree OID
Control> (enable)
```

Related Commands

clear snmp view
show snmp view

8.6 EFT Copy

set span

To enable or disable SPAN and to set up the switch port and VLAN analyzer for multiple SPAN sessions, use the **set span** command.

set span disable [*dest_mod/dest_port* | **all**]

set span disable session *session_number*

set span {*src_mod/src_ports* | *src_vlans* | **sc0**} {*dest_mod/dest_port*} [**rx** | **tx** | **both**]
[**session** *session_number*] [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}]
[**multicast** {**enable** | **disable**}] [**filter** *vlans...*] [**create**]

set span permit-list *mod/port* {**include** | **exclude**}

set span permit-list {**enable** | **disable**}

Syntax Description

disable	Disables SPAN.
dest_mod	(Optional) Monitoring module (SPAN destination).
dest_port	(Optional) Monitoring port (SPAN destination).
all	(Optional) Disables all SPAN sessions.
session *session_number*	Specifies a unique SPAN session across all types of SPAN sessions.
src_mod	Monitored module (SPAN source).
src_ports	Monitored ports (SPAN source).
src_vlans	Monitored VLANs (SPAN source).
sc0	Specifies the inband port is a valid source.
rx	(Optional) Specifies that information received at the source (ingress SPAN) is monitored.
tx	(Optional) Specifies that information transmitted from the source (egress SPAN) is monitored.
both	(Optional) Specifies that information both transmitted from the source (ingress SPAN) and received (egress SPAN) at the source are monitored.
inpkts enable	(Optional) Enables the receiving of normal inbound traffic on the SPAN destination port.
inpkts disable	(Optional) Disables the receiving of normal inbound traffic on the SPAN destination port.
learning enable	(Optional) Enables learning for the SPAN destination port.
learning disable	(Optional) Disables learning for the SPAN destination port.
multicast enable	(Optional) Enables monitoring multicast traffic (egress traffic only).
multicast disable	(Optional) Disables monitoring multicast traffic (egress traffic only).
filter *vlans*	(Optional) Monitors traffic on selected VLANs on source trunk ports.
create	(Optional) Creates a SPAN port.
permit-list	Specifies a list of ports that can be configured as SPAN or RSPAN destinations.
mod/port	Numbers of the modules and numbers of the ports on the modules.
include	Includes the specified ports in the permit list.

exclude	Removes the specified ports from the permit list.
enable	Enables the permit-list feature for all SPAN sessions.
disable	Disables the permit-list feature for all SPAN sessions.

Defaults

- SPAN is disabled,
- No VLAN filtering is enabled.
- Multicast is enabled.
- Input packets are disabled.
- Learning is enabled.
- The permit-list feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After you enable SPAN, system defaults are used if no parameters were ever set. If you changed parameters, the old parameters are stored in NVRAM, and the new parameters are used.

Use a network analyzer to monitor ports.

If you specify multiple SPAN source ports, the ports can belong to different VLANs.

A maximum of two **rx** or **both** SPAN sessions and four **tx** SPAN sessions can exist simultaneously. If you use a remote SPAN station, the maximum number of **rx** or **both** SPAN sessions is one.

Use the **inpkts** keyword with the **enable** option to allow the SPAN destination port to receive normal incoming traffic in addition to the traffic mirrored from the SPAN source. Use the **disable** option to prevent the SPAN destination port from receiving normal incoming traffic.

You can specify an MSM port as the SPAN source port. However, you cannot specify an MSM port as the SPAN destination port.

When you enable the **inpkts** option, a warning message notifies you that the destination port does not join STP and may cause loops if this option is enabled.

When you configure multiple SPAN sessions, the destination module number/port number must be known to index the particular SPAN session.

If you do not specify the keyword **create** and you have only one session, the session will be overwritten. If a matching destination port exists, the particular session will be overwritten (with or without specifying **create**). If you specify the keyword **create** and there is no matching destination port, the session will be created.

If any VLANs on SPAN source port(s) are blocked by spanning tree, you may see extra packets transmitted on the destination port that were not actually transmitted out of the source port(s). The extra packets seen at the destination port are packets sent through the switch fabric to the source port and then blocked by spanning tree at the source port.

To specify a unique SPAN session across all types of SPAN sessions (local SPAN, RSPAN, and ESPAN), enter the **session** *session_number* option. If you do not specify a SPAN session number, one is provided by the software. The software provides a session number only if the basic check for SPAN session limits and sanity is successful.

If you provide a session number, but the same session number for the same session type is present in the SPAN database already, the session number that you enter overwrites the SPAN session with the same number. If the same session number is already present in the database, but that session number is for a different session type, the session number that you enter is rejected.

If you provide a session number that does not exist in the SPAN database, the number is regarded as a new SPAN session request and is subject to SPAN session limits.

You can specify multiple destination ports in the CLI. However, you cannot mix VLANs and ports in the same SPAN session.

Examples

This example shows how to configure SPAN so that both transmit and receive traffic from port 1/1 (the SPAN source) is mirrored on port 2/1 (the SPAN destination):

```
Console> (enable) set span 1/1 2/1
Enabled monitoring of Port 1/1 transmit/receive traffic by Port 2/1
Console> (enable)
```

This example shows how to set VLAN 522 as the SPAN source and port 2/1 as the SPAN destination:

```
Console> (enable) set span 522 2/1
Enabled monitoring of VLAN 522 transmit/receive traffic by Port 2/1
Console> (enable)
```

This example shows how to set VLAN 522 as the SPAN source and port 3/12 as the SPAN destination. Only transmit traffic is monitored. Normal incoming packets on the SPAN destination port are allowed:

```
Console> (enable) set span 522 2/12 tx inpkts enable
SPAN destination port incoming packets enabled.
Enabled monitoring of VLAN 522 transmit traffic by Port 2/12
Console> (enable)
```

This example shows how to set port 3/2 as the SPAN source and port 2/2 as the SPAN destination:

```
Console> (enable) set span 3/2 2/2 tx create
Enabled monitoring of port 3/2 transmit traffic by Port 2/1
Console> (enable)
```

This example shows how to disable SPAN if multiple SPAN sessions are not defined:

```
Console> (enable) set span disable
This command WILL disable your span session(s).
Do you want to continue (y/n) [n]?y
Disabled all sessions
Console> (enable)
```

This example shows what happens if you try to enter the **set span disable** command (without the destination module number/port number defined) and multiple SPAN sessions are defined:

```
Console> (enable) set span disable
Multiple active span sessions. Please specify span destination to disable.
Console> (enable)
```

Related Commands

clear config
show span

set spantree backbonefast

To enable or disable the spanning tree BackboneFast Convergence feature, use the **set spantree backbonefast** command.

set spantree backbonefast {**enable** | **disable**}

Syntax Description

enable	Enables BackboneFast Convergence.
disable	Disables BackboneFast Convergence.

Defaults

The default is BackboneFast convergence is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

This command is not available in Multi-Instance Spanning Tree Protocol (MISTP) mode.

This command is not available in Multiple Spanning Tree (MST) mode.

For BackboneFast Convergence to work, you must enable it on all switches in the network.

When you try to enable BackboneFast and the switch is in Rapid PVST+ mode, this message is displayed:

```
Cannot enable backbonefast when the spantree mode is RAPID-PVST+.
```

Examples

This example shows how to enable BackboneFast Convergence:

```
Console> (enable) set spantree backbonefast enable
Backbonefast enabled for all VLANs.
Console> (enable)
```

This example shows the message that is displayed when you try to enable BackboneFast in Rapid PVST+ mode:

```
Console> (enable) set spantree backbonefast enable
Cannot enable backbonefast when the spantree mode is RAPID-PVST+.
Console> (enable)
```

Related Commands

show spantree

set spantree bpdu-filter

To enable or disable BPDU packet filtering on a port, use the **set spantree bpdu-filter** command.

set spantree bpdu-filter *mod/port* {**enable** | **disable** | **default**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables BPDU packet filtering.
disable	Disables BPDU packet filtering.
default	Sets BPDU packet filtering to the global BPDU packet filtering state. See the "Usage Guidelines" section for more information.

Defaults

The default is BPDU packet filtering is **default**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

BPDU packet filtering turns off BPDU transmission on ports.

If you enter the **default** keyword, the spanning tree port is set to the global BPDU filtering state.

To enable or disable BPDU filtering for all ports on the switch, enter the **set spantree global-default bpdu-filter** command.

Examples

This example shows how to enable BPDU filtering on module 3, port 4:

```
Console> (enable) set spantree bpdu-filter 3/4 enable
Warning: Ports enabled with bpdu filter will not send BPDUs and drop all
received BPDUs. You may cause loops in the bridged network if you misuse
this feature.
Spantree port 3/4 bpdu filter enabled.
Console> (enable)
```

Related Commands

set spantree global-default
show spantree portfast

8.6 EFT Copy

set spantree bpdu-guard

To enable or disable spanning tree BPDU guard on a port, use the **set spantree bpdu-guard** command.

set spantree bpdu-guard *mod/port* {**enable** | **disable** | **default**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables the spanning tree BPDU guard.
disable	Disables the spanning tree BPDU guard.
default	Sets spanning tree BPDU guard to the global BPDU guard state. See the "Usage Guidelines" section for more information.

Defaults

The default is BPDU guard is **default**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

You must enable PortFast mode before you can enable BPDU guard for BPDU guard to work correctly.

When you enable BPDU guard, a port is moved into an errdisable state when a BPDU is received on that port. When you disable a BPDU guard, a PortFast-enabled nontrunking port will stay up when it receives BPDUs, which may cause spanning tree loops.

If you enter the **default** keyword, the spanning tree port is set to the global BPDU guard state.

To enable or disable BPDU guard for all ports on the switch, enter the **set spantree global-default bpdu-guard** command.

Examples

This example shows how to enable BPDU guard on module 3, port 1:

```
Console> (enable) set spantree bpdu-guard 3/1 enable
Spantree port 3/1 bpdu guard enabled.
Console> (enable)
```

Related Commands

set spantree global-default
show spantree portfast

set spantree bpdu-skewing

To enable or disable collection of the spanning tree BPDU skewing detection statistics, use the **set spantree bpdu-skewing** command.

set spantree bpdu-skewing {**enable** | **disable**}

Syntax Description

enable	Enables BPDU skewing detection statistics collection.
disable	Disables BPDU skewing detection statistics collection.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

You can use this command to troubleshoot slow network convergence due to skewing. Skewing occurs when spanning tree timers lapse, expected BPDUs are not received, and spanning tree detects topology changes. The difference between the expected result and the BPDUs actually received is a "skew." The skew causes BPDUs to reflood the network to keep the spanning tree topology database up to date.

Examples

This example shows how to enable the BPDU skew detection feature:

```
Console> (enable) set spantree bpdu-skewing enable
Spantree bpdu-skewing enabled on this switch.
Console> (enable)
```

This example shows how to disable the BPDU skew detection feature:

```
Console> (enable) set spantree bpdu-skewing disable
Spantree bpdu-skewing disabled on this switch.
Console> (enable)
```

Related Commands

show spantree bpdu-skewing

set spantree channelcost

To set the channel path cost and to automatically adjust the channel port costs, use the **set spantree channelcost** command.

set spantree channelcost {*channel_id* | **all**} *cost*

Syntax Description

channel_id	Channel identification number.
all	Configures all channels.
cost	Channel port costs.

Defaults

The port cost is updated automatically based on the current port costs of the channeling ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can use this command when your switch is in Link Aggregation Control Protocol (LACP) channel mode or in PAgP channel mode.

For differences between PAgP and LACP, refer to the “Guidelines for Port Configuration” section of the “Configuring EtherChannel” chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example shows how to set the channel 768 path cost to 12.

```
Console> (enable) set spantree channelcost 768 12
Port(s) 1/1-2 port path cost are updated to 19.
Channel 768 cost is set to 12.
Warning: channel cost may not be applicable if channel is broken.
Console> (enable)
```

This example shows how to set all channel path costs to 15:

```
Console> (enable) set spantree channelcost all 15
Port(s) 1/1-2 port path cost are updated to 24.
Channel 768 cost is set to 15.
Port(s) 4/3-4 cost is set to 15.
channel 769 cost is set to 15.
Port(s) 4/7-8 cost is set to 15.
channel 770 cost is set to 15.
Warning: channel cost may not be applicable if channel is broken.
Console> (enable)
```

Related Commands

clear lacp-channel statistics
set channelprotocol
set lacp-channel system-priority
set port lacp-channel
set spantree channelvlancost
show lacp-channel
show port lacp-channel

set spantree channelvlancost

To set the channel VLAN path cost and adjust the port VLAN costs of the ports that belong to the channel, use the **set spantree channelvlancost** command.

set spantree channelvlancost *channel_id cost*

Syntax Description

channel_id	Number of the channel identification.
cost	Port costs of the ports in the channel.

Defaults

The command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must set the channel VLAN cost one channel at a time.

You can use this command when your system is in LACP channel mode or PAgP channel mode.

For differences between PAgP and LACP, refer to the “Guidelines for Port Configuration” section of the “Configuring EtherChannel” chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example shows how to set the VLAN cost to 10 for channel 768:

```
Console> (enable) set spantree channelvlancost 768 10
Port(s) 1/1-2 vlan cost are updated to 24.
Channel 768 vlancost is set to 10.
Console> (enable)
```

Related Commands

clear lacp-channel statistics
set channelprotocol
set lacp-channel system-priority
set port lacp-channel
set spantree channelcost
show lacp-channel
show port lacp-channel

set spantree defaultcostmode

To specify the spanning tree default port cost mode, use the **set spantree defaultcostmode** command.

set spantree defaultcostmode {**short** | **long**}

Syntax Description

short	Sets the default port cost for port speeds slower than 10 gigabits.
long	Sets the default port cost mode port speeds of 10 gigabits and faster.

Defaults

The default is short.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set spantree defaultcostmode long** command is available in PVST+ mode only. If you enter this command in MISTP or MISTP-PVST+ mode, this message is displayed:

```
In MISTP or MISTP-PVST+ mode, default portcost and portinstancecost always
use long format default values.
```

All switches in a network must have the same default. If any switch in the network supports port speeds of 10 gigabits and greater, the default cost mode must be set to **long** on all the switches in the network.

For port speeds of 1 gigabits and greater, the default port cost should be set to **long**. For port speeds less than 10 gigabits, the default port cost can be set to **short**.

The default path cost is based on port speed; see Table 2-25 and Table 2-26 for default settings.

Table 2-25 Default Port Cost—Short Mode

Port Speed	Default Port Cost
4 Mb	250
10 Mb	100
16 Mb	62
100 Mb	19
155 Mb	14
1 Gb	4
10 Gb	2

Table 2-26 Default Port Cost—Long Mode

Port Speed	Default Port Cost
100 Kb	200,000,000
1 Mb	20,000,000
10 Mb	2,000,000
100 Mb	200,000
1 Gb	20,000
10 Gb	2,000
100 Gb	200
1 Tb	20
10 Tb	2

Examples

This example shows how to set the spanning tree default port cost mode:

```
Console> (enable) set spantree defaultcostmode long
Portcost and portvlancost set to use long format default values.
Console> (enable)
```

Related Commands

show spantree defaultcostmode

set spantree disable

To disable the spanning tree algorithm for all VLANs or a specific VLAN or disable spanning tree instance, use the **set spantree disable** command.

set spantree disable *vlan*

set spantree disable all

set spantree disable mistp-instance *instance*

set spantree disable mistp-instance all

Syntax Description

vlan	Number of the VLAN; valid values are from 1 to 4094.
all	Specifies all VLANs.
mistp-instance *instance*	Specifies the instance number; valid values are from 1 to 16.
mistp-instance all	Deletes all instances.

Defaults

The default is spanning tree is enabled, and all instances are enabled (flooding disabled).

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

If you do not specify a VLAN number or an instance number, 1 is assumed.

When an instance is enabled, the Spanning Tree Protocol starts running on that instance.

When an instance is disabled, the switch stops sending out config type-length values (TLVs) for that instance and starts flooding incoming TLVs for the same instance (but checks the VLAN mapping on the incoming side). All the traffic running on the VLANs mapped to the instance is flooded as well.

This command is not available in MST mode.

Examples

This example shows how to disable the spanning tree for VLAN 1:

```
Console> (enable) set spantree disable 1
VLAN 1 bridge spanning tree disabled.
Console> (enable)
```

This example shows how to disable spanning tree for a specific instance:

```
Console> (enable) set spantree disable mistp-instance 2
MI-STP instance 2 disabled.
Console> (enable)
```

Related Commands

set spantree enable
show spantree

set spantree enable

To enable the spanning tree algorithm for all VLANs, a specific VLAN, a specific instance, or all instances, use the **set spantree enable** command.

set spantree enable *vlans*

set spantree enable all

set spantree enable mistp-instance *instance*

set spantree enable mistp-instance all

Syntax Description

vlans	Number of the VLAN; valid values are from 1 to 4094.
all	Specifies all VLANs.
mistp-instance *instance*	Specifies the instance number; valid values are from 1 to 16.
mistp-instance all	Enables all instances.

Defaults

The default is enabled, and all instances are enabled (flooding disabled).

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

MISTP and VTP pruning cannot be enabled at the same time.

If you do not specify a VLAN number or an instance number, 1 is assumed.

This command is not available in MST mode.

Examples

This example shows how to activate spanning tree for VLAN 1:

```
Console> (enable) set spantree enable 1
VLAN 1 bridge spanning tree enabled.
Console> (enable)
```

This example shows how to activate spanning tree for an instance:

```
Console> (enable) set spantree enable mistp-instance 1
-STP instance 1 enabled.
Console> (enable)
```

Related Commands

set spantree disable
show spantree

set spantree fwddelay

To set the bridge forward delay for a VLAN or an instance, use the **set spantree fwddelay** command.

set spantree fwddelay *delay* [*vlans*]

set spantree fwddelay *delay* **mistp-instance** [*instances*]

set spantree fwddelay *delay* **mst**

Syntax Description

delay	Number of seconds for the bridge forward delay; valid values are from 4 to 30 seconds.
vlans	(Optional) Number of the VLAN; valid values are from 1 to 4094.
mistp-instance *instances*	Specifies the instance number; valid values are from 1 to 16.
mst	Sets the forward delay time for the IST instance and all MST instances; see the “Usage Guidelines” section for more information.

Defaults

The default is the bridge forward delay is set to 15 seconds for all VLANs.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a VLAN number or an instance number, 1 is assumed.

This command is not supported by the NAM.

If you enable MISTP, you cannot set the VLAN bridge forward delay.

If you enable PVST+, you cannot set the instance bridge forward delay.

If you enter the **set spantree fwddelay** *delay* **mst** command, you set the forward delay time for the IST instance and all MST instances. You do not need to set the forward delay time for each MST instance.

Examples

This example shows how to set the bridge forward delay for VLAN 100 to 16 seconds:

```
Console> (enable) set spantree fwddelay 16 100
Spantree 100 forward delay set to 16 seconds.
Console> (enable)
```

This example shows how to set the bridge forward delay for an instance to 16 seconds:

```
Console> (enable) set spantree fwddelay 16 mistp-instance 1
Instance 1 forward delay set to 16 seconds.
Console> (enable)
```

This example shows how to set the bridge forward delay for the IST and all MST instances to 15 seconds:

```
Console> (enable) set spantree fwddelay 15 mst
MST forward delay set to 15 seconds.
Console> (enable)
```

Related Commands

show spantree

set spantree global-default

To set the global states on the switch, use the **set spantree global-default** command.

set spantree global-default portfast {**enable** | **disable**}

set spantree global-default loop-guard {**enable** | **disable**}

set spantree global-default bpdu-guard {**enable** | **disable**}

set spantree global-default bpdu-filter {**enable** | **disable**}

Syntax Description

portfast	Sets the global PortFast state.
enable	Enables the global state.
disable	Disables the global state.
loop-guard	Sets the global loop guard state.
bpdu-guard	Sets the global BPDU guard state.
bpdu-filter	Sets the global BPDU filter state.

Defaults

All ports are in nonedge state.

Loop guard is disabled on all ports.

BPDU guard is disabled on all ports.

BPDU filter is disabled on all ports.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to disable the global PortFast state on the switch:

```
Console> (enable) set spantree global-default portfast disable
Spantree global portfast state disabled on this switch.
Console> (enable)
```

This example shows how to enable the global loop guard state on the switch:

```
Console> (enable) set spantree global-default loop-guard enable
Spantree global loop-guard state enabled on the switch.
Console> (enable)
```

This example shows how to disable the global BPDU guard state on the switch:

```
Console> (enable) set spantree global-default bpdu-guard disable
Spantree global-default bpdu-guard disabled on this switch.
Console> (enable)
```

This example shows how to disable the global BPDU filter state on the switch:

```
Console> (enable) set spantree global-default bpdu-filter disable
Spantree global-default bpdu-filter disabled on this switch.
Console> (enable)
```

Related Commands

clear spantree mst
set spantree mst config
set spantree portfast bpdu-filter
set spantree portfast bpdu-guard
show spantree mst config

set spantree guard

To enable or disable the spanning tree root guard or loop guard feature on a per-port basis, use the **set spantree guard** command.

set spantree guard {**none** | **root** | **loop**} *mod/port*

Syntax Description

none	Disables the spanning tree guard feature.
root	Enables the root guard feature.
loop	Enables the loop guard feature.
mod/port	Number of the module and ports on the module.

Defaults

The default is root guard and loop guard are disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enable loop guard on a channel and the first link becomes unidirectional, loop guard will block the entire channel until the affected port is removed from the channel.

You can use the root guard feature to prevent switches from becoming the root switch. The root guard feature forces a port to become a designated port so that no switch on the other end of the link can become a root switch.

When you enable root guard, it is automatically applied to all of the active instances or VLANs to which that port belongs. When you disable root guard, it is disabled for the specified ports. If a port goes into the root-inconsistent state, it automatically goes into the listening state. Disabling loop guard moves all loop-inconsistent ports to the listening state.

When using the loop guard feature, follow these guidelines:

- Use care when enabling loop guard. Loop guard is useful only in those topologies where there are blocked ports. Topologies where there are no blocked ports are loop free by definition and do not need this feature to be enabled.
- Enable loop guard only on root and alternate root ports.
- Use loop guard mainly on access switches.
- You cannot enable loop guard on PortFast-enabled or dynamic VLAN ports.
- You cannot enable PortFast on loop guard-enabled ports.
- You cannot enable loop guard if root guard is enabled.

Examples

This example shows how to enable root guard:

```
Console> (enable) set spantree guard root 5/1
Rootguard on port 5/1 is enabled.
Warning!! Enabling rootguard may result in a topolopy change.
Console> (enable)
```

This example shows how to enable the loop guard feature:

```
Console> (enable) set spantree guard loop 5/1
Rootguard is enabled on port 5/1, enabling loopguard will disable rootguard on
 this port.
Do you want to continue (y/n) [n]? y
Loopguard on port 5/1 is enabled.
Console> (enable)
```

Related Commands

show spantree guard

set spantree hello

To set the bridge hello time for a VLAN or an instance, use the **set spantree hello** command.

set spantree hello *interval* [*vlans*]

set spantree hello *interval* **mistp-instance** *instances*

set spantree hello *interval* **mst**

Syntax Description

interval	Number of seconds the system waits before sending a bridge hello message (a multicast message indicating that the system is active); valid values are from 1 to 10 seconds.
vlans	(Optional) Number of the VLAN; valid values are from 1 to 4094.
mistp-instance *instances*	Specifies the instance number; valid values are from 1 to 16.
mst	Sets the hello time for the IST instance and all MST instances. See the "Usage Guidelines" section for more information.

Defaults

The bridge hello time is set to 2 seconds for all VLANs.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a VLAN number or an instance number, 1 is assumed.

This command is not supported by the NAM.

If you enable MISTP, you cannot set the VLAN hello time.

If you enable PVST+, you cannot set the instance hello time.

If you enter the **set spantree hello** *interval* **mst** command, you set the hello time for the Internal Spanning Tree (IST) instance and all MST instances. You do not need to set the hello time for each MST instance.

If you do not configure a hello time on a per-port basis, the global hello time is used on the port.

Examples

This example shows how to set the spantree hello time for VLAN 100 to 3 seconds:

```
Console> (enable) set spantree hello 3 100
Spantree 100 hello time set to 3 seconds.
Console> (enable)
```

This example shows how to set the spantree hello time for an instance to 3 seconds:

```
Console> (enable) set spantree hello 3 mistp-instance 1
Spantree 1 hello time set to 3 seconds.
Console> (enable)
```

This example shows how to set the spantree hello time for the IST and all MST instances to 2 seconds:

```
Console> (enable) set spantree hello 2 mst
MST hello time set to 2 seconds.
Console> (enable)
```

Related Commands

show spantree

set spantree link-type

To configure the link type of a port, use the **set spantree link-type** command.

set spantree link-type *mod/port* {**auto** | **point-to-point** | **shared**}

Syntax Description

mod/port	Number of the module and the port on the module.
auto	Derives the link from either a half-duplex or full-duplex link type. See "Usage Guidelines" for more information.
point-to-point	Connects the port to a point-to-point link.
shared	Connects the port to a shared medium.

Defaults

The link type is **auto**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If the link type is set to **auto** and the link is a half-duplex link, then the link is a shared link. If the link type is set to **auto** and the link is a full-duplex link, then the link is a point-to-point link.

The **set spantree link-type** command is the same as the **set spantree mst link-type** command.

Examples

This example shows how to connect port 1 on module 3 to a point-to-point link:

```
Console> (enable) set spantree link-type 3/1 point-to-point
Link type set to point-to-point on port 3/1
Console> (enable)
```

Related Commands

set spantree global-default
show spantree

set spantree macreduction

To enable or disable the spanning tree MAC address reduction feature, use the **set spantree macreduction** command.

set spantree macreduction enable | disable

Syntax Description

enable	Enables MAC address reduction.
disable	Disables MAC address reduction.

Defaults

The default is MAC address reduction is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The MAC address reduction feature is used to enable extended-range VLAN identification and allows the switch to support a large number of spanning tree instances with a very limited number of MAC addresses and still maintain the IEEE 802.1D bridge-ID requirement for each STP instance.

You cannot disable this feature if extended-range VLANs exist.

You cannot disable this feature on chassis with 64 MAC addresses.

Examples

This example shows how to disable the MAC address reduction feature:

```
Console> (enable) set spantree macreduction disable
MAC address reduction disabled
Console> (enable)
```

Related Commands

show spantree

set spantree maxage

To set the bridge maximum aging time for a VLAN or an instance, use the **set spantree maxage** command.

set spantree maxage *agingtime* [*vlans*]

set spantree maxage *agingtime* **mistp-instance** *instances*

set spantree maxage *agingtime* **mst**

Syntax Description

agingtime	Maximum number of seconds that the system retains the information received from other bridges through Spanning Tree Protocol; valid values are from 6 to 40 seconds.
vlans	(Optional) Number of the VLAN; valid values 1 to 4094.
mistp-instance *instances*	Specifies the instance number; valid values are from 1 to 16.
mst	Sets the maximum aging time for the IST instance and all MST instances. See the "Usage Guidelines" section for more information.

Defaults

The default configuration is 20 seconds for all VLANs.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a VLAN number or an instance number, 1 is assumed.

This command is not supported by the NAM.

If you enable MISTP, you cannot set the VLAN maximum aging time.

If you enable PVST+, you cannot set the instance maximum aging time.

If you enter the **set spantree maxage** *agingtime* **mst** command, you set the maximum aging time for the IST instance and all MST instances. You do not need to set the maximum aging time for each MST instance.

Examples

This example shows how to set the maximum aging time for VLAN 1000 to 25 seconds:

```
Console> (enable) set spantree maxage 25 1000
Spantree 1000 max aging time set to 25 seconds.
Console> (enable)
```

This example shows how to set the maximum aging time for an instance to 25 seconds:

```
Console> (enable) set spantree maxage 25 mistp-instance 1
Instance 1 max aging time set to 25 seconds.
Console> (enable)
```

This example shows how to set the maximum aging time for the IST and all MST instances to 20 seconds:

```
Console> (enable) set spantree maxage 20 mst
MST max age set to 20 seconds.
Console> (enable)
```

Related Commands

show spantree

set spantree mode

To configure the type of Spanning Tree Protocol mode to run, use the **set spantree mode** command.

set spantree mode {**mistp** | **pvst+** | **mistp-pvst+** | **mst** | **rapid-pvst+**}

Syntax Description

mistp	Specifies MISTP mode.
pvst+	Specifies PVST+ mode.
mistp-pvst+	Allows the switch running MISTP to tunnel BPDUs with remote switches running PVST+.
mst	Specifies MST mode.
rapid-pvst+	Specifies per VLAN Rapid Spanning Tree (IEEE 802.1w).

Defaults

The default is **rapid-pvst+**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

When you connect through Telnet into a switch and try to change the spanning tree mode from PVST+ to MISTP or MISTP-PVST+, and no VLANs are mapped to any instance on that switch, this warning message is displayed:

```
Console> (enable) set spantree mode mistp
Warning!! Changing the STP mode from a telnet session will disconnect the
session because there are no VLANs mapped to any MISTP instance.
Do you want to continue [n]?
```

When you connect through Telnet into a switch and try to change the spanning tree mode from MISTP or MISTP-PVST+ to PVST+, or when you connect through Telnet into a switch and try to change the spanning tree mode from PVST+ to MISTP or MISTP-PVST+ and additional VLAN-instance mappings are on that switch, this warning message is displayed:

```
Console> (enable) set spantree mode pvst+
Warning!! Changing the STP mode from a telnet session might disconnect the
session.
Do you want to continue [n]?
```

When you change from MISTP to Rapid PVST+ and over 8000 VLAN ports are currently configured on the switch, this warning message is displayed:

```
Console> (enable) set spantree mode rapid-pvst+
Warning!! This switch has 12345 VLAN-ports currently configured for STP.
Going out of MISTP mode could impact system performance.
Do you want to continue [n]?
```

If you change the spanning tree mode from PVST+ to MISTP or MISTP to PVST+, the STP mode previously running stops, all the information collected at runtime is used to build the port database for the new mode, and the new STP mode restarts the computation of the active topology from zero. All the parameters of the previous STP per VLAN or per instance are kept in NVRAM.

If you change the spanning tree mode from PVST+ to MISTP or MISTP to PVST+ and BackboneFast is enabled, this message is displayed:

```
Console> (enable) set spantree mode mistp
Cannot change the spantree mode to MISTP when backbonefast is enabled.
```

Examples

This example shows how to set the spanning tree mode to PVST+:

```
Console> (enable) set spantree mode pvst+
Warning!! Changing the STP mode from a telnet session might disconnect the session.
Do you want to continue [n]? y
Spantree mode set to PVST+.
Console> (enable)
```

This example shows what happens if you change the spanning tree mode from PVST+ to MISTP:

```
Console> (enable) set spantree mode mistp
Warning!! Changing the STP mode from a telnet session will disconnect the session because
there are no VLANs mapped to any MISTP instance.
Do you want to continue [n]? y
Console> (enable)
```

This example shows how to set the spanning tree mode to MST:

```
Console> (enable) set spantree mode mst
Warning!! Changing the STP mode from a telnet session will disconnect the sessi
n because there are no VLANs mapped to any MISTP instance.
Do you want to continue [n]? y
Console> (enable)
```

This example shows how to set the spanning tree mode to rapid PVST+:

```
Console> (enable) set spantree mode rapid-pvst+
Warning!! Changing the STP mode from a telnet session might disconnect the session.
Do you want to continue [n]? y
Console> (enable)
```

Related Commands

set vlan
show spantree

set spantree mst

To configure the mapping of VLANs to an MST instance or to configure ports that are connected to neighbors that are in pre-standard MST mode, use the **set spantree mst** command.

set spantree mst *instance* **vlan** *vlan*

set spantree mst {*mod/port*} {**pre-std** | **auto**}

Syntax Description

instance	Number of the instance; valid values are from 0 to 4094. See the "Usage Guidelines" section for more information.
vlan *vlan*	Specifies the VLAN number; valid values are from 1 to 4094.
mod/port	Number of the module and the port on the module.
pre-std	Configures a port that is connected to a switch running pre-standard MST. See the "Usage Guidelines" section for more information.
auto	Reverts a port that is in pre-standard MST mode back to standard MST mode (IEEE Std 802.1s). See the "Usage Guidelines" section for more information.

Defaults

Ports are set to **auto**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

All changes made to the region configuration (region information and VLAN mapping) are buffered. Only one user can hold the buffer at a time. This buffer is locked when you first use the **set spantree mst instance** or **set spantree mst config** commands.

If the VLAN is already mapped to some other instance, the VLAN is unmapped from that instance and mapped to the new instance.

Each time you map a new VLAN or VLANs, they are added to the existing mapping.

All unmapped VLANs are automatically mapped to MST instance 0 (IST).

You can configure up to 64 instances, including the mandatory instance 0. If 64 instances have already been configured, you cannot create an additional instance by mapping more VLANs to it.

If a port is connected to a neighbor that is running pre-standard MST, you can configure the port to operate in pre-standard MST mode by entering the **set spantree mst** *mod/port* **pre-std** command.

Pre-standard MST is the implementation of MST that is not compliant with with IEEE Std 802.1s. MST implementation is pre-standard on Catalyst 6500 series switches that are running software before release 8.3(1) . MST implementation is pre-standard on Catalyst 6500 series switches that are running any Cisco IOS software release.

Entering the **set spantree mst** *mod/port* **auto** commands reverts a port that is in pre-standard MST mode back to standard MST mode. In standard MST mode, a port on a neighbor that is in pre-standard MST mode might become a boundary port, even though both switches have the same MST configuration.

The **clear spantree mst** *mod/port* **pre-std** command also reverts a port back to standard MST mode.

Examples

This example shows how to map VLAN 1 to an MST instance 2:

```
Console> (enable) set spantree mst 2 vlan 1
Console> (enable)
```

This example shows how to set a port to pre-standard MST mode:

```
Console> (enable) set spantree mst 4/47 pre-std
Port configured to pre-mst port 4/47.
Console> (enable)
```

Related Commands

clear spantree mst
set spantree mst config

set spantree mst config

To change the MST region information, use the **set spantree mst config** command.

set spantree mst config [**name** *name*] [**revision** *number*]

set spantree mst config commit

set spantree mst config rollback [**force**]

Syntax Description

name *name*	(Optional) Specifies the MST region name. See the "Usage Guidelines" section for more information.
revision *number*	(Optional) Specifies the MST region revision number; *number* is from 0 to 65535. See the "Usage Guidelines" section for more information.
commit	Puts the new MST VLAN mapping into effect.
rollback	Discards changes made to the MST configuration that have not been applied yet.
force	(Optional) Unlocks the MST edit buffer when it is held by another user.

Defaults

Unless you specify a region name, no region name will be given.

The default revision number is 0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The region name can be up to 32 characters long.

The region name and revision number are copied from NVRAM MST region information. You must enter the revision number if the revision number needs to be updated. The revision number is not incremented automatically each time that the MST configuration is committed.

Changes that you make to MST VLAN mapping are buffered, and by entering the **set spantree mst config commit** command, you put the new MST VLAN mapping into effect. After you enter the **set spantree mst config commit** command, the lock for the MST edit buffer is released.

If you enter the **set spantree mst config rollback** command, you discard the changes made to the MST region configuration that are not applied yet (only if you have locked the edit buffer). You can forcefully release the lock set by another user by entering the command **set spantreee mst config rollback force**.

The **set spantree mst config commit** and **set spantree mst config rollback** commands are stored in NVRAM.

Examples

This example shows how to configure an MST region and to give that region a name and revision number:

```
Console> (enable) set spantree mst config name test-lab revision 10
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes
Console> (enable)
```

This example shows how to put the new MST VLAN mapping into effect:

```
Console> (enable) set spantree mst config commit
Console> (enable)
```

This example shows how to discard MST region configuration when you hold the MST edit buffer:

```
Console> (enable) set spantree mst config rollback
Console> (enable)
```

This example shows how to unlock the MST edit buffer when it is held by another user:

```
Console> (enable) set spantree mst config rollback force
Console> (enable)
```

This example shows the message that displays on the console if the switch is either a non-primary server or a client for the MST feature:

```
Console> (enable) set spantree mst config commit
MST configuration cannot be changed on a non primary server
Console> (enable)
```

Related Commands

clear spantree mst
show spantree mst
show spantree mst config

set spantree mst link-type

To configure the link type of a port, use the **set spantree mst link-type** command.

set spantree mst link-type *mod/port* {**auto** | **point-to-point** | **shared**}

Syntax Description

mod/port	Number of the module and the port on the module.
auto	Derives the link from either a half-duplex or full-duplex link type. See the “Usage Guidelines” section for more information about **auto**.
point-to-point	Connects the port to a point-to-point link.
shared	Connects the port to a shared medium.

Defaults

The default link type is **auto**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

MST rapid connectivity only works on point-to-point links between two bridges.

If the link type is set to **auto** and the link is a half-duplex link, then the link is a shared link. If the link type is set to **auto** and the link is a full-duplex link, then the link is a point-to-point link.

Examples

This example shows how to connect port 1 on module 3 to a point-to-point link:

```
Console> (enable) set spantree mst link-type 3/1 point-to-point
Link type set to point-to-point on port 3/1
Console> (enable)
```

Related Commands

clear spantree mst
set spantree global-default
set spantree mst config

set spantree mst maxhops

To set the spanning tree hop count, use the **set spantree mst maxhops** command.

set spantree mst maxhops *maxhops*

Syntax Description

maxhops	Maximum number of hops. Valid values are 1 to 40.

Defaults

The bridge forward delay default is 20 seconds for all instances.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the maximum number of hops:

```
Console> (enable) set spantree mst maxhops 20
Console> (enable)
```

Related Commands

clear spantree mst
set spantree mst config
set spantree mst link-type
set spantree mst vlan
show spantree mst
show spantree mst config

8.6 EFT Copy

set spantree mst vlan

To configure the mapping of VLANs to an MST instance, use the **set spantree mst vlan** command.

set spantree mst *instance* **vlan** *vlan*

Syntax Description

instance	Number of the instance; valid values are from 0 to 15.
vlan *vlan*	Specifies the VLAN number; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

All changes made to the region configuration (region information and VLAN mapping) are buffered. Only one user can hold the buffer at a time. This buffer is locked when you first enter the **set spantree mst** *instance* or **set spantree mst config** commands.

If the VLAN is already mapped to some other instance, the VLAN is unmapped from that instance and mapped to the new instance.

Each time you map a new VLAN or VLANs, they are added to the existing mapping.

All unmapped VLANs are mapped to MST instance 0 (IST).

Examples

This example shows how to map VLANs 400 through 499 to MST instance 4:

```
Console> (enable) set spantree mst 4 vlan 400-499
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes
Console> (enable)
```

Related Commands

clear spantree mst
set spantree mst config
show spantree mst
show spantree mst config

set spantree portcost

To set the path cost for a port, use the **set spantree portcost** command.

set spantree portcost *mod/port cost* [**mst**]

Syntax Description

mod/port	Number of the module and the port on the module.
cost	Number of the path cost; see the "Usage Guidelines" section for additional information.
mst	(Optional) Sets the path cost for an MST port.

Defaults

The default path cost is based on port speed; see Table 2-27 and Table 2-28 for default settings.

Table 2-27 Default Port Cost—Short Mode

Port Speed	Default Port Cost
4 Mb	250
10 Mb	100
16 Mb	62
100 Mb	19
155 Mb	14
1 Gb	4
10 Gb	2

Table 2-28 Default Port Cost—Long Mode

Port Speed	Default Port Cost
100 Kb	200000000 (200 million)
1 Mb	20000000 (20 million)
10 Mb	2000000 (2 million)
10 Mb	200000 (200 thousand)
1 Gb	20000 (20 thousand)
10 Gb	2000 (2 thousand)
100 Gb	200
1 Tb	20
10 Tb	2

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If the spanning tree mode is short and long or MISTP, valid cost values are from 1 to 65535; otherwise, valid cost values are from 1 to 2000000.

This command is not supported by the NAM.

The Spanning Tree Protocol uses port path costs to determine which port to select as a forwarding port. You should assign lower numbers to ports attached to faster media (such as full duplex) and higher numbers to ports attached to slower media.

Examples

This example shows how to set the port cost for port 12 on module 2 to 19:

```
Console> (enable) set spantree portcost 2/12 19
Spantree port 2/12 path cost set to 19.
Console> (enable)
```

Related Commands

set spantree defaultcostmode
show spantree

set spantree portfast

To allow a port that is connected to a single workstation or PC to start faster when it is connected, use the **set spantree portfast** command.

set spantree portfast *mod/port* {**enable** [**trunk**] | **disable** | **default**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables the spanning tree PortFast-start feature on the port.
trunk	(Optional) Enables the spanning tree PortFast-start feature on the trunk port.
disable	Disables the spanning tree PortFast-start feature on the port.
default	Sets the spanning tree PortFast-start feature back to its default setting.

Defaults

The default is the PortFast-start feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

When a port configured with the **spantree portfast enable** command is connected, the port immediately enters the spanning tree forwarding state rather than going through the normal spanning tree states, such as listening and learning.

If you enter the **trunk** keyword, the spanning tree PortFast-start feature is enabled on the specified trunk port.

Examples

This example shows how to enable the spanning tree PortFast-start feature on port 2 on module 1:

```
Console> (enable) set spantree portfast 1/2 enable
Warning: Connecting layer 2 devices to a fast-start port can cause temporary spanning tree
loops. Use with caution.
Spantree port 1/2 fast start enabled.
Console> (enable)
```

This example shows how to enable the spanning tree PortFast-start feature on the trunk port:

```
Console> (enable) set spantree portfast 3/2 enable trunk
Warning: Connecting layer 2 devices to a fast-start port can cause temporary spanning tree
loops. Use with caution.
Spantree port 1/2 fast start enabled.
Console> (enable)
```

Related Commands

show spantree portfast

set spantree portfast bpdu-filter

To enable or disable spanning tree PortFast BPDU packet filtering on a port, use the **set spantree portfast bpdu-filter** command.

set spantree portfast bpdu-filter *mod/port* {**enable** | **disable** | **default**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables spanning tree PortFast BPDU packet filtering.
disable	Disables spanning tree PortFast BPDU packet filtering.
default	Sets spanning tree PortFast BPDU packet filtering to the global BPDU packet filtering state. See the "Usage Guidelines" section for more information.

Defaults

The default is BPDU packet filtering is **default**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Spanning tree PortFast BPDU packet filtering turns off BPDU transmission on PortFast-enabled ports and nontrunking ports.

If you enter the **default** keyword, the spanning tree port is set to the global BPDU filtering state.

To enable or disable spanning tree PortFast BPDU filtering for all ports on the switch, enter the **set spantree global-default bpdu-filter** command.

Examples

This example shows how to enable spanning tree PortFast BPDU filtering on module 3, port 4:

```
Console> (enable) set spantree portfast bpdu-filter 3/4 enable
Warning: Ports enabled with bpdu filter will not send BPDUs and drop all
received BPDUs. You may cause loops in the bridged network if you misuse
this feature.
Spantree port 3/4 bpdu filter enabled.
Console> (enable)
```

Related Commands

set spantree global-default
show spantree portfast

set spantree portfast bpdu-guard

To enable or disable spanning tree PortFast BPDU guard on a port, use the **set spantree portfast bpdu-guard** command.

set spantree portfast bpdu-guard *mod/port* {**enable** | **disable** | **default**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Enables the spanning tree PortFast BPDU guard.
disable	Disables the spanning tree PortFast BPDU guard.
default	Sets spanning tree PortFast BPDU guard to the global BPDU guard state. See the "Usage Guidelines" section for more information.

Defaults

The default is PortFast BPDU guard is **default**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

You must enable spanning tree PortFast mode before you can enable spanning tree PortFast BPDU guard for BPDU guard to work correctly.

When you enable spanning tree PortFast BPDU guard, a nontrunking PortFast-enabled port is moved into an errdisable state when a BPDU is received on that port. When you disable spanning tree PortFast BPDU guard, a PortFast-enabled nontrunking port will stay up when it receives BPDUs, which may cause spanning tree loops.

If you enter the **default** keyword, the spanning tree port is set to the global BPDU guard state.

To enable or disable BPDU guard for all ports on the switch, enter the **set spantree global-default bpdu-guard** command.

Examples

This example shows how to enable spanning tree BPDU guard on module 3, port 1:

```
Console> (enable) set spantree portfast bpdu-guard 3/1 enable
Spantree port 3/1 bpdu guard enabled.
Console> (enable)
```

Related Commands

set spantree global-default
show spantree portfast

set spantree portinstancecost

To assign the path cost of the port for the specified instances, use the **set spantree portinstancecost** command.

set spantree portinstancecost *mod/port* [**cost** *cost*] [*instances*]

set spantree portinstancecost *mod/port* [**cost** *cost*] **mst** [*instances*]

Syntax Description

mod/port	Number of the module and the port on the module.
cost *cost*	(Optional) Indicates the path cost; see the "Usage Guidelines" section for additional information.
mst	Sets the cost for an MST instance.
instances	(Optional) Instance number; valid values are from 0 to 15.

Defaults

The default path cost is based on port speed; see Table 2-29 for default settings.

Table 2-29 Default Port Cost—Short Mode

Port Speed	Default Port Cost
4 Mb	250
10 Mb	100
16 Mb	62
100 Mb	19
155 Mb	14
1 Gb	4
10 Gb	2

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

If the spanning tree mode is short and long or MISTP, valid cost values are from 1 to 65535; otherwise, valid cost values are from 1 to 2,000,000.

The port instance cost applies to trunk ports only.

The value specified is used as the path cost of the port for the specified instances. The rest of the instances have a path cost equal to the port path cost set through the **set spantree instancecost** command. (If not set, the value is the default path cost of the port.)

Examples

These examples show how to use the **set spantree portinstancecost** command and explicitly specify the path cost of a port:

```
Console> (enable) set spantree portinstancecost 2/10 cost 6 1-10
Port 2/10 instances 11-16 have path cost 2000000.
Port 2/10 instances 1-10 have path cost 6.
This parameter applies to trunking ports only.
Console> (enable)
```

These examples show how to use the **set spantree portinstancecost** command without explicitly specifying the path cost of a port:

```
Console> (enable) set spantree portinstancecost 1/2
Port 1/2 Instances 1-1005 have path cost 3100.
Console> (enable)

Console> (enable) set spantree portinstancecost 1/2 16
Port 1/2 Instances 16,22-1005 have path cost 3100.
Console> (enable)
```

This example shows the display if you enter the command when PVST+ is enabled:

```
Console> (enable) set spantree portinstancecost 3/1
This command is only valid when STP is in MISTP or MISTP-PVST+ mode.
Console> (enable)
```

This example shows how to set the port cost for a specific MST instance:

```
Console> (enable) set spantree portinstancecost 2/10 cost 6 1-10 mst
Port 2/10 mst instances 1-10 have path cost 6.
This parameter applies to trunking ports only.
Console> (enable)
```

Related Commands

clear spantree portinstancecost
show spantree mistp-instance

set spantree portinstancepri

To set the port priority for instances in the trunk port, use the **set spantree portinstancepri** command.

set spantree portinstancepri *mod/port priority* [*instances*]

set spantree portinstancepri *mod/port priority* **mst** [*instances*]

Syntax Description

mod/port	Number of the module and the port on the module.
priority	Number that represents the cost of a link in a spanning tree bridge; valid values are **0**, **16**, **32**, **48**, **64**, **80**, **96**, **112**, **128**, **144**,**160**, **176**, **192**, **208**, **224**, **240**, with 0 indicating high priority and 240, low priority. See the "Usage Guidelines" section for more information.
mst	Specifies the port priority for MST instances.
instances	(Optional) Instance number; valid values are from 0 to 15.

Defaults

The default is the port priority is set to 0, with no instances specified.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Priority values that are not a multiple of 16 (between the values of 0 to 63) are converted to the nearest multiple of 16.

This command is not supported by the NAM.

Use this command to add instances to a specified port priority level. Subsequent calls to this command do not replace instances that are already set at a specified port priority level.

This feature is not supported for the MSM.

The **set spantree portinstancepri** command applies to trunk ports only. If you enter this command, you see this message:

```
Port xx is not a trunk-capable port
```

Examples

This example shows how to set the port priority for module 1, port 2, on specific instances:

```
Console> (enable) set spantree portinstancepri 1/2 16 1-11
Port 1/2 instances 1-11 using portpri 16.
This parameter applies to trunking ports only.
Console> (enable)
```

This example shows how to set the port priority for module 8, port 1, on MST instance 2:

```
Console> (enable) set spantree portinstancepri 8/1 31 mst 2
Port 8/1 instances 2 using portpri 31.
Port 8/1 instances 0-1, 3-15 using portpri 32.
Console> (enable)
```

Related Commands

clear spantree portinstancecost
show spantree mistp-instance

8.6 EFT Copy

set spantree portpri

To set the bridge priority for a spanning tree port, use the **set spantree portpri** command.

set spantree portpri *mod/port priority* [**mst**]

Syntax Description

mod/port	Number of the module and the port on the module.
priority	Number that represents the cost of a link in a spanning tree bridge; valid values are **0**, **16**, **32**, **48**, **64**, **80**, **96**, **112**, **128**, **144**,**160**, **176**, **192**, **208**, **224**, **240**, with **0** indicating high priority and **240**, low priority. See the “Usage Guidelines” section for more information.
mst	(Optional) Sets the bridge priority for an MST port.

Defaults

The default is all ports with bridge priority are set to 32.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A priority value that is not a multiple of 16 (between the values of 0 to 63) is converted to the nearest multiple of 16.

This command is not supported by the NAM.

Examples

This example shows how to set the priority of port 1 on module 4 to 63:

```
Console> (enable) set spantree portpri 2/3 48
Bridge port  2/3 port priority set to 48.
Console> (enable)
```

This example shows the output when you have specified a priority value that is not a multiple of 16:

```
Console> (enable) set spantree portpri 2/3 2
Vlan port priority must be one of these numbers:0, 16, 32, 48, 64, 80,
96, 112, 128, 144,
160, 176, 192, 208, 224, 240
converting 2 to 0 nearest multiple of 16
Bridge port  2/3 port priority set to 0.
Console> (enable)
```

Related Commands

show spantree

set spantree portvlancost

To assign a lower path cost to a set of VLANs on a port, use the **set spantree portvlancost** command.

set spantree portvlancost *mod/port* [**cost** *cost*] [*vlan_list*]

Syntax Description

mod/port	Number of the module and the port on the module.
cost *cost*	(Optional) Sets the path cost; valid values are from 1 to 65535.
vlan_list	(Optional) Number of the VLAN; valid values are from 1 to 4094.

Defaults

The default path cost is based on port speed; see Table 2-30 and Table 2-31 for default settings.

Table 2-30 Default Port Cost—Short Mode

Port Speed	Default Port Cost
4 Mb	250
10 Mb	100
16 Mb	62
100 Mb	19
155 Mb	14
1 Gb	4
10 Gb	2

Table 2-31 Default Port Cost—Long Mode

Port Speed	Default Port Cost
100 Kb	200,000,000
1 Mb	20,000,000
10 Mb	2,000,000
10 Mb	200,000
1 Gb	20,000
10 Gb	2,000
100 Gb	200
1 Tb	20
10 Tb	2

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Follow these guidelines when you set the path cost for VLANs on a port:

- The *cost* value specified is used as the path cost of the port for the specified set of VLANs. The rest of the VLANs have a path cost equal to the port path cost set through the **set spantree portcost** command. If not set, the value is the default path cost of the port.
- You must supply a *vlan_list* argument when you first set the cost value. When you subsequently set a new *cost* value, all *cost* values previously set by entering this command are changed to the new *cost* value. If you have never explicitly set a *cost* value for a VLAN by entering this command, the *cost* value for the VLAN does not change.
- If you do not explicitly specify a cost value but cost values were specified previously, the port VLAN cost is set to 1 less than the current port cost for a port. However, this reduction might not assure load balancing in all cases.
- When setting the path cost for extended-range VLANs, you can create a maximum of 64 nondefault entries or create entries until NVRAM is full.

This command is not supported by the NAM.

This command is not supported in MISTP mode.

Examples

These examples show how to use the **set spantree portvlancost** command and explicitly specify the path cost of a port:

```
Console> (enable) set spantree portvlancost 2/10 cost 25 1-20
Cannot set portvlancost to a higher value than the port cost, 10, for port 2/10.
Console> (enable)

Console> (enable) set spantree portvlancost 2/10 cost 1-20
Port 2/10 VLANs 1-20 have a path cost of 9.
Console> (enable)

Console> (enable) set spantree portvlancost 2/10 cost 4 1-20
Port 2/10 VLANs 1-20 have path cost 4.
Port 2/10 VLANs 21-1000 have path cost 10.
Console> (enable)

Console> (enable) set spantree portvlancost 2/10 cost 6 21
Port 2/10 VLANs 1-21 have path cost 6.
Port 2/10 VLANs 22-1000 have path cost 10.
Console> (enable)
```

These examples show how to use the **set spantree portvlancost** command without explicitly specifying the path cost of a port:

```
Console> (enable) set spantree portvlancost 1/2
Port 1/2 VLANs 1-1005 have path cost 3100.
Console> (enable)

Console> (enable) set spantree portvlancost 1/2 21
Port 1/2 VLANs 1-20,22-1005 have path cost 3100.
Port 1/2 VLANs 21 have path cost 3099.
Console> (enable)
```

Related Commands

clear spantree portvlancost
set channel vlancost
show spantree

set spantree portvlanpri

To set the port priority for a subset of VLANs in the trunk port, use the **set spantree portvlanpri** command.

set spantree portvlanpri *mod/port priority* [*vlans*]

Syntax Description

mod/port	Number of the module and the port on the module.
priority	Number that represents the cost of a link in a spanning tree bridge; valid values are **0**, **16**, **32**, **48**, **64**, **80**, **96**, **112**, **128**, **144**,**160**, **176**, **192**, **208**, **224**, **240**, with 0 indicating high priority and 240, low priority. See the "Usage Guidelines" section for more information.
vlans	(Optional) VLANs that use the specified priority level; valid values are from 1 to 1005.

Defaults

The default is the port VLAN priority is set to 0, with no VLANs specified.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The priority value that is not a multiple of 16 (between the values of 0 to 63) is converted to the nearest multiple of 16.

This command is not supported by the NAM.

This command is not supported by extended-range VLANs.

Use this command to add VLANs to a specified port priority level. Subsequent calls to this command do not replace VLANs that are already set at a specified port priority level.

This feature is not supported for the MSM.

The **set spantree portvlanpri** command applies only to trunk ports. If you enter this command, you see this message:

```
Port xx is not a trunk-capable port
```

Examples

This example shows how to set the port priority for module 1, port 2, on VLANs 21 to 40:

```
Console> (enable) set spantree portvlanpri 1/2 16 21-40
Port 1/2 vlans 3,6-20,41-1000 using portpri 32
Port 1/2 vlans 1-2,4-5,21-40 using portpri 16
Console> (enable)
```

Related Commands

clear spantree portvlanpri
show spantree

set spantree priority

To set the bridge priority for a VLAN or an instance when PVST+ or MISTP is running, use the **set spantree priority** command.

set spantree priority *bridge_priority vlans*

set spantree priority *bridge_priority* **mistp-instance** *instances*

set spantree priority *bridge_priority* **mst** *instances*

Syntax Description

bridge_priority	Number representing the priority of the bridge; see the "Usage Guidelines" section for valid values.
vlans	Number of the VLAN; valid values are from 1 to 4094.
mistp-instance *instances*	Specifies the instance numbers; valid values are from 1 to 16.
mst *instances*	Specifies the MST instance numbers; valid values are from 1 to 15.

Defaults

The default is the bridge priority is set to 32768.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM or the MSM.

If MISTP or the MAC reduction feature is enabled, valid *bridge_priority* values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440, with 0 indicating high priority and 61440, low priority.

If MISTP or the MAC reduction feature is disabled, valid *bridge_priority* values are from 0 to 65535.

If you enable MISTP, you cannot set the VLAN bridge priority.

If you enable PVST+, you cannot set the instance priority.

If you try to set instance priority with PVST+ enabled, this message is displayed:

```
This command is only valid when STP is in MISTP or MISTP-PVST+ mode.
```

Examples

This example shows how to set the bridge priority of instance 3:

```
Console> (enable) set spantree priority 14 mistp-instance 3
Instance 3 bridge priority set to 14.
Instance 3 does not exist.
Your configuration has been saved to NVRAM only.
Console> (enable)
```

This example shows how to set the bridge priority for MST instance 0:

```
Console> (enable) set spantree priority 28672 mst 0
MST Spantree 0 bridge priority set to 28672.
Console> (enable)
```

This example shows how to set the bridge priority for multiple MST instances:

```
Console> (enable) set spantree priority 28672 mst 0-4
MST Spantrees 0-4 bridge priority set to 28672.
Console> (enable)
```

Related Commands

show spantree

set spantree root

To set the primary or secondary root for specific VLANs, all VLANs of the switch, or an instance, use the **set spantree root** command.

set spantree root [**secondary**] [*vlans*] [**dia** *network_diameter*] [**hello** *hello_time*]

set spantree root [**secondary**] **mistp-instance** *instance* [**dia** *network_diameter*]
[**hello** *hello_time*]

set spantree root [**secondary**] **mst** *instance* [**dia** *network_diameter*] [**hello** *hello_time*]

Syntax Description

secondary	(Optional) Designates this switch as a secondary root, should the primary root fail.
vlans	(Optional) Number of the VLAN; valid values are from 1 to 4094.
dia *network_diameter*	(Optional) Specifies the maximum number of bridges between any two points of end stations; valid values are from 1 through 7.
hello *hello_time*	(Optional) Specifies in seconds, the duration between the generation of configuration messages by the root switch.
mistp-instance *instance*	Specifies the instance number; valid values are from 0 to 4094.
mst *instance*	Specifies an MST instance; valid values are from 0 to 4094.

Defaults

If you do not specify the **secondary** keyword, the default is to make the switch the primary root.

The default value of the network diameter is 7.

If you do not specify the *hello_time* value, the current value of *hello_time* is calculated from the network diameter.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a VLAN number, VLAN 1 is assumed.

This command is not supported by the NAM.

This command is run on backbone or distribution switches.

You can run the secondary root many times to create backup switches in case of a root failure.

The **set spantree root secondary** bridge priority value is 16384, except when MAC reduction or MISTP are enabled, then the value is 28672.

The **set spantree root** bridge priority value is 16384, except when MAC reduction or MISTP are enabled, then the value is 24576.

This command increases path costs to a value greater than 3000.

If you enable MISTP, you cannot set the VLAN root. If you enable PVST+, you cannot set the instance root.

Examples

This example shows how to set the primary root for a range of VLANs:

```
Console> (enable) set spantree root 1-10 dia 4
VLANs 1-10 bridge priority set to 8192
VLANs 1-10 bridge max aging time set to 14 seconds.
VLANs 1-10 bridge hello time set to 2 seconds.
VLANs 1-10 bridge forward delay set to 9 seconds.
Switch is now the root switch for active VLANs 1-6.
Console> (enable)
```

This example shows how to set the primary root for an instance:

```
Console> (enable) set spantree root mistp-instance 2-4 dia 4
Instances 2-4 bridge priority set to 8192
VLInstances 2-4 bridge max aging time set to 14 seconds.
Instances 2-4 bridge hello time set to 2 seconds.
Instances 2-4 bridge forward delay set to 9 seconds.
Switch is now the root switch for active Instances 1-6.
Console> (enable)
```

This example shows how to set the primary root for MST instance 5:

```
Console> (enable) set spantree root mst 5
Instance 5 bridge priority set to 24576.
Instance 5 bridge max aging time set to 16.
Instance 5 bridge hello time set to 2.
Instance 5 bridge forward delay set to 15.
Switch is now the root switch for active Instance 5.
Console> (enable)
```

This example shows how to set the secondary root for MST instance 0:

```
Console> (enable) set spantree root secondary mst 0
Instance 0 bridge priority set to 28672.
Instance 0 bridge max aging time set to 20.
Instance 0 bridge hello time set to 2.
Instance 0 bridge forward delay set to 15.
Console> (enable)
```

This example shows how to set the maximum number of bridges and the hello time of the root for MST instance 0:

```
Console> (enable) set spantree root mst 0 dia 7 hello 2
Instance 0 bridge priority set to 24576.
Instance 0 bridge max aging time set to 20.
Instance 0 bridge hello time set to 2.
Instance 0 bridge forward delay set to 15.
Switch is now the root switch for active Instance 0.
Console> (enable)
```

These examples show that setting the bridge priority to 8192 was not sufficient to make this switch the root. The priority was further reduced to 7192 (100 less than the current root switch) to make this switch the root switch. However, reducing it to this value did not make it the root switch for active VLANs 16 and 17.

```
Console> (enable) set spantree root 11-20.
VLANs 11-20 bridge priority set to 7192
VLANs 11-10 bridge max aging time set to 20 seconds.
VLANs 1-10 bridge hello time set to 2 seconds.
VLANs 1-10 bridge forward delay set to 13 seconds.
Switch is now the root switch for active VLANs 11-15,18-20.
Switch could not become root switch for active VLAN 16-17.
Console> (enable)

Console> (enable) set spantree root secondary 22,24 dia 5 hello 1
VLANs 22,24 bridge priority set to 16384.
VLANs 22,24 bridge max aging time set to 10 seconds.
VLANs 22,24 bridge hello time set to 1 second.
VLANs 22,24 bridge forward delay set to 7 seconds.
Console> (enable)
```

Related Commands

show spantree

set spantree uplinkfast

To enable fast switchover to alternate ports when the root port fails, use the **set spantree uplinkfast** command. This command applies to a switch, not to a WAN.

set spantree uplinkfast {**enable** | **disable**} [**rate** *station_update_rate*] [**all-protocols** {**off** | **on**}]

Syntax Description

enable	Enables fast switchover.
disable	Disables fast switchover.
rate *station_update_rate*	(Optional) Specifies the number of multicast packets transmitted per 100 ms when an alternate port is chosen after the root port goes down.
all-protocols	(Optional) Specifies whether or not to generate multicast packets for all protocols (IP, IPX, AppleTalk, and Layer 2 packets).
off	(Optional) Turns off the all-protocols feature.
on	(Optional) Turns on the all-protocols feature.

Defaults

The default *station_update_rate* is 15 packets per 100 milliseconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

This command is not available in MST mode.

The **set spantree uplinkfast enable** command has the following results:

- Changes the bridge priority to 49152 for all VLANs (allowed VLANs).
- Increases the path cost and portvlancost of all ports to a value greater than 3000.
- On detecting the failure of a root port, an instant cutover occurs to an alternate port selected by Spanning Tree Protocol.

If you run the **set spantree uplinkfast enable** command on a switch that has this feature already enabled, only the station update rate is updated. The rest of the parameters are not modified.

If you run the **set spantree uplinkfast disable** command on a switch, the UplinkFast feature is disabled but the switch priority and port cost values are not reset to the default settings. To reset the values to the default settings, enter the **clear spantree uplinkfast** command.

The default *station_update_rate* value is 15 packets per 100 milliseconds, which is equivalent to a 1-percent load on a 10-megabit per second Ethernet network. If you specify this value as 0, the generation of these packets is turned off.

You do not have to turn on the all-protocols feature on Catalyst 6500 series switches that have both the UplinkFast and protocol filtering features enabled. Use the all-protocols feature only on Catalyst 6500 series switches that have UplinkFast enabled but do not have protocol filtering; upstream switches in the network use protocol filtering. You must enter the **all-protocols** option to inform the UplinkFast task whether or not to generate multicast packets for all protocols.

Examples

This example shows how to enable spantree UplinkFast and specify the number of multicast packets transmitted to 40 packets per 100 milliseconds:

```
Console> (enable) set spantree uplinkfast enable rate 40
VLANs 1-4094 bridge priority set to 49152.
The port cost and portvlancost of all ports set to above 3000.
Station update rate set to 40 packets/100ms.
uplinkfast all-protocols field set to off.
uplinkfast enabled for bridge.
Console> (enable)
```

This example shows how to disable spantree UplinkFast:

```
Console> (enable) set spantree uplinkfast disable
Uplinkfast disabled for switch.
Use clear spantree uplinkfast to return stp parameters to default.
Console> (enable) clear spantree uplink
This command will cause all portcosts, portvlancosts, and the
bridge priority on all vlans to be set to default.
Do you want to continue (y/n) [n]? y
VLANs 1-1005 bridge priority set to 32768.
The port cost of all bridge ports set to default value.
The portvlancost of all bridge ports set to default value.
uplinkfast disabled for bridge.
Console> (enable)
```

This example shows how to turn on the all-protocols feature:

```
Console> (enable) set spantree uplinkfast enable all-protocols on
uplinkfast update packets enabled for all protocols.
uplinkfast enabled for bridge.
Console> (enable)
```

This example shows how to turn off the all-protocols feature:

```
Console> (enable) set spantree uplinkfast enable all-protocols off
uplinkfast all-protocols field set to off.
uplinkfast already enabled for bridge.
Console> (enable)
```

This example shows the output when instances have been configured:

```
Console> (enable) set spantree uplinkfast enable
Instances 1-15 bridge priority set to 49152.
The port cost and portinstancecost of all ports set to above 3000.
Station update rate set to 15 mpackets/100ms.
uplinkfast all-protocols field set to off.
uplinkfast already enabled for bridge.
Console> (enable)
```

Related Commands

clear spantree uplinkfast
show spantree uplinkfast

set ssh mode

To set the Secure Shell (SSH) version, use the **set ssh mode** command.

set ssh mode {**v1** | **v2**}

Syntax Description

v1	SSH version 1.
v2	SSH version 2.

Defaults

If you do not specify either the **v1** or the **v2** keyword, SSH operates in compatibility mode. See the "Usage Guidelines" for more information about compatibility mode.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The current implementation of Secure Shell encryption supports SSH version 1 and version 2. SSH version 1 supports the DES and 3DES encryption methods, and SSH version 2 supports the 3 DES and AES encryption methods.

Secure shell encryption can be used with RADIUS and TACACS+ authentication. To configure authentication with Secure Shell encryption, use the **telnet** keyword in the **set authentication** commands.

If you enter the **set ssh mode v1** command, the server accepts only SSH version 1 connections. If you enter the **set ssh mode v2** command, the server accepts only SSH version 2 connections.

In compatility mode, both SSH version 1 connections and version 2 connetions are supported. You can return to compatibility mode after operating in version 1 or version 2 mode by entering the **clear ssh mode** command.

Examples

This example shows how to configure SSH to accept only version 1 connections:

```
Console> (enable) set ssh mode v1
SSH protocol mode set to SSHv1 Only.
Console> (enable)
```

This example shows how to configure SSH to accept only version 2 connections:

```
Console> (enable) set ssh mode v2
SSH protocol mode set to SSHv2 Only.
Console> (enable)
```

Related Commands

clear ssh mode
set authentication enable
set authentication login
show ssh

set summertime

To specify whether the system should set the clock ahead one hour during daylight saving time, use the **set summertime** command.

set summertime {**enable** | **disable**} [*zone*]

set summertime recurring [{*week*} {*day*} {*month*} {*hh*:*mm*} {*week* | *day* | *month* | *hh*:*mm*} [*offset*]]

set summertime date {*month*} {*date*} {*year*} {*hh*:*mm*} {*month* | *date* | *year* | *hh*:*mm*} [*offset*]

Syntax Description

enable	Causes the system to set the clock ahead one hour during daylight saving time.
disable	Prevents the system from setting the clock ahead one hour during daylight saving time.
zone	(Optional) Time zone used by the **set summertime** command.
recurring	Specifies the summertime dates that recur every year.
week	(Optional) Week of the month (**first**, **second**, **third**, **fourth**, **last**, **1**...**5**).
day	(Optional) Day of the week (**Sunday**, **Monday**, **Tuesday**, and so forth).
month	Month of the year (**January**, **February**, **March**, and so forth).
hh:mm	Hours and minutes.
offset	(Optional) Amount of offset in minutes (from 1 to 1440 minutes).
date	Day of the month (from 1 to 31).
year	Number of the year (from 1993 to 2035).

Defaults

By default, the **set summertime** command is disabled. Once enabled, the default for *offset* is 60 minutes, following U.S. standards.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After you enter the **clear config** command, the dates and times are set to default.

Unless you configure it otherwise, this command advances the clock one hour at 2:00 a.m. on the first Sunday in April and moves back the clock one hour at 2:00 a.m. on the last Sunday in October.

Examples

This example shows how to cause the system to set the clock ahead one hour during daylight saving time:

```
Console> (enable) set summertime enable PDT
Summertime is enabled and set to “PDT”.
Console> (enable)
```

This example shows how to prevent the system from setting the clock ahead one hour during daylight saving time:

```
Console> (enable) set summertime disable
Summertime disabled.
Console> (enable)
```

This example shows how to set daylight saving time to the zonename AUS and repeat every year, starting from the third Monday of February at noon and ending at the second Saturday of August at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set summertime AUS recurring 3 Mon Feb 12:00 2 Saturday Aug 15:00 30
Summer time is disabled and set to ’AUS’ with offset 30 minutes.
   start: 12:00:00 Sun Feb 13 2000
   end:   14:00:00 Sat Aug 26 2000
   Recurring, starting at 12:00:00 on Sunday of the third week of February and ending
   on Saturday of the fourth week of August.
Console> (enable)
```

This example shows how to set the daylight saving time to start on January 29, 1999 at 2:00 a.m. and end on August 19, 2004 at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set summertime date jan 29 1999 02:00 aug 19 2004 15:00 30
Summertime is disabled and set to ''
Start : Fri Jan 29 1999, 02:00:00
End   : Thu Aug 19 2004, 15:00:00
Offset: 30 minutes
Recurring: no
Console> (enable)
```

This example shows how to set recurring to reset default to US summertime:

```
Console> (enable) set summertime recurring 3 mon feb 4 thurs oct 8:00 500
Command authorization none.
Summertime is enabled and set to ‘’
Start : Mon Feb 21 2000, 03:00:00
End   : Fri Oct 20 2000, 08:00:00
Offset: 500 minutes (8 hours 20 minutes)
Recurring: yes, starting at 03:00am of third Monday of February and ending on 08:00am of
fourth Thursday of October.
Console> (enable)
```

Related Commands

show summertime

set system baud

To set the console port baud rate, use the **set system baud** command.

set system baud *rate*

Syntax Description

rate	Baud rate; valid rates are **600**, **1200**, **2400**, **4800**, **9600**, **19200**, and **38400**.

Defaults

The default is 9600 baud.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the system baud rate to 19200:

```
Console> (enable) set system baud 19200
System console port baud rate set to 19200.
Console> (enable)
```

Related Commands

show system

8.6 EFT Copy

set system contact

To identify a contact person for the system, use the **set system contact** command.

set system contact [*contact_string*]

Syntax Description

contact_string	(Optional) Text string that contains the name of the person to contact for system administration. If you do not specify a contact string, the system contact string is cleared.

Defaults

The default is no system contact is configured.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the system contact string:

```
Console> (enable) set system contact Xena ext.24
System contact set.
Console> (enable)
```

Related Commands

show system

set system core-dump

To enable or disable the core dump feature, use the **set system core-dump** command.

set system core-dump {**enable** | **disable**}

Syntax Description

enable	Enables the core dump feature.
disable	Disables the core dump feature.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The core dump feature generates a report of images when your system fails due to a software error. The core image is stored in the file system. From this file, you can examine an error condition of a process when it is terminated due to an exception.

The size of the file system depends on the memory card size. The core dump file generated is proportional to the size of the system DRAM. Make sure that you have enough memory available to store the core dump file.

In order to maintain the core dump image, the yield CPU is disabled during the core dump process. You should have a redundant supervisor engine installed to take over normal operations. If the switch has a redundant supervisor engine setup, the redundant supervisor engine takes over automatically before the core dump occurs. The previously active supervisor engine resets itself after the core dump completes.

Examples

This example shows how to enable the core dump feature:

```
Console> (enable) set system core-dump enable
(1) In the event of a system crash, this feature will
     cause a core file to be written out.
(2) Core file generation may take up to 20 minutes.
(3) Selected core file is slot0:crash.hz
(4) Please make sure the above device has been installed,
    and ready to use
Core-dump enabled
Console> (enable)
```

This example shows how to disable the core dump feature:

```
Console> (enable) set system core-dump disable
Core-dump disabled
Console> (enable)
```

set system core-file

To specify the core image filename, use the **set system core-file** command.

set system core-file {*device*:[*filename*]}

Syntax Description

device	Device where the core image file resides; valid values are **bootflash** and **slot0**.
filename	(Optional) Name of the core image file.

Defaults

The default *filename* is “crashinfo.”

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A device name check is performed when you enter the **set system core-file** command. If a valid device name is not found, an error message displays.

When a core dump occurs, the actual file written out will append the date to the filename in this format: _{yymmdd}-{hhmmss}.

Examples

This example shows how to use the default core image filename:

```
Console> (enable) set system core-file bootflash:
Attach default filename crashinfo to the device
System core-file set.
Console> (enable)
```

This example shows how to set the core image filename:

```
Console> (enable) set system core-file slot0:abc
System core-file set.
Console> (enable)
```

Related Commands

set system core-dump

set system countrycode

To specify the country where the system is physically located, use the **set system countrycode** command.

set system countrycode *code*

Syntax Description

code	Country code; see the "Usage Guidelines" section for format information.

Defaults

The default is US (United States).

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The country code is a two-letter country code taken from ISO-3166 (for example, VA=Holy See [Vatican City State], VU=Vanuatu, and TF=French Southern Territories).

Examples

This example shows how to set the system country code:

```
Console> (enable) set system countrycode US
Country code is set to US.
Console> (enable)
```

8.6 EFT Copy

set system crashinfo

To permit the system to write a crash information file, use the **set system crashinfo** command.

set system crashinfo {**enable** | **disable**}

set system crashinfo-file *device:filename*

Syntax Description

enable	Permits the system to write a crash information file.
disable	Prevents the system from writing a crash information file.
crashinfo-file	Sets the crash information file name.
device:filename	Device and crash information file name.

Defaults

The crash information feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The crash information file contains extended system information that is captured quickly when the system reloads because of an error condition. Like the crash-dump file, the crash-info file is stored in the file system. The information in the crash information file should be used in addition to the core dump information and does not replace that information. By examining both the crash-info file and core dump file, Cisco TAC can better analyze an error condition.

To clear a system crash information file, enter the **set system crashinfo-file** command with no arguments.

Examples

This example shows how to permit the system to write a crash information file:

```
Console> (enable) set system crashinfo enable
Crashinfo enabled
Console> (enable)
```

This example shows how to specify the device where the crash information file is saved and the name of the file:

```
Console> (enable) set system crashinfo-file slot0:crashinfo
System crashinfo-file set.
Console> (enable)
```

This example shows how to clear a crash information file:

```
Console> (enable) set system crashinfo-file
System crashinfo-file cleared.
Console> (enable)
```

Related Commands

show system

set system crossbar-fallback

To select the action taken when the Switch Fabric Module fails, use the **set system crossbar-fallback** command.

set system crossbar-fallback {**bus-mode** | **none**}

Syntax Description

bus-mode	Fails to the system bus.
none	Does not fail over to the system bus.

Defaults

The default is **bus-mode**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can either have the Switch Fabric Module fail over to the bus or have the switch not fail over at all (in which case, the switch should be down).

This command is supported on systems configured with a Switch Fabric Module and the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to set the Switch Fabric Module to fail over to the system bus:

```
Console> (enable) set system crossbar-fallback bus-mode
System crossbar-fallback set to bus-mode.
Console> (enable)
```

This example shows how to set the Switch Fabric Module to not fail over:

```
Console> (enable) set system crossbar-fallback none
System crossbar-fallback set to none.
Console> (enable)
```

Related Commands

show fabric channel

set system highavailability

To enable or disable high system availability for the switch, use the **set system highavailability** command.

set system highavailability {**enable** | **disable**}

Syntax Description

enable	Activates system high availability.
disable	Deactivates system high availability.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

High availability provides Layer 2 and Layer 3 protocol redundancy.

If you enable high availability while the redundant supervisor engine is running, the switch checks the version compatibility between the two supervisor engines. If the versions are compatible, database synchronization occurs. When you disable high availability, database synchronization does not occur and protocols restart on the redundant supervisor engine after switchover.

If you disable high availability from the enabled state, synchronization from the active supervisor engine is stopped. On the redundant supervisor engine, current synchronization data is discarded. If you enable high availability from the disabled state, synchronization from the active supervisor engine to the redundant supervisor engine starts (if you have a redundant supervisor engine and its image version is compatible with the active supervisor engine).

Examples

This example shows how to enable high availability:

```
Console> (enable) set system highavailability enable
System high availability enabled.
Console> (enable)
```

This example shows how to disable high availability:

```
Console> (enable) set system highavailability disable
System high availability disabled.
Console> (enable)
```

Related Commands

set system highavailability versioning
show system highavailability

set system highavailability versioning

To enable and disable support for supervisor engine image versioning, use the **set system highavailability versioning** command.

set system highavailability versioning {**enable** | **disable**}

Syntax Description

enable	Activates system high-availability versioning.
disable	Deactivates system high-availability versioning.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The high-availability versioning feature allows the Catalyst 6500 series switch to run different images on the active and redundant supervisor engines. When you enable image versioning, Flash image synchronization (from active to the redundant supervisor engines) does not occur, allowing active and redundant supervisor engines to run different images.

Caution When you disable image versioning, the active and redundant supervisor engines must run the same image version.

If you disable the image versioning option from the enabled state, no additional action is necessary on the redundant supervisor engine. (The redundant supervisor engine should be running the same image as the active supervisor engine.) If you want to load a different image, you have to restart the redundant supervisor engine.

If you enable the image versioning option from the disabled state and you have a redundant supervisor engine and active supervisor engine running a different image than that of the active supervisor engine, Flash synchronization will copy the active supervisor engine image to the redundant supervisor engine image and then restart it.

If you enable the image versioning option on the active supervisor engine and the redundant supervisor engine is running a different image, the NVRAM synchronization cannot occur because the NVRAM versions are not compatible. If this is the case, after switchover, the old NVRAM configuration on the supervisor engine is used.

Examples

This example shows how to enable high-availability versioning:

```
Console> (enable) set system highavailability versioning enable
Image versioning enabled.
Console> (enable)
```

This example shows how to disable high-availability versioning:

```
Console> (enable) set system highavailability versioning disable
Image versioning disabled.
Console> (enable)
```

Related Commands

set system highavailability
show system highavailability

set system info-log

To log the output of specified show commands to a server for troubleshooting and debugging, use the **set system info-log** command.

set system info-log {**enable** | **disable**}

set system info-log command {**c***command_string***c**} [*position*]

set system info-log interval *mins*

set system info-log {**tftp** | **ftp** | **rcp** *username*} *host filename*

Syntax Description

enable | **disable**	Activates or deactivates system information logging.
command	Logs the specified **show** command to the server.
c	Delimiting character used to begin and end the **show** command.
command_string	Show command whose output is logged; valid values are show commands.
position	(Optional) Position of the **show** command in the system information logging index; valid values are from 1 to 15.
interval	Specifies the amount of time between system information logging events.
mins	Minutes between system information logging events; valid values are from 1 to 35000 minutes (approximately 25 days).
tftp	Copies system information logging output to a TFTP server.
ftp	Copies system information loggging output to an FTP server.
rcp	Copies system information logging output to an RCP server.
username	RCP username.
host	IP address or IP alias of the host.
filename	Name of the file.

Defaults

System information logging is disabled.

The interval between system information logging events is 1440 minutes.

System information logging output is copied to a TFTP server, and the filename is sysinfo.

If you do not provide an absolute path for the file, the TFTP directory is tftpboot. For RCP, the directory is the user's home directory.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enter the **show** command whose output is to be logged, you must type a delimiting character with no spaces on either side of the command. You can add only one show command at a time.

You can enter a maximum of 15 show commands for system information logging.

Examples

This example shows how to activate the system information logging feature:

```
Console> (enable) set system info-log enable
Successfully enabled system information logging.
Console> (enable)
```

This example shows how to include the output of the **show version** command in the log:

```
Console> (enable) set system info-log command "show version"
System command was successfully added to the list.
Console> (enable)
```

This example shows how to list the **show module** command as the third command in the system information logging index:

```
Console> (enable) set system info-log command >show module> 3
System command was successfully added to the list.
Console> (enable)
```

This example shows how to save system information logging with a specific filename to a specific TFTP server:

```
Console> (enable) set system info-log tftp 10.5.2.10 sysinfo
Successfully set the system information logging file to tftp:sysinfo
Console> (enable)
```

This example shows how to save system information logging with a specific filename to an RCP server:

```
Console> (enable) set system info-log rcp shravan 10.5.2.10 sysinfo
Successfully set the system information logging file to rcp:sysinfo
Console> (enable)
```

Related Commands

clear config
clear system info-log command
show system info-log

set system location

To identify the location of the system, use the **set system location** command.

set system location [*location_string*]

Syntax Description

location_string	(Optional) Text string that indicates where the system is located.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a location string, the system location is cleared.

Examples

This example shows how to set the system location string:

```
Console> (enable) set system location Closet 230 4/F
System location set.
Console> (enable)
```

Related Commands

show system

set system modem

To enable or disable modem control lines on the console port, use the **set system modem** command.

set system modem {**enable** | **disable**}

Syntax Description

enable	Activates modem control lines on the console port.
disable	Deactivates modem control lines on the console port.

Defaults

The default is modem control lines are disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to disable modem control lines on the console port:

```
Console> (enable) set system modem disable
Modem control lines disabled on console port.
Console> (enable)
```

Related Commands

show system

8.6 EFT Copy

set system name

To configure a name for the system, use the **set system name** command.

set system name [*name_string*]

Syntax Description

name_string	(Optional) Text string that identifies the system.

Defaults

The default is no system name is configured.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use the **set system name** command to assign a name to the switch, the switch name is used as the prompt string. However, if you specify a different prompt string using the **set prompt** command, that string is used for the prompt.

If you do not specify a system name, the system name is cleared and a DNS lookup is initiated for a system name. If a name is found, that is the name used; if no name is found, no name is designated.

The system name can be 255 characters long, and the prompt can be 20 characters long. The system name is truncated appropriately when used as a prompt; a greater-than symbol (>) is appended to the truncated system name. If the system name was found from a DNS lookup, it is truncated to remove the domain name.

If the prompt is obtained using the system name, it is updated whenever the system name changes. You can overwrite this prompt any time by setting the prompt manually. Any change in the prompt is reflected in all current open sessions.

If you do not specify a name, the system name is cleared.

Examples

This example shows how to set the system name to Information Systems:

```
Console> (enable) set system name Information Systems
System name set.
Console> (enable)
```

Related Commands

set prompt
show system

set system profile

To configure a system profile file, use the **set system profile** command.

set system profile *device***:***filename*

set system profile {**enable** | **disable**} *mod_list*

Syntax Description

*device***:***filename*	Name of the device and the profile filename separated by a colon.
enable	Enables profile file loading on a per-module basis.
disable	Disables profile file loading on a per-module basis.
mod_list	Numbers of the modules on which profile file loading is enabled or diabled; valid values are from 1 to 9, 15, and 16.

Defaults

The default value for the PROFILE_FILE variable is null.

The system profile feature is enabled on each module.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A profile file allows you to have a customized configuration as the designated configuration on the switch. The profile file allows you to load a configuration on the switch either as the default configuration or as a custom configuration that would enable or disable certain features. With the profile files, you can eliminate the features or processes that might pose security risks (for example, disabling CDP or turning off auto-trunking on a port) to your switch.

A profile file that has most of the security risks disabled is also known as a “lockdown” profile. A lockdown profile changes the functionality of the switch from enabling access to preventing access by default. When a lockdown profile is applied, you must manually enable the features that were disabled by the profile file. For a sample lockdown profile, see to the “Working with Configuration Files” chapter of the *Catalyst 6500 Series Software Configuration Guide*.

Follow these guidelines when working with profile files:

- A profile file can be either from internal bootflash or from PCMCIA slots but not from a TFTP server.
- A profile file must be a Catalyst operating system configuration file type that starts with “begin.”
- Keywords that are supported in release 8.4 are ALL_MODULES, ALL_PORTS, ALL_MODULE_PORTS, and ALL_VLANS.
- The ALL_MODULES, ALL_PORTS, and ALL_VLANS keywords can be anywhere in the profile file.

- The ALL_MODULE_PORTS keyword must be within a module section that is explicitly defined, as all module sections are explicitly defined in Catalyst operating system configuration files. If the ALL_MODULE_PORTS keyword is not in a module section, the keyword statement is ignored.
- A profile name in PROFILE_FILE must be fully qualified. You must specify a device name.
- A profile file configuration must be loaded after a text configuration and before an auto-config configuration.

The **set system profile** {**enable** | **disable**} *mod_list* command allows you to enable or disable profile file loading for a specified module.

For more information about system profile files, see to the “Working with Configuration Files” chapter of the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to set the name of the device and the profile filename:

```
Console> (enable) set system profile bootflash:test.cfg
System is set to be configured with profile file bootflash:test.cfg.
Console> (enable)
```

This example shows how to disable system profile loading on a specified module:

```
Console> (enable) set system profile disable 2
System profile loading is disabled for module 2.
Console> (enable)
```

Related Commands

clear config
clear system profile
show system profile

set system supervisor-update

To configure the Erasable Programmable Logic Device (EPLD) upgrade process, use the **set system supervisor-update** command.

set system supervisor-update {**automatic** | **disable** | **force**}

Syntax Description

automatic	Upgrades an earlier supervisor engine EPLD image at bootup.
force	Upgrades supervisor engine EPLD image regardless of the version label.
disable	Disables automatic updates of supervisor engine EPLD image at bootup.

Defaults

The supervisor engine EPLD upgrade is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you specify the **automatic** keyword, the system checks the version level of the bundled EPLD image and performs the upgrade if the bundled EPLD image version is greater than the existing version.

If you specify the **force** keyword, the system upgrades the existing EPLD image with the bundled EPLD image regardless of the version level. After a forced upgrade, the configuration reverts back to the automatic default setting.

If you specify the **disable** keyword, the automatic EPLD upgrade process is disabled.

Note Supervisor engine EPLD upgrades are supported only on Supervisor Engine 2. Non-supervisor engine module (switching modules and service modules) EPLD upgrades are supported using Supervisor Engine 1 or Supervisor Engine 2.

The EPLD image for Supervisor Engine 2 is included in the Catalyst supervisor engine software image. The EPLD image for non-supervisor engine modules is provided in a separate downloadable image.

Examples

This example shows how to specify the automatic option for EPLD upgrades:

```
Console> (enable) set system supervisor-update automatic
Down-rev supervisor EPLD's will be re-programmed next reset.
Console> (enable)
```

This example shows how to specify the force option for EPLD upgrades:

```
Console> (enable) set system supervisor-update force
Supervisor EPLD's will synchronize to the image bundle during the next reset.
Console> (enable)
```

8.6 EFT Copy

This example shows how to disable EPLD upgrades:

```
Console> (enable) set system supervisor-update disable
Supervisor EPLD update during reset is disabled.
Console> (enable)
```

Related Commands

download
show system supervisor-update
show version

set system switchmode allow

To configure the switching mode for the system, use the **set system switchmode allow** command.

set system switchmode allow {**truncated** | **bus-only**}

Syntax Description

truncated	Specifies truncated mode; see the "Usage Guidelines" section for additional information.
bus-only	Forces the system to be in flow-through mode.

Defaults

The default is truncated.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you install a Switch Fabric Module in a Catalyst 6500 series switch, the traffic is forwarded to and from modules in one of the following modes:

- Flow-through mode—In this mode, data passes between the local bus and the supervisor engine bus. This mode is used for traffic to or from nonfabric-enabled modules.
- Truncated mode—In this mode, only the truncated data (the first 64 bytes of the frame) is sent over the switch fabric channel if both the destination and the source modules are fabric-enabled modules. If either the source or destination is not a fabric-enabled module, the data goes through the switch fabric channel and the data bus. The Switch Fabric Module does not get involved when traffic is forwarded between nonfabric-enabled modules.
- Compact mode—In this mode, a compact version of the DBus header is forwarded over the switch fabric channel, delivering the best possible switching rate. Nonfabric-enabled modules do not support the compact mode and will generate CRC errors if they receive frames in compact mode. This mode is only used if nonfabric-enabled modules are not installed in the chassis.

If you enter the **truncated** keyword and your system does not contain nonfabric-enabled modules, the system is placed in compact mode.

If two or more fabric-enabled modules are installed in your system with a nonfabric-enabled module, forwarding between these modules occurs in truncated mode.

If there is a combination of a Supervisor Engine 720 with switch fabric capability and nonfabric-enabled modules in the chassis, the **bus-only** keyword is not permitted. The system stays in truncated mode.

Examples

This example shows how to set the switching mode to truncated:

```
Console> (enable) set system switchmode allow truncated
System switchmode allow set to truncated.
Console> (enable)
```

8.6 EFT Copy

This example shows how to set the switching mode to bus-only:

```
Console> (enable) set system switchmode allow bus-only
System switchmode allow set to bus-only.
Console> (enable)
```

Related Commands

show system switchmode

set system syslog-dump

To write system messages in the syslog buffer to a flash file before the system fails, use the **set system syslog-dump** command.

set system syslog-dump {**enable** | **disable**}

Syntax Description

enable	Enables the syslog dump feature.
disable	Disables the syslog dump feature.

Defaults

The syslog dump feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If the system fails, a file containing the system messages in the syslog buffer (as displayed when entering the **show logging buffer** command) is produced.

Enter the set **system syslog-file** command to specify the flash device and syslog filename for the syslog dump when the system fails.

Examples

This example shows how to enable the syslog dump feature:

```
Console> (enable) set system syslog-dump enable
(1) In the event of a system crash, this feature will
    cause a syslog file to be written out.
(2) Selected syslog file is slot0:sysloginfo
(3) Please make sure the above device has been installed,
    and ready to use.
Syslog-dump enabled
Console> (enable)
```

This example shows how to disable the syslog dump feature:

```
Console> (enable) set system syslog-dump disable
Syslog-dump disabled
Console> (enable)
```

Related Commands

set system syslog-file
show system

set system syslog-file

To specify the flash device and filename for the syslog dump when the system fails, use the **set system syslog-file** command.

set system syslog-file [*device*:[*filename*]]

Syntax Description

device:	(Optional) Name of the flash device.
filename	(Optional) Name of the file for the syslog dump.

Defaults

The flash device is slot0.

The filename is sysloginfo.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Enter the **set system syslog-dump** command to enable or disable the syslog dump feature. You can change the flash device and the filename when the syslog dump feature is enabled or disabled.

If you only specify the flash device, the filename is automatically set to sysloginfo. If you do not specify the device or the filename, the previous filename for the syslog dump is cleared, and the default flash device and filename (slot0:sysloginfo) are used.

Examples

This example shows how to set the flash device for the syslog dump feature:

```
Console> (enable) set system syslog-file bootflash:
Default filename sysloginfo added to the device bootflash:
System syslog-file set.
Console> (enable)
```

This example shows how to set the flash device and the filename:

```
Console> (enable) set system syslog-file bootflash:sysmsgs1
System syslog-file set.
Console> (enable)
```

This example shows how to restore the flash device and the filename to the default settings:

```
Console> (enable) set system syslog-file
System syslog-file set to the default file.
Console> (enable)
```

Related Commands

set system syslog-dump
show system

8.6 EFT Copy

set tacacs attempts

To configure the maximum number of login attempts allowed to the TACACS+ server, use the **set tacacs attempts** command.

set tacacs attempts *count*

Syntax Description

count	Number of login attempts allowed; valid values are from 1 to 10.

Defaults

The default is three attempts.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to configure the TACACS+ server to allow a maximum of six login attempts:

```
Console> (enable) set tacacs attempts 6
Tacacs number of attempts set to 6.
Console> (enable)
```

Related Commands

show tacacs

set tacacs directedrequest

To enable or disable the TACACS+ directed-request option, use the **set tacacs directedrequest** command. When enabled, you can direct a request to any of the configured TACACS+ servers and only the username is sent to the specified server.

set tacacs directedrequest {**enable** | **disable**}

Syntax Description

enable	Sends the portion of the address before the @ sign (the username) to the host specified after the @ sign.
disable	Sends the entire address string to the default TACACS+ server.

Defaults

The default is the TACACS+ directed-request option is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enable TACACS+ directed-request, you must specify a configured TACACS+ server after the @ sign. If the specified host name does not match the IP address of a configured TACACS+ server, the request is rejected. When TACACS+ directed-request is disabled, the Catalyst 6500 series switch queries the list of servers beginning with the first server in the list and then sends the entire string, accepting the first response from the server. This command is useful for sites that have developed their own TACACS+ server software to parse the entire address string and make decisions based on the contents of the string.

Examples

This example shows how to enable the **tacacs directedrequest** option:

```
Console> (enable) set tacacs directedrequest enable
Tacacs direct request has been enabled.
Console> (enable)
```

Related Commands

show tacacs

set tacacs key

To set the key for TACACS+ authentication and encryption, use the **set tacacs key** command.

set tacacs key *key*

Syntax Description

key	Printable ASCII characters used for authentication and encryption.

Defaults

The default value of *key* is null.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The key must be the same key used on the TACACS+ server. All leading spaces are ignored. Spaces within the key and at the end of the key are included. Double quotation marks are not required, even if there are spaces between words in the key, unless the quotation marks themselves are part of the key. The key can consist of any printable ASCII characters except the tab character.

The key length must be less than 100 characters long.

Examples

This example shows how to set the authentication and encryption key:

```
Console> (enable) set tacacs key Who Goes There
The tacacs key has been set to Who Goes There.
Console> (enable)
```

Related Commands

clear spantree uplinkfast
show tacacs

set tacacs server

To define a TACACS+ server, use the **set tacacs server** command.

set tacacs server *ip_addr* [**primary**]

Syntax Description

ip_addr	IP address of the server on which the TACACS+ server resides.
primary	(Optional) Designates the specified server as the primary TACACS+ server.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure a maximum of three servers. The primary server, if configured, is contacted first. If no primary server is configured, the first server configured becomes the primary server.

Examples

This example shows how to configure the server on which the TACACS+ server resides and to designate it as the primary server:

```
Console> (enable) set tacacs server 170.1.2.20 primary
170.1.2.20 added to TACACS server table as primary server.
Console> (enable)
```

Related Commands

clear tacacs server
show tacacs

set tacacs timeout

To set the response timeout interval for the TACACS+ server daemon, use the **set tacacs timeout** command. The TACACS+ server must respond to a TACACS+ authentication request before this interval expires or the next configured server is queried.

set tacacs timeout *seconds*

Syntax Description

seconds	Timeout response interval in seconds; valid values are from 1 to 255.

Defaults

The default is 5 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the response timeout interval for the TACACS+ server to 8 seconds:

```
Console> (enable) set tacacs timeout 8
Tacacs timeout set to 8 seconds.
Console> (enable)
```

Related Commands

show tacacs

set test diagfail-action

To set the action that the supervisor engine takes when a diagnostics test fails, use the **set test diagfail-action** command.

set test diagfail-action {**offline** | **ignore**}

Syntax Description

offline	Sets the supervisor engine to stay offline after a diagnostics test failure.
ignore	Sets the supervisor engine to ignore the diagnostics test failure and to boot up.

Defaults

The supervisor engine stays offline.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Enter the **show test diagfail-action** command to display the action that the supervisor engine takes after a test failure.

Examples

This example shows how to set the supervisor engine to stay offline:

```
Console> (enable) set test diagfail-action offline
Diagnostic failure action for SUP set to offline.
Console> (enable)
```

This example shows how to set the supervisor engine to ignore the diagnostics test failure and to boot up:

```
Console> (enable) set test diagfail-action ignore
Diagnostic failure action for SUP set to ignore.
Console> (enable)
```

Related Commands

show test

set test diaglevel

To set the diagnostic level, use the **set test diaglevel** command.

set test diaglevel {**complete** | **minimal** | **bypass**}

Syntax Description

complete	Specifies complete diagnostics.
minimal	Specifies minimal diagnostics.
bypass	Specifies bypass diagnostics.

Defaults

The default is **minimal**. See the "Usage Guidelines" section for more information about the three diagnostic levels.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Setting the diagnostic level determines the level of testing that occurs when the system or module is reset. The three levels are as follows:

- **complete**—This level runs all tests.
- **minimal**—This level runs only EARL tests for the supervisor engine and loopback tests for all ports in the system.
- **bypass**—This level skips all tests.

Note Although the default is **minimal**, we recommend that you set the diagnostic level at **complete**. We strongly recommend that you do not set the diagnostic level to **bypass**.

Examples

This example shows how to set the diagnostic level to complete:

```
Console> (enable) set test diaglevel complete
Diagnostic level set to complete.
Console> (enable)
```

This example shows how to set the diagnostic level to bypass:

```
Console> (enable) set test diaglevel bypass
Diagnostic level set to bypass.
Console> (enable)
```

Related Commands

show test

8.6 EFT Copy

set time

To change the time of day on the system clock, use the **set time** command.

set time [*day_of_week*] [*mm/dd/yy*] [*hh:mm:ss*]

Syntax Description

day_of_week	(Optional) Day of the week.
mm/dd/yyyy	(Optional) Month, day, and year.
hh:mm:ss	(Optional) Current time in 24-hour format.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the system clock to Sunday, October 31, 2004, 7:50 a.m:

```
Console> (enable) set time sun 10/31/2004 7:50
Sun Oct 31 2004, 07:50:00
Console> (enable)
```

Related Commands

show time

set timezone

To set the time zone for the system, use the **set timezone** command.

set timezone [*zone_name*] [*hours* [*minutes*]]

Syntax Description

zone_name	(Optional) Name of the time zone to be displayed.
hours	(Optional) Number of hours offset from UTC.
minutes	(Optional) Number of minutes offset from UTC. If the specified *hours* value is a negative number, then the *minutes* value is assumed to be negative as well.

Defaults

The default is the time zone is set to UTC.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set timezone** command is effective only when Network Time Protocol (NTP) is running. If you set the time explicitly and NTP is disengaged, the **set timezone** command has no effect. If you have enabled NTP and have not entered the **set timezone** command, the Catalyst 6500 series switch displays UTC by default.

Examples

This example shows how to set the time zone to pacific standard time with an offset of minus 8 hours from UTC:

```
Console> (enable) set timezone PST -8
Timezone set to "PST", offset from UTC is -8 hours.
Console> (enable)
```

Related Commands

clear timezone
show timezone

set traffic monitor

To configure the threshold at which a high-traffic log will be generated, use the **set traffic monitor** command.

set traffic monitor *threshold*

Syntax Description

threshold	1 to 100 percent.

Defaults

The threshold is set to 100 percent; no high-traffic log is created.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If backplane traffic exceeds the threshold configured by the **set traffic monitor** command, a high-traffic log is created. If the threshold is set to 100 percent, no high-traffic system warning is generated.

Examples

This example shows how to set the high-traffic threshold to 80 percent:

```
Console> (enable) set traffic monitor 80
Traffic monitoring threshold set to 80%.
Console> (enable)
```

Related Commands

show traffic

8.6 EFT Copy

set transceiver-monitoring

To enable or disable transceiver monitoring, use the **set transceiver-monitoring** command.

set transceiver-monitoring {**enable** | **disable** | {**interval** *interval*}}

Syntax Description

enable	Enables transceiver monitoring.
disable	Disables transceiver monitoring.
interval *interval*	Sets the transceiver monitoring interval; valid values are from 4 to 1440 minutes.

Defaults

The defaults are as follows:

- Transceiver monitoring is enabled.
- *interval* is 10 minutes.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The DOM feature measures the transceiver characteristics such as temperature, voltage, laser bias current, receive optical power and laser transmit power and allows software to monitor them against alarm and threshold values.

Examples

This example shows how to enable transceiver monitoring:

```
Console> (enable) set transceiver-monitoring enable
Transceiver monitoring is successfully enabled
Console> (enable)
```

This example shows how to disable transceiver monitoring:

```
Console> (enable) set transceiver-monitoring disable
Transceiver monitoring is successfully disabled
Console> (enable)
```

This example shows how to set the transceiver monitoring interval to 12 minutes:

```
Console> (enable)  set transceiver-monitoring interval 12
Transceiver monitoring interval is set to 12 minutes
Console> (enable)
```

Related Commands

show port transceiver

set trunk

To configure trunk ports and to add VLANs to the allowed VLAN list for existing trunks, use the **set trunk** command.

set trunk *mod/ports* {**on** | **off** | **desirable** | **auto** | **nonegotiate**} [*vlans* | **none**]
[**isl** | **dot1q** | **dot10** | **lane** | **negotiate**]

set trunk all off

Syntax Description

mod/port	Number of the module and the port or ports on the module.
on	Forces the port to become a trunk port and persuade the neighboring port to become a trunk port. The port becomes a trunk port even if the neighboring port does not agree to become a trunk.
off	Forces the port to become a nontrunk port and persuade the neighboring port to become a nontrunk port. The port becomes a nontrunk port even if the neighboring port does not agree to become a nontrunk port.
desirable	Causes the port to negotiate actively with the neighboring port to become a trunk link.
auto	Causes the port to become a trunk port if the neighboring port tries to negotiate a trunk link.
nonegotiate	Forces the port to become a trunk port but prevents it from sending DTP frames to its neighbor.
vlans	(Optional) VLANs to add to the list of allowed VLANs on the trunk; valid values are from 1 to 4094.
none	(Optional) Clears all VLANs from the trunk. See the “Usage Guidelines” section for more information.
isl	(Optional) Specifies an ISL trunk on a Fast or Gigabit Ethernet port.
dot1q	(Optional) Specifies an IEEE 802.1Q trunk on a Fast or Gigabit Ethernet port.
dot10	(Optional) Specifies an IEEE 802.10 trunk on a FDDI or CDDI port.
lane	(Optional) Specifies an ATM LANE trunk on an ATM port.
negotiate	(Optional) Specifies that the port become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring port.
all off	Turns off trunking on all ports.

Defaults

The default port mode is **auto**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

The following usage guidelines apply when using the **set trunk** command:

- If a trunk-type keyword (**isl**, **dot1q**, **negotiate**) is not specified when configuring an EtherChannel trunk, the current trunk type is not affected.
- To return a trunk to its default trunk type and mode, enter the **clear trunk** *mod/port* command.
- Trunking capabilities are hardware-dependent. Refer to the *Catalyst 6500 Series Module Installation Guide* to determine the trunking capabilities of your hardware, or enter the **show port capabilities** command.
- Catalyst 6500 series switches use DTP to negotiate trunk links automatically on EtherChannel ports. Whether or not a port will negotiate to become a trunk port depends on both the mode and the trunk type specified for that port. Refer to the *Catalyst 6500 Series Switch Switch Software Configuration Guide* for detailed information on how trunk ports are negotiated.
- DTP is a point-to-point protocol. However, some internetworking devices might improperly forward DTP frames. You can avoid this problem by ensuring that trunking is turned **off** on ports connected to non-Catalyst 6500 series switch devices if you do not intend to trunk across those links. When enabling trunking on a link to a Cisco router, enter the **noneg** keyword to cause the port to become a trunk but not generate DTP frames.
- To remove VLANs from the allowed list for a trunk, enter the **clear trunk** *mod/port vlans* command. When you first configure a port as a trunk, the **set trunk** command always adds *all* VLANs to the allowed VLAN list for the trunk, even if you specify a VLAN range. (The specified VLAN range is ignored.)
- To remove VLANs from the allowed list, enter the **clear trunk** *mod/port vlans* command. To later add VLANs that were removed, enter the **set trunk** *mod/port vlans* command.
- You cannot change the allowed VLAN range on the MSM port. The MSM port can be configured only as an IEEE 802.1Q-type trunk.
- For trunking to be negotiated on EtherChannel ports, the ports must be in the same VTP domain. However, you can use the **on** or **noneg** mode to force a port to become a trunk, even if it is in a different domain.
- When you configure a trunk, all VLANs are active on the trunk by default. If you do not want any active VLANs on the trunk, enter the **none** keyword. The **none** keyword clears all VLANs from the trunk.

Examples

This example shows how to set port 2 on module 1 as a trunk port:

```
Console> (enable) set trunk 1/2 on
Port(s) 1/2 trunk mode set to on.
Console> (enable)
```

This example shows how to add VLANs 5 through 50 to the allowed VLAN list for a trunk port (VLANs were previously removed from the allowed list with the **clear trunk** command):

```
Console> (enable) set trunk 1/1 5-50
Adding vlans 5-50 to allowed list.
Port(s) 1/1 allowed vlans modified to 1,5-50,101-1005.
Console> (enable)
```

This example shows how to set port 5 on module 4 as an 802.1Q trunk port in **desirable** mode:

```
Console> (enable) set trunk 4/5 desirable dot1q
Port(s) 4/5 trunk mode set to desirable.
Port(s) 4/5 trunk type set to dot1q.
Console> (enable)
```

8.6 EFT Copy

This example shows how to configure a trunk without any VLANs:

```
Console> (enable) set trunk 7/1 on none dot1q
Removing Vlan(s) 1-4094 from allowed list.
Port 7/1 allowed vlans modified to none.
Port(s) 7/1 trunk mode set to on.
Port(s) 7/1 trunk type set to dot1q.
Console> (enable)
```

Related Commands

clear trunk
set vtp
show port dot1q-ethertype
show trunk
show vtp statistics

set udld

To enable or disable the UDLD information display on specified ports or globally on all ports, use the **set udld** command.

set udld enable | **disable** [*mod/port*]

Syntax Description

enable	Enables the UDLD information display.
disable	Disables the UDLD information display.
mod/port	(Optional) Number of the module and port on the module.

Defaults

The defaults are as follows:

- UDLD global enable state—Globally disabled.
- UDLD per-port enable state for fiber-optic media—Enabled on all Ethernet fiber-optic ports.
- UDLD per-port enable state for twisted-pair (copper) media—Disabled on all Ethernet 10/100 and 1000BASE-TX ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Whenever a unidirectional connection is detected, UDLD displays a syslog message to notify you and the network management application (through SNMP) that the port on which the misconfiguration has been detected has been disabled.

If you enter the global **set udld enable** or **disable** command, UDLD is globally configured. If UDLD is globally disabled, UDLD is automatically disabled on all interfaces, but the per-port enable (or disable) configuration is not changed. If UDLD is globally enabled, whether or not UDLD is running on an interface depends on its per-port configuration.

UDLD is supported on both Ethernet fiber and copper interfaces. UDLD can only be enabled on Ethernet fiber or copper interfaces.

Examples

This example shows how to enable the UDLD message display for port 1 on module 2:

```
Console> (enable) set udld enable 2/1
UDLD enabled on port 2/1.
Warning:UniDirectional Link Detection
should be enabled only on ports not connected to hubs,
media converters or similar devices.
Console> (enable)
```

This example shows how to disable the UDLD message display for port 1 on module 2:

```
Console> (enable) set udld disable 2/1
UDLD disabled on port 2/1.
Warning:UniDirectional Link Detection
should be enabled only on ports not connected to hubs,
media converters or similar devices.
Console> (enable)
```

This example shows how to enable the UDLD message display for all ports on all modules:

```
Console> (enable) set udld enable
UDLD enabled globally.

Console> (enable)
```

This example shows how to disable the UDLD message display for all ports on all modules:

```
Console> (enable) set udld disable
UDLD disabled globally
Console> (enable)
```

Related Commands

show udld

set udld aggressive-mode

To enable or disable the UDLD aggressive mode on specified ports, use the **set udld aggressive-mode** command.

set udld aggressive-mode enable | **disable** *mod/port*

Syntax Description

enable	Enables UDLD aggressive mode.
disable	Disables UDLD aggressive mode.
mod/port	Number of the module and port on the module.

Defaults

The default is aggressive mode is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can use the aggressive mode in cases in which a port that sits on a bidirectional link stops receiving packets from its neighbor. When this happens, if aggressive mode is enabled on the port, UDLD will try to reestablish the connection with the neighbor. If connection is not reestablished after eight failed retries, the port is error disabled.

We recommend that you use this command on point-to-point links between Cisco switches only.

This command is not supported by the NAM.

Examples

This example shows how to enable aggressive mode:

```
Console> (enable) set udld aggressive-mode enable 2/1
Aggressive UDLD enabled on port 5/13.
Warning:Aggressive Mode for UniDirectional Link Detection
should be enabled only on ports not connected to hubs,
media converters or similar devices.
Console> (enable)
```

Related Commands

set udld
show udld

8.6 EFT Copy

set udld interval

To set the UDLD message interval timer, use the **set udld interval** command.

set udld interval *interval*

Syntax Description

interval	Message interval in seconds; valid values are from 7 to 90 seconds.

Defaults

The default is 15 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to set the message interval timer:

```
Console> (enable) set udld interval 90
UDLD message interval set to 90 seconds
Console> (enable)
```

Related Commands

set udld
show udld

set vlan

To group ports into a VLAN, set the private VLAN type, map or unmap VLANs to or from an instance, specify an 802.1X port to a VLAN, or secure a range of VLANs on a Firewall Services Module, use the **set vlan** command.

set vlan {*vlans*}{*mod/ports*}

set vlan {*vlans*} [**name** *name*] [**type** *type*] [**state** *state*] [**said** *said*] [**mtu** *mtu*]
[**bridge** *bridge_num*] [**mode** *bridge_mode*] [**stp** *stp_type*] [**translation** *vlan_num*]
[**aremaxhop** *hopcount*] [**pvlan-type** *pvlan_type*] [**mistp-instance** *mistp_instance*]
[**ring** *hex_ring_number*] [**decring** *decimal_ring_number*] [**parent** *vlan_num*]
[**backupcrf** {**off** | **on**}] [**stemaxhop** *hopcount*] [**rspan**]

set vlan {*vlans*} **firewall-vlan** {*mod*}

set vlan {*vlan*} **firewall-vlan** {*mod*} **msfc-fwsm-interface**

Syntax Description

vlans	Number identifying the VLAN; valid values are from 1 to 4094.
mod/ports	Number of the module and ports on the module belonging to the VLAN.
name *name*	(Optional) Defines a text string used as the name of the VLAN; valid values are from 1 to 32 characters.
type *type*	(Optional) Identifies the VLAN type.
state *state*	(Optional) Specifies whether the state of the VLAN is active or suspended.
said *said*	(Optional) Specifies the security association identifier; valid values are from 1 to 4294967294.
mtu *mtu*	(Optional) Specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from 576 to 18190.
bridge *bridge_num*	(Optional) Specifies the identification number of the bridge; valid values are hexadecimal numbers from 0x1 to 0xF.
mode *bridge_mode*	(Optional) Specifies the bridge mode; valid values are **srt** and **srb**.
stp *stp_type*	(Optional) Specifies the STP type; valid values are **ieee**, **ibm**, and **auto**.
translation *vlan_num*	(Optional) Specifies a translational VLAN used to translate FDDI or Token Ring to Ethernet; valid values are from 1 to 4094.
aremaxhop *hopcount*	(Optional) Specifies the maximum number of hops for All-Routes Explorer frames; valid values are from 1 to 13.
pvlan-type *pvlan-type*	(Optional) Keyword and options to specify the private VLAN type. See the "Usage Guidelines" section for valid values.
mistp-instance *mistp_instance*	(Optional) Specifies the MISTP instance; valid values are **none** and from 1 to 16.
ring *hex_ring_number*	(Optional) Keyword to specify the VLAN as the primary VLAN in a private VLAN.
decring *decimal_ring_number*	(Optional) Specifies the decimal ring number; valid values are from 1 to 4095.
parent *vlan_num*	(Optional) Specifies the VLAN number of the parent VLAN; valid values are from 1 to 4094.
backupcrf off | **on**	(Optional) Specifies whether the TrCRF is a backup path for traffic.

stemaxhop *hopcount*	(Optional) Specifies the maximum number of hops for Spanning Tree Explorer frames; valid values are from 1 to 14.
rspan	(Optional) Creates a VLAN for remote SPAN.
firewall-vlan	Specifies VLANs that are secured by a Firewall Services Module; see the "Usage Guidelines" section for more information about specifying a VLAN range for a Firewall Services Module.
mod	Number of the Firewall Services Module.
msfc-fwsm-interface	Specifies the VLAN that is to be the interface between the MSFC and the Firewall Services Module.

Defaults

The default values are as follows:

- Switched Ethernet ports and Ethernet repeater ports are in VLAN 1.
- *said* is 100001 for VLAN 1, 100002 for VLAN 2, 100003 for VLAN 3, and so forth.
- *type* is Ethernet.
- *mtu* is 1500 bytes.
- *state* is active.
- *hopcount* is 7.
- *pvlan type* is none.
- *mistp_instance* is no new instances have any VLANs mapped. For an existing VLAN, the existing instance configuration is used.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

If you are configuring normal-range VLANs, you cannot use the **set vlan** command until the Catalyst 6500 series switch is either in VTP transparent mode (**set vtp mode transparent**) or until a VTP domain name has been set (**set vtp domain name**). To create a private VLAN, UTP mode must be transparent.

If you set the VTP version to 3, VLAN 1 (the Cisco default VLAN) and VLANs 1002-1005 are configurable. If your switch has VTP version 1 or VTP version 2 neighbors, only default values are advertised for these VLANs. We recommend that you do not modify these VLANs if you want interoperability with older versions of VTP.

If you specify a range of VLANs, you cannot use the VLAN name.

If you enter the **mistp-instance none** command, the specified VLANs are unmapped from any instance they are mapped to.

The **set vlan** *vlan_num* **mistp-instance** *mistp_instance* command is available in PVST+ mode.

You cannot set multiple VLANs for ISL ports using this command. The VLAN name can be from 1 to 32 characters in length. If you are adding a new VLAN or modifying an existing VLAN, the VLAN number must be within the range of 1 to 4094.

If you use the **rspan** keyword for remote SPAN VLANs, you should not configure an access port (except the remote SPAN destination ports) on these VLANs. Learning is disabled for remote SPAN VLANs.

If you use the **rspan** keyword for remote SPAN VLANs, only the **name** *name* and the **state** {**active** | **suspend**} variables are supported.

The **stemaxhop** *hopcount* parameter is valid only when defining or configuring TrCRFs.

The **bridge** *bridge_num*, **mode** *bridge_mode*, **stp** *stp_type*, and **translation** *vlan_num* keywords and values are supported only when the Catalyst 6500 series switch is used as a VTP server for Catalyst 5000 family switches in the Token Ring and FDDI networks.

You must configure a private VLAN on the supervisor engine.

Valid values for *pvlan-type* are as follows:

- **primary** specifies the VLAN as the primary VLAN in a private VLAN.
- **isolated** specifies the VLAN as the isolated VLAN in a private VLAN.
- **community** specifies the VLAN as the community VLAN in a private VLAN.
- **twoway-community** specifies the VLAN as a bidirectional community VLAN that carries the traffic among community ports and to and from community ports to and from the MSFC.
- **none** specifies that the VLAN is a normal Ethernet VLAN, not a private VLAN.

Only regular VLANs with no access ports assigned to them can be used in private VLANs. Do not use the **set vlan** command to add ports to a private VLAN; use the **set pvlan** command to add ports to a private VLAN.

VLANs 1001, 1002, 1003, 1004, and 1005 cannot be used in private VLANs.

VLANs in a suspended state do not pass packets.

To secure a range of VLANs on a Firewall Services Module, these conditions must be satisfied:

1. Port membership must be defined for the VLANs, and the VLANs must be in active state.
2. The VLANs do not have a Layer 3 interface in active state on the MSFC.
3. The VLANs are not reserved VLANs.

VLANs that do not satisfy condition number 2 in the list above are discarded from the range of VLANs that you attempt to secure on the Firewall Services Module. VLANs that meet condition number 2 and condition number 3 but do not meet condition number 1 are stored in the supervisor engine database; these VLANs are sent to the Firewall Services Module as soon as they meet condition number 1.

Starting in software release 8.4(1), the WS-X6380-NAM management port (port 2) does not have to be in the same VLAN as the sc0 interface on the switch. The **set vlan** *vlan mod/port* command can be used to put the NAM management port in any VLAN other than VLAN 1. If the **set vlan** command is not used to specify a VLAN for the NAM management port, then the NAM management port by default will be set to the same VLAN as the sc0 interface on the switch.

Examples

This example shows how to set VLAN 850 to include ports 3 through 7 on module 3:

```
Console> (enable) set vlan 850 3/3-7
VLAN 850 modified.
VLAN  Mod/Ports
---- -----------------------
850   3/4-7
Console> (enable)
```

This example shows how to set VLAN 7 as a primary VLAN:

```
Console> (enable) set vlan 7 pvlan-type primary
Console> (enable)
```

This example shows how to set VLAN 901 as an isolated VLAN:

```
Console> (enable) set vlan 901 pvlan-type isolated
Console> (enable)
```

This example shows how to set VLAN 903 as a community VLAN:

```
Console> (enable) set vlan 903 pvlan-type community
Console> (enable)
```

This example shows how to unmap all instances currently mapped to VLAN 5:

```
Console> (enable) set vlan 5 mistp-instance none
Vlan 5 configuration successful
Console> (enable)
```

This example shows how to secure a range of VLANs on a Firewall Services Module:

```
Console> (enable) set vlan 2-55 firewall-module 7
Console> (enable)
```

This example shows the message that appears when VLAN port-provisioning verification is enabled:

```
Console> (enable) set vlan 10 2/1
Port Provisioning Verification is enabled on the switch.
To move port(s) into the VLAN, use 'set vlan <vlan> <port> <vlan_name>'
command.
Console> (enable)
```

Related Commands

clear config pvlan
clear pvlan mapping
clear vlan
set pvlan
set spantree macreduction
set vlan mapping
set vlan verify-port-provisioning
show pvlan
show pvlan mapping
show vlan

8.6 EFT Copy

set vlan mapping

To map 802.1Q VLANs to ISL VLANs, use the **set vlan mapping** command.

set vlan mapping dot1q *1q_vlan_num* **isl** *isl_vlan_num*

Syntax Description

dot1q *1q_vlan_num*	Specifies the 802.1Q VLAN; valid values are from 1001 to 4094.
isl *isl_vlan_num*	Specifies the ISL VLAN; valid values are from 1 to 1000.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

VLAN and MISTP instance mapping can be set only on the switch that is in either VTP server mode or in transparent mode.

Use this feature to map 802.1Q VLANs above 1000 to ISL VLANs.

The total of all mappings must be less than or equal to eight. Only one 802.1Q VLAN can be mapped to an ISL VLAN. For example, if 802.1Q VLAN 800 has been automatically mapped to ISL VLAN 800, do not manually map any other 802.1Q VLANs to ISL VLAN 800.

You cannot overwrite existing 802.1Q VLAN mapping. If the 802.1Q VLAN number already exists, the command is aborted. You must first clear that mapping.

You cannot overwrite existing VLAN mapping. If the VLAN number already exists, the command is aborted. You must first clear that mapping.

If the VLAN number does not exist, then either of the following occurs:

- If the switch is in server or transparent mode, the VLAN is created with all default values.
- If the switch is in client mode, then the command proceeds without creating the VLAN. A warning will be given indicating that the VLAN does not exist.

If the table is full, the command is aborted with an error message indicating the table is full.

The dot1q VLANs are rejected if any extended-range VLANs are present.

You cannot enable global VLAN mapping and per-port/per-ASIC VLAN mapping simultaneously.

Examples

This example shows how to map VLAN 850 to ISL VLAN 1022:

```
Console> (enable) set vlan mapping dot1q 850 isl 1022
Vlan 850 configuration successful
Vlan mapping successful
Console> (enable)
```

This example shows the display if you enter a VLAN that does not exist:

```
Console> (enable) set vlan mapping dot1q 2 isl 1016
Vlan Mapping Set
Warning: Vlan 2 Nonexistent
Console> (enable)
```

This example shows the display if you enter an existing mapping:

```
Console> (enable) set vlan mapping dot1q 3 isl 1022
1022 exists in the mapping table. Please clear the mapping first.
Console> (enable)
```

This example shows the display if the mapping table is full:

```
Console> (enable) set vlan mapping dot1q 99 isl 1017
Vlan Mapping Table Full.
Console> (enable)
```

Related Commands

clear vlan mapping
show vlan

set vlan verify-port-provisioning

To enable or disable VLAN port-provisioning verification on all ports, use the **set vlan verify-port-provisioning** command.

set vlan verify-port-provisioning {**enable** | **disable**}

Syntax Description

enable	Enables VLAN port-provisioning verification.
disable	Disables VLAN port-provisioning verification.

Defaults

VLAN port-provisioning verification is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When VLAN port-provisioning verification is enabled, you must specify the VLAN name in addition to the VLAN number when assigning switch ports to VLANs. Because you are required to specifiy both the VLAN name and the VLAN number, this verification feature helps ensure that ports are not inadvertently placed in the wrong VLAN.

When the feature is enabled, you can still create new VLANs using the **set vlan** *vlan mod/port* command, but you cannot add additional ports to the VLAN without specifying both the VLAN number and the VLAN name. The feature does not affect assigning ports to VLANs using other features such as SNMP, dynamic VLANs, and 802.1X.

Examples

This example shows how to enable VLAN port-provisioning verification on all ports:

```
Console> (enable) set vlan verify-port-provisioning enable
Vlan verify-port-provisioning feature enabled
Console> (enable)
```

This example shows how to disable VLAN port-provisioning verification on all ports:

```
Console> (enable) set vlan verify-port-provisioning disable
vlan verify-port-provisioning feature disabled
Console> (enable)
```

Related Commands

show vlan verify-port-provisioning

set vmps config-file

To set the backup configuration file for the VLAN Membership Policy Server (VMPS), use the **set vmps config-file** command.

set vmps config-file *device*:[*filename*]

set vmps config-file auto-save {**enable** | **disable**}

Syntax Description

device:	Device name where the backup configuration is stored.
filename	(Optional) Filename of the backup configuration. See the "Usage Guidelines" section for more information.
auto-save	Specifies the feature that automatically saves the VMPS configuration.
enable	Enables the auto-save feature.
disable	Disables the auto-save feature.

Defaults

If you do not specify a *filename* argument, the filename is automatically called vmps-backup-config-database.1.

The auto-save feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can use the **set vmps config-file auto-save** command to automatically save the downloaded VMPS configuration in the local storage of the switch. If you enable the auto-save feature, the switch backs up the downloaded configuration file into the specified device with the specified filename.

If you do not specify a specific backup device or a specific backup configuration filename, the switch automatically saves the file in the following device with the following filename:

bootflash:vmps-backup-config-database.1.

Examples

This example shows how to specify a backup device and a backup filename for the VMPS configuration:

```
Console> (enable) set vmps config-file disk0:vmps_config_engineering
Vmps back-up file name is set to disk0:vmps_config_engineering
Console> (enable)
```

This example shows how to enable the feature that automatically saves the VMPS configuration:

```
Console> (enable) set vmps config-file auto-save enable
Auto save to store vmps configuration file is enabled.
Console> (enable)
```

8.6 EFT Copy

This example shows to disable the feature that automatically saves the VMPS configuration:

```
Console> (enable) set vmps config-file auto-save disable
Auto save to store vmps configuration file is disabled.
Console> (enable)
```

Related Commands

show vmps

set vmps downloadmethod

To specify whether to use TFTP or rcp to download the VMPS database, use the **set vmps downloadmethod** command.

set vmps downloadmethod {**rcp** | **tftp**} [*username*]

Syntax Description

rcp	Specifies rcp as the method for downloading the VLAN Membership Policy Server (VMPS) database.
tftp	Specifies TFTP as the method for downloading the VMPS database.
username	(Optional) Username for downloading with rcp.

Defaults

If no method is specified, TFTP will be used.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The *username* option is not allowed if you specify **tftp** as the download method.

Examples

This example shows how to specify the method for downloading the VMPS database:

```
Console> (enable) set vmps downloadmethod rcp jdoe
vmps downloadmethod : RCP
rcp vmps username   : jdoe
Console> (enable)
```

Related Commands

download
set rcp username
show vmps

set vmps downloadserver

To specify the IP address of the TFTP or rcp server from which the VMPS database is downloaded, use the **set vmps downloadserver** command.

set vmps downloadserver *ip_addr* [*filename*]

Syntax Description

ip_addr	IP address of the TFTP or rcp server from which the VMPS database is downloaded.
filename	(Optional) VMPS configuration filename on the TFTP or rcp server.

Defaults

If *filename* is not specified, the **set vmps downloadserver** command uses the default filename vmps-config-database.1.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to specify the server from which the VMPS database is downloaded and how to specify the configuration filename:

```
Console> (enable) set vmps downloadserver 192.168.69.100 vmps_config.1
IP address of the server set to 192.168.69.100
VMPS configuration filename set to vmps_config.1
Console> (enable)
```

Related Commands

download
set vmps state
show vmps

set vmps server

To configure the VMPS, use the **set vmps server** command.

set vmps server *ip_addr* [**primary**]

set vmps server retry *count*

set vmps server reconfirminterval *interval*

Syntax Description

ip_addr	IP address of the VMPS.
primary	(Optional) Specifies the device as the primary VMPS.
retry *count*	Specifies the retry interval; valid values are from 1 to 10 minutes.
reconfirminterval *interval*	Specifies the reconfirmation interval; valid values are from 0 to 120 minutes.

Defaults

If no IP address is specified, the VMPS uses the local VMPS configuration.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can specify the IP addresses of up to three VMPSs. You can define any VMPS as the primary VMPS.

If the primary VMPS is down, all subsequent queries go to a secondary VMPS. VMPS checks on the primary server's availability once every five minutes. When the primary VMPS comes back online, subsequent VMPS queries are directed back to the primary VMPS.

To use a co-resident VMPS (when VMPS is enabled in a device), configure one of the three VMPS addresses as the IP address of interface sc0.

When you specify the **reconfirminterval** *interval*, enter 0 to disable reconfirmation.

Examples

This example shows how to define a primary VMPS:

```
Console> (enable) set vmps server 192.168.10.140 primary
192.168.10.140 added to VMPS table as primary domain server.
Console> (enable)
```

This example shows how to define a secondary VMPS:

```
Console> (enable) set vmps server 192.168.69.171
192.168.69.171 added to VMPS table as backup domain server.
Console> (enable)
```

Related Commands

clear vmps server
show vmps

set vmps state

To enable or disable VMPS, use the **set vmps state** command.

set vmps state {**enable** | **disable**}

Syntax Description

enable	Enables VMPS.
disable	Disables VMPS.

Defaults

By default, VMPS is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Before using the **set vmps state** command, you must use the **set vmps tftpserver** command to specify the IP address of the server from which the VMPS database is downloaded.

Examples

This example shows how to enable VMPS:

```
Console> (enable) set vmps state enable
Vlan membership Policy Server enabled.
Console> (enable)
```

This example shows how to disable VMPS:

```
Console> (enable) set vmps state disable
All the VMPS configuration information will be lost and the resources released on disable.
Do you want to continue (y/n[n]):y
VLAN Membership Policy Server disabled.
Console> (enable)
```

Related Commands

download
show vmps

set vtp

To set the options for VTP, use the **set vtp** command.

set vtp domain *domain_name*

set vtp mode {**client** | **server** | **transparent** | **off**} [**vlan** | **mst** | **unknown**]

set vtp passwd *passwd* [**hidden**]

set vtp pruning {**enable** | **disable**}

set vtp version {**1** | **2** | **3**}

set vtp primary [**vlan** | **mst**] [**force**]

Syntax Description

domain *domain_name*	Defines the name that identifies the VLAN management domain. The *domain_name* can be from 1 to 32 characters in length.
mode {**client** | **server** | **transparent** | **off**}	Specifies the VTP mode.
vlan	(Optional) Specifies the VLAN database.
mst	(Optional) Specifies the MST database.
unknown	(Optional) Specifies an unknown feature. See the "Usage Guidelines" section for more information.
passwd *passwd*	Defines the VTP password; the VTP password can be from 1 to 64 characters in length.
hidden	(Optional) Hides the password in the configuration. See the "Usage Guidelines" section for more information.
pruning {**enable** | **disable**}	Enables or disables VTP pruning for the entire management domain in VTP versions 1 and 2. Enables or disables VTP pruning only on the local switch in VTP version 3.
version {**1** | **2** | **3**}	Specifies the VTP version.
primary	Sets the VTP version 3 primary server.
force	(Optional) Forces the switch to be the primary server.

Defaults

The defaults are as follows:

- no domain name
- server mode
- no password
- pruning disabled
- version 1

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The following guidelines apply to VTP versions 1, 2, and 3:

- VTP supports four different modes: server, client, transparent, and off. If you make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all of the switches in the same VTP domain.
- If the VTP password has already been defined, entering **passwd 0** (zero) clears the VTP password. If you enter the **hidden** keyword after you specify the VTP password, the password does not appear in the configuration; an encrypted hexadecimal value appears in place of the password.
- If the receiving switch is in server mode and its revision number is higher than the sending switch, the configuration is not changed. If the revision number is lower, the configuration is duplicated.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.
- If the receiving switch is in server mode, the configuration is not changed.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. Make sure to make all VTP or VLAN configuration changes on a switch in server mode.
- If the receiving switch is in transparent mode, the configuration is not changed. Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to the other switches in the network.
- When you configure the VTP off mode, the switch functions the same as in VTP transparent mode except that VTP advertisements are not forwarded.
- You cannot enable VTP pruning and MISTP at the same time.
- Use the **clear config all** command to remove the domain from the switch.

Caution Be careful when you use the **clear config all** command. This command clears the entire switch configuration, not just the VTP domain.

- The **set vtp** command is not supported by the NAM.

The following guidelines apply only to VTP versions 1 and 2:

- All switches in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on switches in the same domain.
- If all switches in a VTP domain are VTP version 2-capable, you only need to enable VTP version 2 on one switch by using the **set vtp version 2** command. The version number is then propogated to other version 2-capable switches in the VTP domain.
- The **pruning** keyword is used to enable or disable VTP pruning for the entire VTP domain. VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN out a particular switch port. Use the **set vtp pruneeligible** and **clear vtp pruneeligible** commands to specify which VLANs should or should not be pruned when pruning is enabled for the domain.

The following guidelines apply only to VTP version 3:

- VTP version 3 works concurrently with VTP versisons 1 and 2. VTP version 3 is implemented independently because it only distributes a list of databases over an administrative domain. VTP version 3 does not directly handle VLANs.

- The **unknown** keyword allows you to configure the behavior of the switch databases that it cannot interpret. (These databases will be features handled by future extensions of VTP version 3). If you enter **set vtp mode transparent unknown**, packets for unknown features are flooded through the switch. If you enter **set vtp mode off unknown**, packets are dropped.
- VTP version 3 is a local configuration for the switch. Pruning does not propagate throughout the domain but only the local switch.
- MST mapping is propagated only if the switch is running VTP version 3 in software release 8.3(1). If the switch is running VTP version 3 without the MST feature and receives an MST database, it takes action based on the unknown database mode. If the unknown database mode is transparent, the switch relays the VTP version 3 packet that carries the MST database. If the unknown database mode is off, the switch drops the packet.

Note A switch running VTP version 1 or version 2 ignores the MST database that is sent by the VTP version 3 switch in the network.

Note A switch can commit any new MST mapping only if it is a primary server for the MST feature.

Examples

This example shows how to set the VTP domain name:

```
Console> (enable) set vtp domain Lab_Network
VTP domain Lab_Network modified
Console> (enable)
```

This example shows how to set the VTP mode to server mode:

```
Console> (enable) set vtp mode server
Changing VTP mode for all features
VTP3 domain Lab_Network modified
Console> (enable)
```

This example shows what happens if you try to change VTP to server or client mode and dynamic VLAN creation is enabled:

```
Console> (enable) set vtp mode server
Failed to Set VTP to Server. Please disable Dynamic VLAN Creation First.
Console> (enable)
```

This example shows how to set VTP to off mode:

```
Console> (enable) set vtp mode off
VTP domain modified
Console> (enable)
```

This example shows how to set the VTP password:

```
Console> (enable) set vtp passwd Sa7r12ah
Generating the secret associated to the password.
VTP domain pubs modified
Console> (enable)
```

This example shows how to set the VTP password and hide it in the configuration:

```
Console> (enable) set vtp passwd Sa7r12ah hidden
Generating the secret associated to the password.
The VTP password will not be shown in the configuration.
VTP domain pubs modified
Console> (enable)
```

This example shows how to set the VTP mode for the MST feature:

```
Console> (enable) set vtp mode server mst
Changing VTP mode for mst feature
VTP3 domain map1 modified
Console> (enable)
```

This example shows how to set the primary server for the MST feature:

```
Console> (enable) set vtp primary mst
This switch is becoming primary server for feature mst.
Do you want to continue (y/n) [n]? y
Console> (enable)
```

Related Commands

clear vlan
clear vtp pruneeligible
set vlan
set vtp pruneeligible
show vlan
show vtp domain

set vtp pruneeligible

To specify which VTP domain VLANs are pruning eligible, use the **set vtp pruneeligible** command.

set vtp pruneeligible *vlans*

Syntax Description

vlans	Range of VLAN numbers; valid values are from 2 to 1000.

Defaults

The default is VLANs 2 through 1000 are eligible for pruning.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN out a particular switch port. Use the **set vtp** command to enable VTP pruning.

By default, VLANs 2 through 1000 are pruning eligible. You do not need to use the **set vtp pruneeligible** command unless you have previously used the **clear vtp pruneeligible** command to make some VLANs pruning ineligible. If VLANs have been made pruning ineligible, use the **set vtp pruneeligible** command to make them pruning eligible again.

Examples

This example shows how to configure pruning eligibility for VLANs 120 and 150:

```
Console> set vtp pruneeligible 120,150
Vlans 120,150 eligible for pruning on this device.
VTP domain nada modified.
Console>
```

In this example, VLANs 200–500 were made pruning ineligible using the **clear vtp pruneeligible** command. This example shows how to make VLANs 220 through 320 pruning eligible again:

```
Console> set vtp pruneeligible 220-320
Vlans 2-199,220-320,501-1000 eligible for pruning on this device.
VTP domain Company modified.
Console>
```

Related Commands

clear vtp pruneeligible
set vlan
show vtp domain

set web-auth

To enable or disable web-based proxy authentication globally, use the **set web-auth** command.

set web-auth {**disable** | **enable**}

Syntax Description

disable	Disables web-based proxy authentication.
enable	Enables web-based proxy authentication.

Defaults

Disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Note If you have disabled web-based proxy authentication globally, web-based proxy authentication on a port may not start but will be stored in the configuration.

Examples

This example shows how to enable web-based proxy authentication globally:

```
Console> (enable) set web-auth enable
web-authentication successfully enabled on globally.
Console> (enable)
```

This example shows how to disable web-based proxy authentication globally:

```
Console> (enable) set web-auth disable
web-authentication successfully disabled on globally.
Console> (enable)
```

Related Commands

clear web-auth
set port web-auth
set port web-auth initialize
set web-auth login-attempts
set web-auth login-fail-page
set web-auth login-page
set web-auth quiet-timeout
set web-auth session-timeout
show port web-auth
show web-auth summary

set web-auth login-attempts

To specify the maximum number of unsuccessful login attempts allowed before blocking the user, use the **set web-auth login-attempts** command.

set web-auth login-attempts *count*

Syntax Description

count	Maximum number of unsuccessful login attempts allowed; valid values are from 3 to 10 attempts.

Defaults

3 attempts.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to specify the maximum number of login attempts:

```
Console> (enable) set web-auth login-attempts 2
web-authentication max retry count set to 2
Console> (enable)
```

Related Commands

clear web-auth
set port web-auth
set port web-auth initialize
set web-auth
set web-auth login-fail-page
set web-auth login-page
set web-auth quiet-timeout
set web-auth session-timeout
show port web-auth
show web-auth summary

8.6 EFT Copy

set web-auth login-fail-page

To configure the URL for the Login Fail page, use the **set web-auth login-fail-page** command.

set web-auth login-fail-page *url*

Syntax Description

url	Login Fail page URL.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The URL that you enter must be fewer than 256 characters and must begin with http://.

Examples

This example shows how to configure the URL for the Login Fail page:

```
Console> (enable) set web-auth login-fail-page http://proxyauth.cisco.com/login.html
web-auth login fail page configured.
Console> (enable)
```

Related Commands

clear web-auth
set port web-auth
set port web-auth initialize
set web-auth
set web-auth login-attempts
set web-auth login-page
set web-auth quiet-timeout
set web-auth session-timeout
show port web-auth
show web-auth summary

8.6 EFT Copy

set web-auth login-page

To configure the URL for the Login page, use the **set web-auth login-page** command.

set web-auth login-page url *url*

Syntax Description

url	Login page URL.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The URL that you enter must be fewer than 256 characters and must begin with http://.

Examples

This example shows how to configure the URL for the Login page:

```
Console> (enable) set web-auth login-page http://proxyauth.cisco.com/login.html
web-auth login-page configured.
Console> (enable)
```

Related Commands

clear web-auth
set port web-auth
set port web-auth initialize
set web-auth
set web-auth login-attempts
set web-auth login-fail-page
set web-auth quiet-timeout
set web-auth session-timeout
show port web-auth
show web-auth summary

set web-auth quiet-timeout

To set the quiet timeout interval for which the web-based proxy authentication is in the Held state, use the **set web-auth quiet-timeout** command.

set web-auth quiet-timeout *seconds*

Syntax Description

seconds	Quiet timeout interval; valid values are from1 to 43200 seconds.

Defaults

60 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The quiet-timeout interval is the time that the web-based proxy authentication is in the Held state after maximum authentication attempts have been exceeded.

Examples

This example shows how to set the quiet timeout interval for web-based proxy authentication:

```
Console> (enable) set web-auth session-timeout 55
web-authentication session-timeout set to 55 seconds.
Console> (enable)
```

Related Commands

clear web-auth
set port web-auth
set port web-auth initialize
set web-auth
set web-auth login-attempts
set web-auth login-fail-page
set web-auth login-page
set web-auth session-timeout
show port web-auth
show web-auth summary

8.6 EFT Copy

set web-auth session-timeout

To set the global session timeout for the web-authenticated sessions, use the **set web-auth session-timeout** command.

set web-auth session-timeout *seconds*

Syntax Description

seconds	Global session timeout interval; valid values are from 300 to 86400 seconds.

Defaults

3600 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The session-timeout interval is the time that this session is valid. The web-authenticated sessions are terminated after this timeout. The RADIUS-supplied session timeout takes precedence over the locally configured value.

Examples

This example shows how to set the global session timeout for the web-authenticated sessions:

```
Console> (enable) set web-auth session-timeout 1800
web-authentication session-timeout set to 1800 seconds.
Console> (enable)
```

Related Commands

clear web-auth
set port web-auth
set port web-auth initialize
set web-auth
set web-auth login-attempts
set web-auth login-fail-page
set web-auth login-page
set web-auth quiet-timeout
show port web-auth
show web-auth summary

show accounting

To display accounting setup and configuration information on the switch, use the **show accounting** command.

show accounting

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows the configuration details of a switch with RADIUS accounting enabled:

```
Console> (enable) show accounting
Event     Method1 Mode
-----     ------- -----
exec:     Radius  stop-only
connect:  Radius  stop-only
system:   -       -
commands:
config:   -       -
all:      -       -

TACACS+ Suppress for no username: disabled
Update Frequency: newinfo

Accounting information:
-----------------------

Active Accounted actions on tty21680592841, User NULL Priv 15
 Task ID 3, EXEC Accounting record, 0,00:00:22 Elapsed
 task_id=3 start_time=934463479 timezone=UTC service=shell

Active Accounted actions on tty01, User kannank Priv 15
 Task ID 2, EXEC Accounting record, 0,00:01:23 Elapsed
 task_id=2 start_time=934463418 timezone=UTC service=shell

Active Accounted actions on tty21680592841, User danny Priv 15
 Task ID 4, Connection Accounting record, 0,00:00:07 Elapsed
 task_id=4 start_time=934463495 timezone=UTC service=connection protocol=telnet
addr=-1407968771 cmd=telnet 172.20.25.253
```

```
Overall Accounting Traffic:
          Starts    Stops  Active
Exec      1         0       2
Connect   0         0       1
Command   0         0       0
System    0         0       0

Console> (enable)
```

This example shows the configuration details of a switch with TACACS+ accounting enabled:

```
Console> (enable) show accounting
TACACS+:
Update: periodic (25 seconds)
Supress:   disabled

           Status    Mode
           --------  -----------
exec:      disabled  stop-only
connect:   disabled  stop-only
system:    disabled  stop-only
network:   disabled  stop-only
commands:
 config:   disabled  stop-only
 all:      disabled  stop-only

Radius:
           Status    Mode
           --------  -----------
exec:      disabled  stop-only
connect:   disabled  stop-only
system:    disabled  stop-only

 TACACS+ Suppress for no username: disabled
 Update Frequency: newinfo

 Accounting information:
 -----------------------

 Active Accounted actions on tty2168059284l, User NULL Priv 15
  Task ID 3, EXEC Accounting record, 0,00:00:22 Elapsed
  task_id=3 start_time=934463479 timezone=UTC service=shell

 Active Accounted actions on tty0l, User kannank Priv 15
  Task ID 2, EXEC Accounting record, 0,00:01:23 Elapsed
  task_id=2 start_time=934463418 timezone=UTC service=shell

 Active Accounted actions on tty2168059284l, User danny Priv 15
  Task ID 4, Connection Accounting record, 0,00:00:07 Elapsed
  task_id=4 start_time=934463495 timezone=UTC service=connection protocol=telnet
addr=-1407968771 cmd=telnet 172.20.25.253

 Overall Accounting Traffic:
           Starts    Stops  Active
 Exec      1         0       2
 Connect   0         0       1
 Command   0         0       0
 System    0         0       0

Console> (enable)
```

Related Commands

set accounting commands
set accounting connect
set accounting exec
set accounting suppress
set accounting system
set accounting update

show acllog

To display the status of ACL log rate limiting, use the **show acllog** command.

show acllog

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the status of ACL log rate limiting:

```
Console> show acllog
ACL log rate limit enabled, rate = 500 pps.
Console>
```

Related Commands

clear acllog
set acllog ratelimit

show acl mac-packet-classify

To display a list of VLANs that have the MAC-based ACL feature enabled, use the **show acl mac-packet-classify** command.

show acl mac-packet-classify

Syntax Description

This command has no arguments or kewords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display VLANs with the MAC-based ACL feature enabled:

```
Console> show acl mac-packet-classify
Feature enabled on source vlan(s) 1,5.
Console>
```

Related Commands

clear acl mac-packet-classify
set acl mac-packet-classify

show aclmerge algo

To display information about the ACL merge algorithm, use the **show aclmerge algo** command.

show aclmerge algo

Syntax Description

This command has no arguments or kewords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the ACL merge algorithm currently in use:

```
Console> (enable) show aclmerge algo
Current acl merge algorithm is odm.
Console> (enable)
```

8.6 EFT Copy

show alias

To display a listing of defined command aliases, use the **show alias** command.

show alias [*name*]

Syntax Description

name	(Optional) Name of the alias to be displayed.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If *name* is not specified, all defined aliases are displayed.

Examples

This example shows how to display all aliases:

```
Console> show alias
shint           show interface
cc              clear config
shf             show flash
sip             show ip route
Console>
```

Related Commands

clear alias
set alias

show arp

To display the ARP table, use the **show arp** command.

show arp [*ip_addr* | *hostname*] [**noalias**]

Syntax Description

ip_addr	(Optional) Number of the IP address.
hostname	(Optional) Name of the host.
noalias	(Optional) Forces the display to show only IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

ARP aging time is the period of time that indicates when an ARP entry is removed from the ARP table. Set this value by entering the **set arp agingtime** command. The remaining lines of the display show the mappings of IP addresses (or IP aliases) to MAC addresses.

Use the *ip_addr* or the *hostname* options to specify an IP host when the ARP cache is large.

Examples

This example shows how to display the ARP table:

```
Console> (enable) show arp
ARP Aging time = 300 sec
+ - Permanent Arp Entries
* - Static Arp Entries
* 2.2.2.2                       at 00-08-cc-44-aa-18 on vlan 5
+ 1.1.1.1                       at 00-08-94-cc-02-aa on vlan 5
142.10.52.195                           at 00-10-07-3c-05-13 port 7/1-4 on vlan 5
192.70.31.126                           at 00-00-0c-00-ac-05 port 7/1-4 on vlan 5
121.23.79.121                           at 00-00-1c-03-00-40 port 7/1-4 on vlan 5
Console> (enable)
```

Related Commands

clear arp
set arp

show authentication

To display authentication information, use the **show authentication** command.

show authentication

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display authentication information:

```
Console> show authentication
                       Console Session   Telnet Session   Http Session
Login Authentication:
---------------------  ----------------  ---------------  -----------
tacacs                 disabled          disabled         disabled
radius                 disabled          disabled         enabled(*)
kerberos               disabled          disabled         disabled
local                  enabled(*)        enabled(*)       enabled
local                  enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          3                 3                 3
lockout timeout (sec)  disabled          disabled          disabled

Enable Authentication: Console Session   Telnet Session    Http Session
---------------------- ----------------- ----------------  ----------------
tacacs                 disabled          disabled          disabled
radius                 disabled          disabled          disabled
kerberos               disabled          disabled          disabled
local                  enabled(primary)  enabled(primary)  enabled(primary)
attempt limit          3                 3                 3
lockout timeout (sec)  disabled          disabled          disabled
Console>
```

Related Commands

set authentication enable
set authentication login

show authorization

To display authorization setup and configuration information on the switch, use the **show authorization** command.

show authorization

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display authorization setup and configuration information:

```
Console> (enable) show authorization
Telnet:
-------
            Primary   Fallback
            -------   --------
exec:       tacacs+    deny
enable:     tacacs+    deny
commands:
 config:    tacacs+    deny
 all:       -         -

Console:
--------
            Primary   Fallback
            -------   --------
exec:       tacacs+    deny
enable:     tacacs+    deny
commands:
 config:    tacacs+    deny
 all:       -         -

Console> (enable)
```

Related Commands

set authorization commands
set authorization enable
set authorization exec

8.6 EFT Copy

show autoshut

To display the automatic module shutdown configuration and current status information, use the **show autoshut** command.

show autoshut

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The run-time variable states for Ethernet modules do not synchronize with the standby supervisor engine. The output of the **show autoshut** command on a standby supervisor engine does not track with the number of resets or the reasons for the resets. If the module is powered down by the **set autoshut** command, the output stays the same.

Examples

This example shows how to display the automatic module shutdown configuration and current status information:

```
Console> show autoshut
AutoShut Frequency:     3 times
AutoShut Period:        5 minutes

Mod Autoshut Current  Number Reason for last Time of last reset
num status   status   resets reset
--- -------- -------- ------ ---------------- -------------------------
1   NA       ok      -      -               -
2   enabled  shutdown 4      inband failure  Mon Jul 14 2003, 22:55:45
3   disabled ok      0      None            -
4   enabled  ok       1     scp failure      Mon Jul 14 2003, 21:03:17
Console>
```

Related Commands

clear autoshut
set autoshut
set module autoshut

show banner

To view the message of the day (MOTD), the Catalyst 6500 series Switch Fabric Module LCD banner, and the status of the Telnet banner stored in NVRAM, use the **show banner** command.

show banner

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the MOTD, the Catalyst 6500 series Switch Fabric Module LCD banner, and the status of the Telnet banner:

```
Console> show banner
MOTD banner:

LCD config:

Telnet Banner:
disabled
Console>
```

Related Commands

set banner lcd
set banner motd
set banner telnet

show boot

To display the contents of the BOOT environment variables and the configuration register setting, use the **show boot** command.

show boot [*mod*]

Syntax Description

mod	(Optional) Number of the supervisor engine containing the Flash device.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the BOOT environment variable:

```
Console> show boot
BOOT variable = bootflash:cat6000-sup.5-5-1.bin,1;slot0:cat6000-sup.5-4-1.bin,1;
CONFIG_FILE variable = slot0:switch.cfg

Configuration register is 0x800f
ignore-config: disabled
auto-config: non-recurring, overwrite, sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console>
```

Related Commands

set boot auto-config
set boot config-register
set boot system flash

show boot device

To display the NAM boot string stored in NVRAM, use the **show boot device** command.

show boot device *mod*

Syntax Description

mod	Number of the module containing the Flash device.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported by the NAM module only.

Examples

This example shows how to display the boot device information for module 2:

```
Console> show boot device 2
Device BOOT variable = hdd:2
Console>
```

Related Commands

clear boot device
set boot device

show cam

To display CAM table entries, use the **show cam** command.

show cam {**dynamic** | **static** | **permanent** | **system**} [{*mod/port*} | *vlan*]

show cam *mac_addr* [*vlan*]

Syntax Description

dynamic	Displays dynamic CAM entries.
static	Displays static CAM entries.
permanent	Displays permanent CAM entries.
system	Displays system CAM entries.
mod/port	(Optional) Number of the module and the port on the module.
vlan	(Optional) Number of the VLAN; valid values are from 1 to 4094.
mac_addr	MAC address.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you specify a VLAN, then only those CAM entries matching the VLAN number are displayed.

If you do not specify a VLAN, all VLANs are displayed.

If the MAC address belongs to a router, it is shown by appending an “R” to the MAC address.

You can set the traffic filter for unicast addresses only; you cannot set the traffic filter for multicast addresses.

To continue displaying the entire list of CAM entries when you enter the **show cam dynamic** command, press the Y key or the space bar.

Examples

This example shows how to display dynamic CAM entries for all VLANs:

```
Console> show cam dynamic
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  -------------------------------------------
1     00-60-5c-86-5b-81    *    4/1 [ALL]
1     00-60-2f-35-48-17    *    4/1 [ALL]
1     00-80-24-f3-47-20    *    1/2 [ALL]
1     00-60-09-78-96-fb    *    4/1 [ALL]
```

```
1     00-80-24-1d-d9-ed    *    1/2 [ALL]
1     00-80-24-1d-da-01    *    1/2 [ALL]
1     08-00-20-7a-63-01    *    4/1 [ALL]

Total Matching CAM Entries Displayed = 7
Console>
```

This example shows how to display dynamic CAM entries for VLAN 1:

```
Console> show cam dynamic 1
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des  [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------  -----  -------------------------------------------
1     00-40-0b-60-d7-3c           2/1-2 [IP]
1     00-e0-34-8b-d3-ff           2/1-2 [IP]
1     00-e0-14-0f-df-ff           2/1-2 [IP]
1     00-00-0c-35-7f-42           2/1-2 [IP]
1     00-90-6f-a3-bb-ff           2/1-2 [IP]
1     00-e0-8f-63-7f-ff           2/1-2 [IP]
1     00-00-0c-35-7f-42           2/1-2 [GROUP]
.
. Display truncated
.
1     00-e0-f9-c8-33-ff           2/1-2 [IP]
Console>
```

This example shows routers listed as the CAM entries:

```
Console> show cam 00-00-81-01-23-45
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry
X = Port Security Entry

Router Watergate with IP address 172.25.55.1 has CAM entries:
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  -------------------------------------------
1     00-00-81-01-23-45R    *    2/9 [IP]
2     00-00-81-01-23-45R    *    2/10 [IP]
Total Matching CAM Entries = 2
Console>

Console> (enable) show cam 00-00-81-01-23-45
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  -------------------------------------------
1     00-00-81-01-23-45R    *    FILTER
Console>
```

Related Commands

clear cam
set cam
show cam agingtime
show config

show cam agingtime

To display CAM aging time information for all configured VLANs, use the **show cam agingtime** command.

show cam agingtime [*vlan*]

Syntax Description

vlan	(Optional) Number of the VLAN or range of VLANs; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display CAM aging time information:

```
Console> show cam agingtime
VLAN   1 aging time = 300 sec
VLAN   3 aging time = 300 sec
VLAN   5 aging time = 300 sec
VLAN   9 aging time = 300 sec
VLAN 100 aging time = 300 sec
VLAN 200 aging time = 300 sec
VLAN 201 aging time = 300 sec
VLAN 202 aging time = 300 sec
VLAN 203 aging time = 300 sec
Console>
```

This example shows how to display CAM aging time information for a specific VLAN:

```
Console> show cam agingtime 1005
VLAN 1005 aging time = 300 sec
Console>
```

Related Commands

clear cam
set cam
show cam

show cam count

To display the number of CAM entries only, use the **show cam count** command.

show cam count {**dynamic** | **static** | **permanent** | **system**} [*vlan*]

Syntax Description

dynamic	Displays dynamic CAM entries.
static	Displays static CAM entries.
permanent	Displays permanent CAM entries.
system	Displays system CAM entries.
vlan	(Optional) Number of the VLAN; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a VLAN, all VLANs are displayed.

Examples

This example shows how to display the number of dynamic CAM entries:

```
Console> (enable) show cam count dynamic
Total Matching CAM Entries = 6
Console> (enable)
```

Related Commands

clear cam
set cam

show cam monitor

To display the global configuration for CAM monitoring or the configuration for specific interfaces, use the **show cam monitor** command.

show cam monitor [*mod/ports* | *vlan* | **all**]

Syntax Description

mod/ports	(Optional) Number of the module and ports on the module.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
all	(Optional) Displays monitoring configuration on all interfaces.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod/port* or *vlan* argument or the **all** keyword, the global CAM monitoring configuration displays.

Examples

This example shows how to display the global CAM monitoring configuration:

```
Console> show cam monitor
Cam monitor global configuration:
enabled  : TRUE
interval : 20
Console>
```

This example shows how to display the CAM monitoring configuration on all interface:

```
Console> show cam monitor all

mod/port Enabled  Low        Low        High       High       No. of
                  Threshold  Action     Threshold  Action     mac addrs
------------------------------------------------------------------------------
  3/1          Y        500  warning        28000  shutdown           0
Console>
```

Related Commands

clear cam monitor
set cam monitor

8.6 EFT Copy

show cam msfc

To display the router's MAC-VLAN entries, use the **show cam msfc** command.

show cam msfc {*mod*} [*vlan*]

Syntax Description

mod	Number of the module for which MSFC information is displayed.
vlan	(Optional) Number of the VLAN; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you specify the VLAN, only CAM entries that belong to that VLAN are displayed.

Examples

This example shows how to display all CAM entries:

```
Console> (enable) show cam msfc
VLAN  Destination MAC      Destination-Ports or VCs        Xtag  Status
----  ------------------   ------------------------------  ----  ------
194   00-e0-f9-d1-2c-00R   7/1                             2     H
193   00-00-0c-07-ac-c1R   7/1                             2     H
193   00-00-0c-07-ac-5dR   7/1                             2     H
202   00-00-0c-07-ac-caR   7/1                             2     H
204   00-e0-f9-d1-2c-00R   7/1                             2     H
195   00-e0-f9-d1-2c-00R   7/1                             2     H
192   00-00-0c-07-ac-c0R   7/1                             2     H
192   00-e0-f9-d1-2c-00R   7/1                             2     H
204   00-00-0c-07-ac-ccR   7/1                             2     H
202   00-e0-f9-d1-2c-00R   7/1                             2     H
Total Matching CAM Entries Displayed = 14
Console> (enable)
```

This example shows how to display CAM entries for a specific VLAN:

```
Console> show cam msfc 15 192
VLAN  Destination MAC      Destination-Ports or VCs        Xtag  Status
----  ------------------   ------------------------------  ----  ------
192   00-00-0c-07-ac-c0R   7/1                             2     H
192   00-e0-f9-d1-2c-00R   7/1                             2     H
Console>
```

Related Commands

show cam

show cam notification

To display the status of CAM table notifications, notification intervals, MAC addresses added and deleted, and MAC move counters statistics, use the **show cam notification** command.

show cam notification {**all** | **counters** | **enable** | **historysize** | **interval** | **move** | **threshold** | *mod/port*}

show cam notification history [{[**-**]*number_of_log_entries*}]

show cam notification move counters [*vlan*]

Syntax Description

all	Displays the CAM notification counters, enable, interval, and historysize information.
counters	Displays CAM notification counter information.
enable	Displays CAM notification feature information.
historysize	Displays the size of the CAM notification log.
interval	Displays the CAM notification interval.
move	Displays MAC move notification status.
threshold	Displays CAM usage monitoring status and parameters.
mod/port	Number of the module and port.
history	Displays CAM notification history logs.
-	(Optional) Specifies the most recent log entries.
number_of_log_entries	(Optional) Number of the CAM notification log entries to display; if a CAM notification log number is not specified, the entire log is displayed.
move counters	Displays MAC move statistics.
vlan	(Optional) Number of the VLAN; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The MAC move counter records a maximum of 1000 MAC moves per VLAN only. Once this maximum has been exceeded, new moves are not recorded on the VLAN. You can enter the **clear cam notification move counters** command to clear the counters.

Due to differences between the CPU and the ASIC processing speed differences, the number of moves reported by the MAC move counter may differ from the actual number of MAC moves.

MAC move counter notification is not supported on EARL 4 and earlier.

Examples

This example shows how to display CAM notification counters:

```
Console> show cam notification counters
MAC addresses added = 3
MAC addresses removed = 5
MAC addresses added overflowed = 0
MAC addresses removed overflowed = 0
MAC address SNMP traps generated = 0
Console>
```

This example shows how to display CAM notification feature information:

```
Console> show cam notification enable
MAC address change detection enabled
Console>
```

This example shows how to display CAM notification information for ports 1-6 on module 2:

```
Console> show cam notification 2/1-6
Mod/Port   Added     Removed
---------  --------  --------
2/1        enabled   disabled
2/2        enabled   disabled
2/3        enabled   enabled
2/4        enabled   enabled
2/5        disabled  enabled
2/6        disabled  enabled
Console>
```

This example shows how to display CAM notification intervals:

```
Console> show cam notification interval
CAM notification interval = 10 second(s).
Console>
```

This example shows how to display CAM notification history information:

```
Console> show cam notification history
Index Timestamp  Operation Address           Vlan Mod/Port
===============================================================================
    4  16676708  Unlearned 00:00:00:00:00:64    2 2/6
                 Unlearned 00:00:00:00:00:63    2 2/6
                 Unlearned 00:00:00:00:00:62    2 2/6
                 Learned   00:00:00:00:00:61    2 2/4
                 Learned   00:00:00:00:00:60    2 2/4
                 Unlearned 00:00:00:00:00:5f    2 2/4
                 Unlearned 00:00:00:00:00:5e    2 2/5
    5  16697903  Learned   00:00:00:00:00:1a    1 2/1
Console>
```

This example shows how to display CAM notification history size information:

```
Console> show cam notification historysize
MAC address change history log size = 300
Console>
```

This example shows how to display CAM notification configuration information:

```
Console> show cam notification all
MAC address change detection enabled
CAM notification interval = 15 second(s).
MAC address change history log size = 1
MAC addresses added = 22936547
MAC addresses removed = 262132
MAC addresses added overflowed = 0
MAC addresses removed overflowed = 0
MAC address SNMP traps generated = 0
MAC address move notification disabled
CAM notification threshold disabled
CAM notification threshold limit = 100%
CAM notification threshold interval = 120 seconds
Console>
```

This example shows the output of the **show cam notification move counters** command when MMC is disabled:

```
Console> show cam notification move counters
MAC move counters are disabled
Console>
```

This example shows the output of the **show cam notification move counters** command when MMC is enabled and no entries are present:

```
Console> show cam notification move counters
No entries found
Console>
```

This example shows the output of the **show cam notification move counters** command when you do not specify a VLAN:

```
Console> show cam notification move counters
MAC move statistics of all the Vlans will be displayed
Console>
```

This example shows the output of the **show cam notification move counters** command when MMC is enabled:

```
Console> show cam notification move counters
-----------------------------------------------------------------------------------
 Vlan   Mac Address          From Mod/Port            To Mod/Port           Count
 ---- ----------------- ----------------------- ----------------------- ------------
    1 00-01-02-04-04-01                     2/3                     3/1        10
  200 00-01-05-03-02-01                     5/3                     5/1        20
Console>
```

This example shows the output when you specify a VLAN:

```
Console> show cam notification move counters 1
-----------------------------------------------------------------------------------
 Vlan   Mac Address          From Mod/Port            To Mod/Port           Count
 ---- ----------------- ----------------------- ----------------------- ------------
    1 00-01-02-04-04-01                     2/3                     3/1        15
6.2.2.4 From Mod/Port is part of an EtherChannel
Console>
```

This example shows the output when the To Mod/Port is part of an EtherChannel:

```
Console> show cam notification move counters
-----------------------------------------------------------------------------------
 Vlan   Mac Address          From Mod/Port            To Mod/Port           Count
 ---- ----------------- ----------------------- ----------------------- ------------
    1 00-01-02-07-08-01                     3/1         2/1,2/3,2/5,2/7        10
Console>
```

8.6 EFT Copy

This example shows the output when both the From Mod/Port and To Mod/Port are part of an EtherChannel:

```
Console> show cam notification move counters
---------------------------------------------------------------------------------
 Vlan   Mac Address            From Mod/Port            To Mod/Port           Count
 ---- ----------------- ----------------------- ----------------------- ------------
    1 00-01-02-06-08-01         3/1,3/3,3/5,3/7         2/1,2/3,2/5,2/7        15
Console>
```

Related Commands

clear cam
clear cam notification
set cam
set cam notification
set snmp trap
show cam

show cdp

To display Cisco Discovery Protocol (CDP) information, use the **show cdp** command.

show cdp

show cdp neighbors [*mod*[/*port*]] [**vlan** | **duplex** | **capabilities** | **detail**]

show cdp neighbors exclude ip-phone

show cdp port [*mod*[/*port*]]

Syntax Description

neighbors	Shows CDP information for Cisco products connected to the switch.
[*mod*[/*port*]]	(Optional) Number of the module for which CDP information is displayed and optionally, the number of the port for which CDP information is displayed.
vlan	(Optional) Shows the native VLAN number for the neighboring Cisco products.
duplex	(Optional) Shows the duplex type of the neighboring Cisco products.
capabilities	(Optional) Shows the capability codes for the neighboring Cisco products; valid values are **R**, **T**, **B**, **S**, **H**, **I**, and **r** (R = Router, T = Trans Bridge, B = Source Route Bridge, S = Switch, H = Host, I = IGMP, and r = Repeater).
detail	(Optional) Shows detailed information about neighboring Cisco products.
exclude ip-phone	Excludes IP phone information from the display of neighboring Cisco products.
port	Shows CDP port settings.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The per-port output of the **show cdp port** command is not displayed if you globally disable CDP. If you globally enable CDP, the per-port status is displayed.

If you enter the **show cdp neighbors** command for a device that supports earlier versions of CDP, “unknown” is displayed in the VTP Management Domain, Native VLAN, and Duplex fields.

Examples

This example shows how to display CDP information for the system:

```
Console> show cdp
CDP                 :enabled
Message Interval    :60
Hold Time           :180
```

This example shows how to display detailed CDP neighbor information. The display varies depending on your network configuration at the time you run the command.

```
Console> show cdp neighbors 4 detail
Port (Our Port):4/4
Device-ID:69046406
Device Addresses:
  IP Address:172.20.25.161
Holdtime:150 sec
Capabilities:TRANSPARENT_BRIDGE SWITCH
Version:
  WS-C6009 Software, Version NmpSW: 5.4(1)CSX
  Copyright (c) 1995-1999 by Cisco Systems
Port-ID (Port on Device):4/8
Platform:WS-C6009
VTP Management Domain:unknown
Native VLAN:1
Duplex:half
Console>
```

This example shows how to display CDP information about neighboring systems:

```
Console> show cdp neighbors
* - indicates vlan mismatch.
# - indicates duplex mismatch.

Port     Device-ID                       Port-ID                   Platform
-------- ------------------------------- ------------------------- ------------
3/5      002267619                       3/6 *                     WS-C6000
3/6      002267619                       3/5                       WS-C6000
4/1      002267619                       4/2                       WS-C6000
4/2      002267619                       4/1 #                     WS-C6000
4/20     069000057                       8/5                       WS-C6000
5/1      005763872                       2/1                       WS-C6009
5/1      066506245                       2/1                       WS-C6009
5/1      066508595                       5/12 *#                   WS-C6009
5/1      066508596                       5/1                       WS-C6009
Console>
```

This example shows how to display duplex information about neighboring systems:

```
Console> show cdp neighbors duplex
* - indicates vlan mismatch.
# - indicates duplex mismatch.

Port     Device-ID                       Port-ID                   Duplex
-------- ------------------------------- ------------------------- ------
3/5      002267619                       3/6 *                     half
3/6      002267619                       3/5                       half
4/1      002267619                       4/2                       full
4/2      002267619                       4/1 #                     full
4/20     069000057                       8/5                       -
5/1      005763872                       2/1                       -
5/1      066506245                       2/1                       -
5/1      066508595                       5/12 *#                   half
5/1      066508596                       5/1                       half
Console>
```

This example shows how to display VLAN information about neighboring systems:

```
Console> show cdp vlan
* - indicates vlan mismatch.
# - indicates duplex mismatch.
```

```
Port     Device-ID                       Port-ID                   NativeVLAN
-------- ------------------------------- ------------------------- ----------
3/5      002267619                       3/6 *                     1
3/6      002267619                       3/5                       1
4/1      002267619                       4/2                       1
4/2      002267619                       4/1 #                     1
4/20     069000057                       8/5                       -
5/1      005763872                       2/1                       -
5/1      066506245                       2/1                       -
5/1      066508595                       5/12 *#                   1
5/1      066508596                       5/1                       1
Console>
```

This example shows how to display capability information about neighboring systems:

```
Console> (enable) show cdp neighbors capabilities
* - indicates vlan mismatch.
# - indicates duplex mismatch.
Capability Codes:R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Port     Device-ID                       Port-ID Capabilities
-------- ------------------------------- ------------------------- ------------
 4/30    TBA04200588                     4/34                      T S I
 4/31    TBA04200588                     4/35                      T S I
 4/32    TBA04200588                     4/36                      T S I
 4/33    TBA04200588                     4/37                      T S I
 4/34    TBA04200588                     4/38                      T S I
 4/35    TBA04200588                     4/39                      T S I
 4/36    TBA04200588                     4/40                      T S I
 4/45    19991108                        4/46                      T S I
 4/46    19991108                        4/45                      T S I
 5/1     TBA04200588                     1/2                       T S I
 5/2     TBA04200588                     1/1                       T S I
 5/3     TBA04200588                     2/1                       T S I
Console> (enable)
```

This example shows how to display CDP information for all ports:

```
Console> show cdp port
CDP               :enabled
Message Interval  :60
Hold Time         :180

Port      CDP Status
--------  ----------
 2/1      enabled
 2/2      enabled
 5/1      enabled
 5/2      enabled
 5/3      enabled
 5/4      enabled
 5/5      enabled
 5/6      enabled
 5/7      enabled
 5/8      enabled
Console>
```

Related Commands

set cdp

show channel

To display EtherChannel information for a channel, use the **show channel** command.

show channel [*channel_id*] [**info** | **statistics** | **mac**]

show channel [*channel_id*] [**info** [*type*]]

show channel [*channel_id* | **all**] **protocol**

Syntax Description

channel_id	(Optional) Number of the channel.
info	(Optional) Displays channel information.
statistics	(Optional) Displays statistics about the port (PAgP packets sent and received).
mac	(Optional) Displays MAC information about the channel.
type	(Optional) Displays feature-related parameters; valid values are **spantree**, **trunk**, **protcol**, **gmrp**, **gvrp**, **qos**, **rsvp, cops, dot1qtunnel, auxiliaryvlan**, and **jumbo**.
all	(Optional) Displays protocols of all channels.
protocol	Displays channel protocol.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify the *channel_id* value, EtherChannel information is shown for all channels.

No information is displayed if the channel specified is not in use.

If you enter the optional **info** *type*, the specified feature-related parameters are displayed in the output.

To display protocols on all channels, enter the **show channel all protocol** command.

Examples

This example shows how to display channel information for a specific channel:

```
Console> show channel 865
Channel Ports                                           Status    Channel
id                                                                Mode
------- ----------------------------------------------- --------- --------------
    865 4/1-2                                           connected desirable
                                                                  non-silent
Console>
```

This example shows how to display channel information for all channels:

```
Console> show channel
Channel Id   Ports
-----------  -----------------------------------------------
768          2/1-2
769          4/3-4
770          4/7-8
Console>
```

This example shows how to display port information for a specific channel:

```
Console> show channel 769
Chan Port  Port     Portfast Port    Port
id         priority          vlanpri vlanpri-vlans
---- ----- -------- -------- ------- ------------------------------------------
769  1/1         32  disabled       0
769  1/2         32  disabled       0

Chan Port  IP       IPX      Group
id
---- ----- -------- -------- --------
769  1/1   on       auto-on  auto-on
769  1/2   on       auto-on  auto-on

Chan Port  GMRP     GMRP         GMRP
id         status   registration forwardAll
---- ----- -------- ------------ ----------
769  1/1   enabled  normal       disabled
769  1/2   enabled  normal       disabled

Chan Port  GVRP     GVRP          GVRP
id         status   registeration applicant
---- ----- -------- ------------- ---------
 769  1/1  disabled normal        normal
 769  1/2  disabled normal        normal

Chan Port  Qos-Tx Qos-Rx Qos-Trust    Qos-DefCos Qos-Port-based
id
---- ----- ------ ------ ------------ ---------- --------------
 769  1/1  2q2t   1q4t   untrusted             0 false
 769  1/2  2q2t   1q4t   untrusted             0 false

Chan Port  ACL name                         Protocol
id
---- ----- -------------------------------- --------
 769  1/1                                   IP
                                            IPX
                                            MAC
 769  1/2                                   IP
                                            IPX
                                            MAC
Console>
```

This example shows how to display port information for all channels:

```
Console> show channel info
Chan Port  Status     Channel   Admin Speed Duplex Vlan PortSecurity/
id                    mode      group                   Dynamic Port
---- ----- ---------- --------- ----- ----- ------ ---- -------------
 769  1/1  notconnect on          195 1000  full      1 -
 769  1/2  notconnect on          195 1000  full      1 -
 865  4/1  notconnect on          194 100   half      1 -
 865  4/2  notconnect on          194 100   half      1 -
```

```
Chan Port  if-   Oper-group Neighbor   Chan  Oper-Distribution
id         Index            Oper-group cost  Method
---- ----- ----- ---------- ---------- ----- -----------------
 769  1/1  -              1                0 ip both
 769  1/2  -              1                0 ip both
 865  4/1  -              1                0 ip both
 865  4/2  -              1                0 ip both

Chan Port  Device-ID                       Port-ID                   Platform
id
---- ----- ------------------------------- ------------------------- ----------
 769  1/1
 769  1/2
 865  4/1
 865  4/2

Chan Port  Trunk-status Trunk-type    Trunk-vlans
id
----- ----- ------------ ------------- -----------------------------------------
 769  1/1   not-trunking negotiate     1-1005
 769  1/2   not-trunking negotiate     1-1005
 865  4/1   not-trunking negotiate     1-1005
 865  4/2   not-trunking negotiate     1-1005

.
.
.
Console>
```

This example shows how to display PAgP information for all channels:

```
Console> show channel statistics
Port  Channel PAgP Pkts   PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts
       id      Transmitted Received  InFlush   RetnFlush OutFlush  InError
----- ------- ----------- --------- --------- --------- --------- ---------
 2/1      768           0         0         0         0         0         0
 2/2      768           0         0         0         0         0         0
 4/3      769           0         0         0         0         0         0
 4/4      769           0         0         0         0         0         0
 4/7      770           0         0         0         0         0         0
 4/8      770           0         0         0         0         0         0
Console>
```

This example shows how to display PAgP information for a specific channel:

```
Console> show channel 768 statistics
Port  Channel PAgP Pkts   PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts
       id      Transmitted Received  InFlush   RetnFlush OutFlush  InError
----- ------- ----------- --------- --------- --------- --------- ---------
 2/1      768           0         0         0         0         0         0
 2/2      768           0         0         0         0         0         0
Console>
```

This example shows how to display statistics for a specific channel:

```
Console> show channel 768 mac
Channel  Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
768                       525                  959                  827

Channel  Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
768                       384                   88                    1
```

```
Port     Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------
768                    469263                48083

Channel  Dely-Exced MTU-Exced  In-Discard Lrn-Discrd In-Lost    Out-Lost
-------- ---------- ---------- ---------- ---------- ---------- ----------
768               0          0          0          0          0          0
Console>
```

This example shows how to display statistics for all channels:

```
Console> show channel mac
Channel  Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
 -------- -------------------- -------------------- --------------------
 768                    532290                  163                    6
 769                         0                    0                    0
 771                         4                   64                    0

 Channel  Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
 -------- -------------------- -------------------- --------------------
 768                    602591                   77                    3
 769                         0                    0                    0
 771                    636086                  222                   12

 Port     Rcv-Octet            Xmit-Octet
 -------- -------------------- --------------------
 768                  44873880             45102132
 769                         0                    0
 771                     64153             64831844

 Channel  Dely-Exced MTU-Exced  In-Discard Lrn-Discrd In-Lost    Out-Lost
 -------- ---------- ---------- ---------- ---------- ---------- ----------
 768               0          0          0          0          0          0
 769               0          0          0          0          0          0
 771               0         18          0          0          0          0
Last-Time-Cleared
--------------------------
Wed Jun 10 1999, 20:31:13
Console>
```

These examples show how to display feature-specific parameter information:

```
Console> show channel 769 info trunk
Chan Port  Trunk-status Trunk-type    Trunk-vlans
id
----- ----- ------------ ------------- -----------------------------------------
769  1/1  not-trunking negotiate     1-1005
769  1/2  not-trunking negotiate     1-1005

Chan Port  Portvlancost-vlans
id
---- ----- ---------------------------------------------------------------------
769  1/1
769  1/2
Console>
Console> show channel 769 info spantree
Chan Port  Port     Portfast Port    Port
id         priority          vlanpri vlanpri-vlans
---- ----- -------- -------- ------- ------------------------------------------
769  1/1        32 disabled       0
769  1/2        32 disabled       0
Console>
Console> show channel 769 info protcol
Chan Port  IP       IPX      Group
id
---- ----- -------- -------- --------
769  1/1  on       auto-on  auto-on
769  1/2  on       auto-on  auto-on
Console>

Console> show channel 769 info gmrp
Chan Port  GMRP     GMRP         GMRP
id         status   registration forwardAll
---- ----- -------- ------------ ----------
769  1/1  enabled  normal       disabled
769  1/2  enabled  normal       disabled
Console>

Console> show channel 769 info gvrp
Chan Port  GVRP     GVRP          GVRP
id         status   registeration applicant
---- ----- -------- ------------- ---------
769  1/1  disabled normal       normal
769  1/2  disabled normal       normal
Console>

Console> show channel 769 info qos
Chan Port  Qos-Tx   Qos-Rx   Qos-Trust    Qos-DefCos Qos-Interface
id         PortType PortType Type                    Type
---- ----- -------- -------- ------------ ---------- --------------
769  1/1   2q2t     1q4t     untrusted             0 port-based
769  1/2   2q2t     1q4t     untrusted             0 port-based

Chan Port  ACL name                         Type
id
---- ----- -------------------------------- ----
769  1/1                                    IP
                                            IPX
                                            MAC
769  1/2                                    IP
                                            IPX
                                            MAC
Console>
```

Related Commands

show channel group
show port channel

show channel group

To display EtherChannel group status information, use the **show channel group** command.

show channel group [*admin_group*] [**info** | **statistics**]

show channel group [*admin_group*] [**info** [*type*]]

Syntax Description

admin_group	(Optional) Number of the administrative group; valid values are from 1 to 1024.
info	(Optional) Displays group information.
statistics	(Optional) Displays statistics about the group.
type	(Optional) Displays feature-related parameters; valid values are **spantree**, **trunk**, **protcol**, **gmrp**, **gvrp**, **qos**, **rsvp, cops, dot1qtunnel, auxiliaryvlan**, and **jumbo**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify the *admin_group* value, EtherChannel information is shown for all administrative groups.

If you enter the optional **info** *type*, the specified feature-related parameters are displayed in the output.

Examples

This example shows how to display Ethernet channeling information for all administrative groups:

```
Console> show channel group
Admin Group  Ports
-----------  ----------------------------------------------
7            1/1-2
Console>
```

This example shows how to display Ethernet channeling information for a specific group:

```
Console> show channel group 154
Admin Port  Status     Channel   Channel
group                  Mode      id
----- ----- ---------- --------- --------
  154  1/1  notconnect on             769
  154  1/2  connected  on             769
```

```
Admin Port  Device-ID                       Port-ID                   Platform
group
----- ----- ------------------------------ ------------------------- ----------
 154  1/1
  154  1/2    066510644(cat26-lnf(NET25))        2/1                        WS-C5505
Console>
```

This example shows how to display group information:

```
Console> show channel group 154 info
Admin Port  Status     Channel   Ch    Speed Duplex Vlan PortSecurity/
group                  mode      id                        Dynamic Port
----- ----- ---------- --------- ----- ----- ------ ---- -------------
  154  1/1  notconnect on          769 1000  full      1 - Dynamic port
  154  1/2  connected  on          769 1000  full      1 - Dynamic port

Admin Port  if-   Oper-group Neighbor   Chan  Oper-Distribution
group       Index            Oper-group cost  Method
----- ----- ----- ---------- ---------- ----- -----------------
  154  1/1  -              1                0 mac both
  154  1/2  868            1                0 mac both

Admin Port  Device-ID                       Port-ID                   Platform
group
----- ----- ------------------------------- ------------------------- ----------
  154  1/1
  154  1/2  066510644(cat26-lnf(NET25))     2/1                       WS-C5505

Admin Port  Trunk-status Trunk-type    Trunk-vlans
group
----- ----- ------------ ------------- -----------------------------------------
  154  1/1  not-trunking negotiate     1-1005
  154  1/2  not-trunking negotiate     1-1005

Admin Port  Portvlancost-vlans
group
----- ----- --------------------------------------------------------------------
  154  1/1
  154  1/2

Admin Port  Port     Portfast Port    Port
group       priority          vlanpri vlanpri-vlans
----- ----- -------- -------- ------- ------------------------------------------
  154  1/1        32 disabled       0
  154  1/2        32 disabled       0

Admin Port  IP       IPX      Group
group
----- ----- -------- -------- --------
  154  1/1  on       auto-on  auto-on
  154  1/2  on       auto-on  auto-on

Admin Port  GMRP     GMRP         GMRP
group       status   registration forwardAll
----- ----- -------- ------------ ----------
  154  1/1  enabled  normal       disabled
  154  1/2  enabled  normal       disabled

Admin Port  GVRP     GVRP          GVRP
group       status   registeration applicant
----- ----- -------- ------------- ---------
  154  1/1  disabled normal       normal
  154  1/2  disabled normal       normal
```

```
Admin Port  Qos-Tx Qos-Rx Qos-Trust    Qos-DefCos Qos-Port-based
group
----- ----- ------ ------ ------------ ---------- --------------
  154  1/1  2q2t   1q4t   untrusted             0 false
  154  1/2  2q2t   1q4t   untrusted             0 false

Admin Port  ACL name                         Protocol
group
----- ----- -------------------------------- --------
  154  1/1  ip_acl                           IP
            ipx_acl                          IPX
            mac_acl                          MAC
  154  1/2                                   IP
                                             IPX
                                             MAC
Console>
```

These examples show how to display feature-specific parameter information:

```
Console> show channel group 154 info trunk
Admin Port  Trunk-status Trunk-type    Trunk-vlans
group
----- ----- ------------ ------------- -----------------------------------------
  154  1/1  not-trunking negotiate     1-1005
  154  1/2  not-trunking negotiate     1-1005
Console>

Console> show channel group 154 info spantree
Admin Port  Portvlancost-vlans
group
----- ----- --------------------------------------------------------------------
  154  1/1
  154  1/2

Admin Port  Port     Portfast Port    Port
group       priority          vlanpri vlanpri-vlans
----- ----- -------- -------- ------- ------------------------------------------
  154  1/1        32 disabled       0
  154  1/2        32 disabled       0
Console>

Console> show channel group 154 info protcol
Admin Port  IP       IPX      Group
group
----- ----- -------- -------- --------
  154  1/1  on       auto-on  auto-on
  154  1/2  on       auto-on  auto-on
Console>

Console> show channel group 154 info gmrp
Admin Port  GMRP     GMRP         GMRP
group       status   registration forwardAll
----- ----- -------- ------------ ----------
  154  1/1  enabled  normal       disabled
  154  1/2  enabled  normal       disabled
Console>
Console> show channel group 154 info gvrp
Admin Port  GVRP     GVRP          GVRP
group       status   registeration applicant
----- ----- -------- ------------- ---------
  154  1/1  disabled normal       normal
  154  1/2  disabled normal       normal
Console>
```

```
Console> show channel group 769 info qos
Chan Port  Qos-Tx   Qos-Rx   Qos-Trust    Qos-DefCos Qos-Interface
id         PortType PortType Type                    Type
---- ----- -------- -------- ------------ ---------- --------------
769  1/1  2q2t     1q4t     untrusted             0 port-based
769  1/2  2q2t     1q4t     untrusted             0 port-based

Chan Port  ACL name                         Type
id
---- ----- -------------------------------- ----
769  1/1                                    IP
                                            IPX
                                            MAC
769  1/2                                    IP
                                            IPX
                                            MAC
Console>
```

Related Commands

show channel
show port channel

show channel hash

To display the channel port the traffic goes to based on the current channel distribution mode, use the **show channel hash** command.

show channel hash *channel_id src_ip_addr* [*dest_ip_addr*]

show channel hash *channel_id dest_ip_addr*

show channel hash *channel_id src_mac_addr* [*dest_mac_addr*]

show channel hash *channel_id dest_mac_addr*

show channel hash *channel_id src_port dest_port*

show channel hash *channel_id dest_port*

show channel hash *channel_id src_ip_addr vlan src_port* [*dest_ip_addr vlan dest_port*]

show channel hash *channel_id dest_ip_addr vlan dest_port*

Syntax Description

channel_id	Number of the channel.
src_ip_addr	Source IP address.
dest_ip_addr	(Optional) Destination IP address.
src_mac_addr	Source MAC address.
dest_mac_addr	(Optional) Destination MAC address.
src_port	Number of the source port; valid values are from 0 to 65535.
dest_port	Number of the destination port; valid values are from 0 to 65535.
vlan	Number of the VLAN of the packet.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify the *channel_id* value, EtherChannel information is shown for all channels.

No information is displayed if the channel specified is not in use.

Examples

This example shows how to display hash information in a channel:

```
Console> show channel hash 769 10.6.1.1 10.6.2.3
Selected channel port:1/2
Console>
```

Related Commands

set port channel

8.6 EFT Copy

show channel mac

To display MAC information in the channel, use the **show channel mac** command.

show channel mac

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display MAC information in a channel:

```
Console> (enable) show channel mac
Channel  Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------

Channel  Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------

Channel  Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------

Channel  Dely-Exced MTU-Exced  In-Discard Lrn-Discrd In-Lost    Out-Lost
-------- ---------- ---------- ---------- ---------- ---------- ----------
```

show channelprotocol

To display the channeling protocol used by each module in the system, use the **show channelprotocol** command.

show channelprotocol

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

PAgP and LACP manage channels differently. When all the ports in a channel get disabled, PAgP removes them from its internal channels list; **show** commands do not display the channel. With LACP, when all the ports in a channel get disabled, LACP does not remove the channel; **show** commands continue to display the channel even though all its ports are down. To determine if a channel is actively sending and receiving traffic with LACP, use the **show port** command to see if the link is up or down.

LACP does not support half-duplex links. If a port is in active or passive mode and becomes half duplex, the port is suspended (and a syslog message is generated). The port is shown as "connected" using the **show port** command and as "not connected" using the **show spantree** command. This discrepancy occurs because the port is physically connected, but it never joined spanning tree. If you set the duplex to full or set the channel mode to off for the port, the port will join spanning tree

For more information about PAgP and LACP, refer to the "Guidelines for Port Configuration" section of the "Configuring EtherChannel" chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example shows how to display the protocol used by each module in the system:

```
Console> show channelprotocol
        Channel
Module  Protocol
------  --------
1       LACP
2       LACP
3       PAGP
4       LACP
Console>
```

Related Commands set channelprotocol

show channel traffic

To display channel port utilization based on MAC counters, use the **show channel traffic** command.

show channel traffic [*channel_id*]

Syntax Description

channel_id	(Optional) Number of the channel.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify the *channel_id* value, EtherChannel information is shown for all channels.

No information is displayed if the channel specified is not in use.

Examples

This example shows how to display traffic information in a channel:

```
Console> show channel traffic 769
ChanId Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ ----- ------- ------- ------- ------- ------- -------
   769  1/1    0.00%   0.00%   0.00%   0.00%   0.00%   0.00%
   769  1/2  100.00% 100.00% 100.00% 100.00%   0.00%   0.00%
Console>
```

show config

To display the nondefault system or module configuration, use the **show config** command.

show config [**all**]

show config [**system** | *mod*] [**all**]

show config acl location

Syntax Description

all	(Optional) Specifies all module and system configuration information, including the IP address.
system	(Optional) Displays system configuration.
mod	(Optional) Displays module configuration.
acl location	Displays ACL configuration file location.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To view specific information within the **show config** output, if you enter /*text* and press the **Return** key at the --More-- prompt, the display starts two lines above the line containing the *text* string. If the text string is not found, “Pattern Not Found” is displayed. You can also enter “**n**” at the --More-- prompt to search for the last entered *text* string.

A comment appears in the configuration file to help you to determine where the QoS configuration originated—traditional QoS or automatic QoS.

Examples

This example shows how to display the nondefault system and module configuration:

```
Console> (enable) show config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
........
..

begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Mon Apr 17 2000, 08:33:09
!
#version 5.5(1)
#System Web Interface Version 5.0(0.25)
```

```
!
set editing disable
!
#frame distribution method
set port channel all distribution mac unknown
!
#snmp
set snmp trap 0.0.0.0
set snmp trap 0.0.0.0
!
#kerberos
set kerberos server  0.0.0.0
set kerberos server  0.0.0.0
set kerberos realm
set kerberos realm
!
#vtp
set vtp domain Lab_Network
set vtp v2 enable
set vtp pruning enable
set vlan 1 name default type ethernet mtu 1500 said 100001 state active
set vlan 2 name VLAN0002 type ethernet mtu 1500 said 100002 state active
set vlan 6 name VLAN0006 type ethernet mtu 1500 said 100006 state active
set vlan 10 name VLAN0010 type ethernet mtu 1500 said 100010 state active
set vlan 20 name VLAN0020 type ethernet mtu 1500 said 100020 state active
set vlan 50 name VLAN0050 type ethernet mtu 1500 said 100050 state active
set vlan 100 name VLAN0100 type ethernet mtu 1500 said 100100 state active
set vlan 152 name VLAN0152 type ethernet mtu 1500 said 100152 state active
set vlan 200 name VLAN0200 type ethernet mtu 1500 said 100200 state active
set vlan 300 name VLAN0300 type ethernet mtu 1500 said 100300 state active
set vlan 303 name VLAN0303 type fddi mtu 1500 said 100303 state active
set vlan 400 name VLAN0400 type ethernet mtu 1500 said 100400 state active
set vlan 500 name VLAN0500 type ethernet mtu 1500 said 100500 state active
set vlan 521 name VLAN0521 type ethernet mtu 1500 said 100521 state active
set vlan 524 name VLAN0524 type ethernet mtu 1500 said 100524 state active
set vlan 570 name VLAN0570 type ethernet mtu 1500 said 100570 state active
set vlan 801 name VLAN0801 type trbrf mtu 4472 said 100801 state active bridge
set vlan 850 name VLAN0850 type ethernet mtu 1500 said 100850 state active
set vlan 917 name VLAN0917 type ethernet mtu 1500 said 100917 state active
set vlan 999 name VLAN0999 type ethernet mtu 1500 said 100999 state active
set vlan 1002 name fddi-default type fddi mtu 1500 said 101002 state active
set vlan 1004 name fddinet-default type fddinet mtu 1500 said 101004 state acti
set vlan 1005 name trbrf-default type trbrf mtu 4472 said 101005 state active b
set vlan 802 name VLAN0802 type trcrf mtu 4472 said 100802 state active parent
set vlan 1003 name trcrf-default type trcrf mtu 4472 said 101003 state active p
set vlan 3 translation 303 translation 0
set vlan 4 translation 304 translation 0
set vlan 5 translation 305 translation 0
set vlan 303 translation 3 translation 0
set vlan 304 translation 4 translation 0
set vlan 305 translation 5 translation 0
set vlan 351 translation 524 translation 0
set vlan 524 translation 351 translation 0
!
#ip
set interface sc0 1 1.10.11.212/255.255.255.0 1.10.11.255

set ip route 0.0.0.0/0.0.0.0         172.20.52.126
set ip route 0.0.0.0/0.0.0.0         172.20.52.125
set ip route 0.0.0.0/0.0.0.0         172.20.52.121
!
```

```
#rcp
set rcp username 1
!
#dns
set ip dns server 171.68.10.70 primary
set ip dns server 171.68.10.140
set ip dns enable
set ip dns domain cisco.com
!
#spantree
set spantree fwddelay 4     801
set spantree maxage   10    801
#portfast
set spantree portfast bpdu-guard enable
#vlan 802
set spantree fwddelay 4     802
set spantree maxage   10    802
set spantree portstate 802 block 801
#vlan 1003
set spantree fwddelay 4     1003
set spantree maxage   10    1003
set spantree portstate 1003 block 1005
!
#syslog
set logging server 172.20.101.182
!
#set boot command
set boot config-register 0x100
set boot system flash bootflash:cat6000-sup.5-5-1.bin
!
#HTTP commands
set ip http server enable
set ip http port 1922
!
# default port status is disable
!
#mls
set mls nde disable
!
#qos
set qos enable
set qos map 1q4t 1 1 cos 2
set qos map 1q4t 1 1 cos 3
set qos map 1q4t 1 1 cos 4
set qos map 1q4t 1 1 cos 5
set qos map 1q4t 1 1 cos 6
set qos map 1q4t 1 1 cos 7
!
#Accounting
set accounting commands enable config stop-only tacacs+
!
# default port status is enable
!
#module 1 : 2-port 1000BaseX Supervisor
!
#module 2 empty
!
#module 3 : 48-port 10/100BaseTX (RJ-45)
set spantree portfast   3/8 enable
!
```

```
#module 4 empty
!
#module 5 : 48-port 10/100BaseTX (RJ-45)
!
#module 6 empty
!
set vlan 100  6/1
set spantree portcost    6/1  200
!
#module 7 : 24-port 10/100BaseTX Ethernet
set vlan 5    7/5
set vlan 100  7/23
set vlan 200  7/9
set port disable    7/5

set port name       7/9  1528 Hub
set port security 7/10 enable
set port security 7/10 maximum 200
set port security 7/10 00-11-22-33-44-55
set port security 7/10 00-11-22-33-44-66
set port security 7/10 00-11-22-33-44-77
set port security 7/10 violation restrict
set port security 7/10 age 30
set trunk 7/1  desirable isl 1-1005
set trunk 7/2  desirable isl 1-1005
set trunk 7/3  desirable isl 1-1005
set trunk 7/4  desirable isl 1-1005
set trunk 7/10 off negotiate 1-1005
set trunk 7/23 on isl 1-1005
set spantree portcost    7/23  150
set spantree portvlancost 7/23 cost 50 100

#port security
set port security auto-configure enable
!
#module 8 empty
!
#module 9 empty
!
#module 15 empty
!
#module 16 empty
end
Console>
```

This example shows how to display default and nondefault configuration information:

```
Console> (enable) show config all
begin
!
# ***** ALL (DEFAULT and NON-DEFAULT) CONFIGURATION *****
!
#Current time: Mon Apr 17 2000, 08:33:09
!
#version 5.51(1)
!
set password $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set enablepass $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set prompt Console>
set length 24 default
set logout 20
set banner motd ^C^C
!
```

```
#system
set system baud  9600
set system modem disable
set system name
set system location
set system contact
!
.
.
.
Console>
```

This example shows how to display nondefault system configuration information:

```
Console> (enable) show config system
begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
#time: Mon Apr 17 2000, 08:33:09
!
#version 5.5(1)
!
!
#set boot command
set boot config-register 0x2
set boot system flash bootflash:kk1
end
Console>
```

This example shows how to display all system default and nondefault configuration information:

```
Console> (enable) show config system all
begin
!
#system
set system baud  9600
set system modem disable
set system name
set system location
set system contact
!
end
Console>
```

This example shows how to display module nondefault configuration information:

```
Console> (enable) show config 1
..............
begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Mon Apr 17 2000, 08:33:09
!
#version 5.5(1)
!
!
#module 1 : 4-port 10/100BaseTX Supervisor
!
end
Console>
```

This example shows how to display the ACL configuration file location:

```
Console> (enable) show config acl location
ACL configuration is being saved in NVRAM.
Console> (enable)
```

This example shows that the QoS configuration was made through automatic QoS:

```
Console> (enable) show config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
.................


...............................

............................

..

begin
<snip>
#qos - qos configuration via autoqos
set qos enable
set qos map 2q2t tx 2 1 cos 1
set qos map 2q2t tx 2 1 cos 2
<snip>
Console> (enable)
```

Related Commands

clear config
write

show config checkpoints

To display configuration checkpoint file information, use the **show config checkpoints** command.

show config checkpoints

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The output of this command shows all configuration checkpoint filenames, the devices on which they have been saved, and the date and time when they were saved.

Examples

This example shows how to display configuration checkpoint information:

```
Console> (enable) show config checkpoints
Checkpoint          File id                                 Date
==========          =======                                 ====
CKP0_0722040712     bootflash:CKP0_07220407128.4(0.79)COC   Thu Jul 22 2000, 07:12:43
SARAH_07122002      bootflash:SARAH_071220028.4(0.79)COC    Thu Jul 22 2000, 07:19:05
Console> (enable)
```

Related Commands

clear config checkpoint
set config checkpoint
set config rollback

show config differences

To compare configuration files that are stored on the system to determine differences between configuration files or to check if changes have been made to the system configuration, use the **show config differences** command.

show config differences [**ignorecase**] [**context** [*val*]] **all** *file*

show config differences [**ignorecase**] [**context** [*val*]] *file* [*file*]

Syntax Description

ignorecase	(Optional) Ignores case sensitivity while comparing files.
context	(Optional) Displays differences with context.
val	(Optional) Number of lines of context.
all	Compares the file to both default and nondefault configurations.
file	Configuration filename.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you specify only one configuration filename, that configuration file is compared with the current configuration on the switch.

Examples

This example shows how to compare two configuration files:

```
Console> (enable) show config differences 1.cfg 2.cfg
--- bootflash:1.cfg
+++ bootflash:2.cfg
@@ -8,1 +8,1 @@
-#version 8.2(0.11-Eng)DEL
+#VERSION 8.2(0.11-eNG)del
@@ -11,1 +11,1 @@
-set config mode text auto-save interval 1
+SET CONFIG MODE TEXT AUTO-SAVE INTERVAL 1
Console> (enable)
```

This example shows how to ignore case sensitivity while comparing two files:

```
Console> (enable) show config differences ignorecase 1.cfg 2.cfg
Files bootflash:1.cfg and bootflash:2.cfg are identical
Console> (enable)
```

Related Commands

show config

show config mode

To display the system configuration mode currently running on the switch, use the **show config mode** command.

show config mode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the current system configuration mode when set to text:

```
Console> (enable) show config mode
System configuration mode set to text.
System configuration file = bootflash:switch.cfg
auto-save to nvram disabled
auto-save interval set to 45
Console> (enable)
```

This example shows how to display the current system configuration mode when set to binary:

```
Console> (enable) show config mode
System configuration mode set to binary.
auto-save to nvram disabled
auto-save interval set to 4320
Console> (enable)
```

This example shows how to display the current system configuration when the configuration mode is set to text and when the text configuration is saved in NVRAM:

```
Console> (enable) show config mode
System configuration mode set to text.
System configuration file set to nvram.
auto-save to nvram enabled
auto-save interval set to 2880
Console> (enable)
```

Related Commands

set config mode

8.6 EFT Copy

show config qos acl

To display the committed access lists in a command line format, use the **show config qos acl** command.

show config qos acl {*acl_name* | **all**}

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
all	Specifies all committed access lists.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display all committed access lists:

```
Console> show config qos acl all
#ipx1:
set qos acl ipx ipx1 dscp 1 any AA BB
set qos acl ipx ipx1 dscp 1 0 AA CC
#default-action:
set qos acl default-action ip dscp 0
set qos acl default-action ipx dscp 0
set qos acl default-action mac dscp 0
Console>
```

This example shows how to display a specific committed access list:

```
Console> show config qos acl my_ip_acl
#my_ip_acl:
set qos acl ip my_ip_acl trust-dscp microflow my-micro tcp 1.2.3.4/255.0.0.0 eq
port 21 172.20.20.1/255.255.255.0 tos 5
set qos acl ip my_ip_acl trust-dscp microflow my-micro aggregate agg tcp
173.22.3.4/255.0.0.0 eq port 19 173.22.20.1/255.255.255.0 tos 5
Console>
```

Related Commands

commit

show cops

To display COPS information, use the **show cops** command.

show cops info [**diff-serv** | **rsvp**] [**noalias**]

show cops roles

Syntax Description

info	Displays COPS status and configuration information.
diff-serv	(Optional) Specifies the differentiated services server table.
rsvp	(Optional) Specifies the RSVP server table.
noalias	(Optional) Forces the display to show only IP addresses, not IP aliases.
roles	Displays the ports assigned to each role.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

A few minutes after a switchover occurs between active and redundant supervisor engines, if you enter the **show cops roles** command, the output may be incorrect. If this is the case, the following warning is displayed:

```
COPS High Availability Switch Over in progress, hardware may be
programmed differently than as suggested by the output of these
commands.
```

Examples

This example shows how to display COPS status and configuration information:

```
Console> show cops info
COPS general configuration
---------------------------
COPS domain name            : -
Connection retry intervals  : initial   = 30 seconds
                              increment = 30 seconds
                              max       = 300 seconds
COPS Diff-Serv client state
---------------------------
COPS connection state       :not-connected
Last active server          :172.20.25.3 [port:3288]
Primary configured server   :172.20.25.3 [port:3288]
Secondary configured server :-
COPS RSVP client state
------------------------
```

```
COPS connection state       : connected
Last active server          : 171.21.34.56
Primary configured server   : 171.21.34.56 [3288]
Secondary configured server : 171.21.34.57 [3288]
Console>
```

This example shows how to display COPS RSVP status and configuration information:

```
Console> show cops info rsvp
COPS general configuration
---------------------------
COPS domain name            : -
Connection retry intervals  : initial   = 30 seconds
                              increment = 30 seconds
                              max       = 300 seconds

COPS RSVP client state
------------------------
COPS connection state       : connected
Last active server          : 171.21.34.56
Primary configured server   : 171.21.34.56 [3288]
Secondary configured server : 171.21.34.57 [3288]
Console>
```

This example shows how to display the ports assigned to each role:

```
Console> show cops roles
Admin Roles                     Mod/Ports
------------------------------- ---------------------------------------
access_port                     1/1-2,3/1-5,3/8
backbone_port                   1/1-2,3/8
branch_office_port              3/6-7,4/1-8
net_port                        -

Oper Roles                      Mod/Ports
------------------------------- ---------------------------------------
access_port                     1/1-2,3/1-5,3/8
backbone_port                   1/1-2,3/8
branch_office_port              3/6-7,4/1-8
Console>
```

This example shows how to display only IP addresses, not IP aliases:

```
Console> show cops noalias
COPS general configuration
---------------------------
COPS domain name            : -
Connection retry intervals  : initial   = 30 seconds
                              increment = 30 seconds
                              max       = 300 seconds

COPS Diff-Serv client state
---------------------------
COPS connection state       : not-connected
TCP  connection state       : not-connected
Last active server          : -
Primary configured server   : -
Secondary configured server : -
```

```
COPS RSVP client state
----------------------
COPS connection state       : not-connected
TCP  connection state       : not-connected
Last active server          : -
Primary configured server   : -
Secondary configured server : -
Console>
```

Related Commands

clear cops
set cops

show counters

To display hardware counters for a port, all ports on a module, or a supervisor engine, use the **show counters** command.

show counters {*mod* | *mod/port*}

show counters supervisor

Syntax Description

mod	Number of the module.
mod/port	Number of the module and the port.
supervisor	Displays counters for the supervisor engine.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The "Last-Time-Cleared" timestamp at the end of the **show counters** {*mod* | *mod/port*} command output is either the last time the counters were cleared on the specified port or the last time that the module was inserted or the switch was reset, whichever happened last.

Examples

This example shows how to display the counters for module 2, port 1:

Note The counters displayed may change depending on the module type queried.

```
Console> show counters 2/1
Generic counters version 1
64 bit counters
0  rxHCTotalPkts                      =            2170558
1  txHCTotalPkts                      =            2588911
2  rxHCUnicastPkts                    =            2142669
3  txHCUnicastPkts                    =            2585457
4  rxHCMulticastPkts                  =              19552
5  txHCMulticastPkts                  =               1789
6  rxHCBroadcastPkts                  =               8332
7  txHCBroadcastPkts                  =               1665
8  rxHCOctets                         =          190513843
9  txHCOctets                         =          227423299
10 rxTxHCPkts64Octets                 =              20996
11 rxTxHCPkts65to127Octets            =            4737279
12 rxTxHCPkts128to255Octets           =               1170
13 rxTxHCPkts256to511Octets           =                 16
14 rxTxHCpkts512to1023Octets          =                  8
```

```
15 rxTxHCpkts1024to1518Octets         =                    0
16 rxDropEvents                       =                    0
17 txHCTrunkFrames                    =                    0
18 rxHCTrunkFrames                    =                    0
19 rxHCDropEvents                     =                    0
32 bit counters
0  rxCRCAlignErrors                   =          0
1  rxUndersizedPkts                   =          0
2  rxOversizedPkts                    =          0
3  rxFragmentPkts                     =          0
4  rxJabbers                          =          0
5  txCollisions                       =          0
6  ifInErrors                         =          0
7  ifOutErrors                        =          0
8  ifInDiscards                       =          0
9  ifInUnknownProtos                  =          0
10 ifOutDiscards                      =          0
11 txDelayExceededDiscards            =          0
12 txCRC                              =          0
13 linkChange                         =          2
Dot3 counters version 1
0  dot3StatsAlignmentErrors           =          0
1  dot3StatsFCSErrors                 =          0
2  dot3StatsSingleColFrames           =          0
3  dot3StatsMultiColFrames            =          0
4  dot3StatsSQETestErrors             =          0
5  dot3StatsDeferredTransmisions      =          0
6  dot3StatsLateCollisions            =          0
7  dot3StatsExcessiveCollisions       =          0
8  dot3StatsInternalMacTransmitErrors =          0
9  dot3StatsCarrierSenseErrors        =          0
10 dot3StatsFrameTooLongs             =          0
11 dot3StatsInternalMacReceiveErrors  =          0
Flowcontrol counters version 1
0  txPause                            =          0
1  rxPause                            =          0
Last-Time-Cleared
--------------------------
Tue Mar 21 2000, 19:19:03
Console>
```

This example shows how to display the counters for the supervisor engine:

```
Console> show counters supervisor
Acl Manager Error Stats Counter(s)
======================================
IP checksum errors   = 00000

Forwarding Engine Error Stats Counters
======================================
IP length errors     = 0
IP too short errors  = 0
IP checksum errors   = 0
IPX length errors    = 0
IPX too short errors = 0
Console>
```

Table 2-32 describes the possible fields in the **show counters** command output.

Table 2-32 show counters Command Output Fields

Field	Description
64-bit counters	
rxHCTotalPkts	Number of packets (including bad packets, broadcast packets, and multicast packets) received on a link.
txHCTotalPkts	Number of packets (including bad packets, broadcast packets, and multicast packets) transmitted on a link.
rxHCUnicastPkts	Number of packets, delivered by this sublayer to a higher (sub)layer, which were not addressed to a multicast or broadcast address at this sublayer.
txHCUnicastPkts	Number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent.
rxHCMulticastPkts	Number of packets, delivered by this sublayer to a higher (sub)layer, which were addressed to a multicast address at this sublayer. For a MAC layer protocol, this includes both Group and Functional addresses.
txHCMulticastPkts	Number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sublayer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses.
rxHCBroadcastPkts	Number of packets, delivered by this sublayer to a higher (sub)layer, which were addressed to a broadcast address at this sublayer.
txHCBroadcastPkts	Number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sublayer, including those that were discarded or not sent.
rxHCOctets	Number of octets received on the interface, including framing characters.
txHCOctets	Number of octets transmitted out of the interface, including framing characters.
rxTxHCPkts64Octets	Number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
rxTxHCPkts65to127Octets	Number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
rxTxHCPkts128to255Octets	Number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
rxTxHCPkts256to511Octets	Number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
rxTxHCpkts512to1023Octets	Number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
rxTxHCpkts1024to1518Octets	Number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
rxDropEvents[1]	Number of events in which packets were dropped by the probe due to lack of resources.

Table 2-32 show counters Command Output Fields (continued)

Field	Description
32-bit counters	
rxCRCAlignErrors	Number of packets received that had a length (excluding framing bits, but including FCS octets) between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
rxUndersizedPkts	Number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
rxOversizedPkts	Number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well-formed.
rxFragmentPkts[2]	Number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
rxJabbers[3]	Number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
txCollisions[4]	The best estimate of the total number of collisions on this Ethernet segment. The value returned will depend on the location of the RMON probe. Section 8.2.1.3 (10BASE5) and section 10.3.1.3 (10BASE2) of IEEE standard 802.3 states that a station must detect a collision in the receive mode if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus, a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment would. Probe location plays a much smaller role when considering 10BASE-T.
ifInErrors	Number of frames received on a particular interface with the following errors: dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsFrameTooLongs, dot3StatsInternalMacReceiveErrors, and dot3StatsSymbolErrors.
ifOutErrors	Number of octets transmitted out of the interface, including framing characters.
ifInDiscards	Number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their delivery to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
ifInUnknownProtos	Number of inbound packets with unknown protocols.
ifOutDiscards	Number of inbound packets chosen to be discarded even though no errors had been detected to prevent their delivery to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
txDelayExceededDiscards	Number of frames discarded by this port due to excessive transmit delay.
txCRC	Number of CRC errors.
linkChange	Number of times the port toggled between a connect state to a non-connect state.
Dot3 counters version 1	
dot3StatsAlignmentErrors[5]	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
dot3StatsFCSErrors[6]	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.

Table 2-32 show counters Command Output Fields (continued)

Field	Description
dot3StatsSingleColFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrames object.
dot3Stats MultiColFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object.
dot3StatsSQETestErrors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
dot3StatsDeferred Transmisions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
dot3StatsLateCollisions[7]	Number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.
dot3StatsExcessiveCollisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
dot3StatsInternalMacTransmitErrors[8]	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.
dot3StatsCarrierSenseErrors	Number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
dot3StatsFrameTooLongs	A count of frames received on a particular interface that exceeds the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are counted exclusively according to the error status presented to the LLC.
dot3StatsInternalMacReceiveErrors[9]	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsFrameTooLongs object, the dot3StatsAlignmentErrors object, or the dot3StatsFCSErrors object.

Table 2-32 show counters Command Output Fields (continued)

Field	Description
dot3StatsSymbolErrors	For an interface operating at 100 Mb per second, the number of times there was an invalid data symbol when a valid carrier was present. For an interface operating in half-duplex mode at 1000 Mb per second, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII. For an interface operating in full-duplex mode at 1000 Mb per second, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII. The count represented by an instance of this object is incremented at most once per carrier event, even if multiple symbol errors occur during the carrier event. This count does not increment if a collision is present. Discontinuities in the value of this counter can occur at reinitialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Flowcontrol counters version 1	
txPause	Number of control frames transmitted at the gigabit level. This counter is valid only on a Gigabit Ethernet port.
rxPause	Number of control frames received at the gigabit level. This counter is valid only on a Gigabit Ethernet port.
rxTotalDrops	The rxTotalDrops field includes these counters: • Number of bad packets because of a CRC error, a coding violation, or a sequence error. • Number of CBL blocking drops. • Number of instances of invalid encapsulation. • Number of broadcast suppression drops. • Number of drops because the packet length is less than 64 or greater than 1518.

[1] This number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.

[2] It is entirely normal for etherStatsFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.

[3] This definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2), which define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

[4] An RMON probe inside a repeater should ideally report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.

[5] This number is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are counted exclusively according to the error status presented to the LLC.

[6] This number is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are counted exclusively according to the error status presented to the LLC.

[7] 512 bit-times corresponds to 51.2 microseconds on a 10-Mbps system. A (late) collision represented by an instance of this object is also considered as a (generic) collision for other collision-related statistics.

[8] The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface not otherwise counted.

[9] The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of receive errors on a particular interface not otherwise counted.

Related Commands

clear counters

show crypto key

To display RSA key pair information, use the **show crypto key** command.

show crypto key

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **crypto** commands are supported on systems that run these image types only:

- supk9 image—for example, cat6000-supk9.6-1-3.bin
- supcvk9 image—for example, cat6000-supcvk9.6-1-3.bin

Examples

This example shows how to display key pair information:

```
Console> (enable) show crypto key
RSA keys was generated at: Tue Dec 14 1999, 14:22:48
1024 37 1120518394839901301166714853840995094745037456682394891249441779951543727187159999
64368303391096438617934227204437132666869289489849842570531592978972460769210453547 2010393
868648783669579338660482094092720514951237657028608860832162809370173090068651870589350241
85402826063185974102411558894697025607154868421
Console> (enable)
```

Related Commands

clear crypto key rsa
set crypto key rsa

show default

To check the status of the default port status setting, use the **show default** command.

show default

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The command shows whether the **set default portstatus** command is in disable or enable mode.

Examples

This example shows how to display the status of the default port status:

```
Console> (enable) show default
portstatus: disable
Console> (enable)
```

Related Commands

set default portstatus

show dhcp-snooping bindings

To display DHCP bindings learned from DHCP snooping, use the **show dhcp-snooping bindings** command.

show dhcp-snooping bindings [*ip_addr*] [*mac_addr*] [**vlan** *vlan*] [**port** *mod/port*]

Syntax Description

ip_addr	(Optional) IP address.
mac_addr	(Optional) MAC address.
vlan *vlan*	(Optional) Specifies the VLAN.
port *mod/port*	(Optional) Specifies the module number and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **show dhcp-snooping bindings** command displays DHCP bindings gathered through DHCP snooping. If you do not enter any arguments or keywords, all DHCP bindings are displayed.

Examples

This example shows how to display DHCP binding information using a VLAN number:

```
Console> show dhcp-snooping bindings vlan 10
MacAddress          IpAddress        Lease(sec)    VLAN  Port
------------------  ---------------  ----------    ----  -----

00-01-7b-9b-05-3f   192.168.80.221   86377          10   1/8
Console>
```

This example shows how to display DHCP binding information using a port number:

```
Console> show dhcp-snooping bindings port 3/96
MAC Address         IP Address       Lease(sec)    VLAN  Port
------------------  ---------------  ----------    ----  -----------------

00-aa-06-02-00-03   192.168.80.3          86382     810   3/96
00-aa-06-02-00-09   192.168.80.9          86383     810   3/96
00-aa-06-02-00-06   192.168.80.6          86382     810   3/96
00-aa-06-02-00-05   192.168.80.5          86382     810   3/96
00-aa-06-02-00-07   192.168.80.7          86382     810   3/96
00-aa-06-02-00-0a   192.168.80.10         86383     810   3/96
00-aa-06-02-00-02   192.168.80.2          86382     810   3/96
00-aa-06-02-00-08   192.168.80.8          86382     810   3/96
00-aa-06-02-00-04   192.168.80.4          86382     810   3/96
00-aa-06-02-00-01   192.168.80.1          86381     810   3/96
Console>
```

Related Commands

clear dhcp-snooping bindings
set port dhcp-snooping

show dhcp-snooping config

To display the DHCP snooping configuration, use the **show dhcp-snooping config** command.

show dhcp-snooping config

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the DHCP snooping configuration:

```
Console> show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-d0-00-4c-1b-ff.
Console>
```

Related Commands

set dhcp-snooping
show port dhcp-snooping

show dhcp-snooping statistics

To display DHCP snooping statistics, use the **show dhcp-snooping statistics** command.

show dhcp-snooping statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the DHCP snooping statistics:

```
Console> show dhcp-snooping statistics
Packets forwarded                     =          245
Packets dropped                       =          56
Packets dropped from untrusted ports  =          56
Number of binding entries             =          23
Console>
```

Related Commands

clear dhcp-snooping statistics

show diagnostic

To display the online diagnostic tests that are configured for specific modules and to check the results of these tests, use the **show diagnostic** command.

show diagnostic bootup level

show diagnostic content module {*mod_num* | **all**}

show diagnostic diagfail-action

show diagnostic events [**event-type** {**error** | **info** | **warning**} | **module** *mod_num*]

show diagnostic ondemand settings

show diagnostic result module {*mod_list* {**detail** | **test** *test_list*}} | **all** [**detail**]}

show diagnostic schedule module *mod_list*

show diagnostic status

Syntax Description

bootup level	Displays the level of bootup diagnostics.
content	Displays diagnostics test content.
module	Specifies the module.
mod_num	Number of the module.
all	Specifies all modules.
diagfail-action	Displays how the supervisor engine responds in the event of an online diagnostics failure.
events	Displays information about the online diagnostics event log.
event-type	Specifies the event type to be displayed.
error	Displays error events.
info	Displays informative events.
warning	Displays warning events.
ondemand settings	Displays on-demand settings for online diagnostics.
result	Display online diagnostics results.
mod_list	List of module numbers.
detail	Displays detailed results.
test	Displays results for a specific test.
test_list	Test number.
all	Displays results for all tests.
schedule	Displays schedule for online diagnostics.
status	Displays online diagnostics status for all modules.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Note GOLD is supported on the Supervisor Engine 720 and the Supervisor Engine 32 only. Earlier diagnostic commands are still supported on the Supervisor Engine 1 and the Supervisor Engine 2.

Examples

This example shows how to display the level at which bootup diagnostics is configured:

```
Console> show diagnostic bootup level
Current bootup diagnostic level: bypass
Console>
```

This example shows how to display how the supervisor engine responds in the event of an online diagnostics failure

```
Console> show diagnostic diagfail-action
Diagnostic failure action for SUP at last bootup : offline
Diagnostic failure action for SUP at next reset  : offline
Console>
```

This example shows how to display on-demand settings for online diagnostics:

```
Console> show diagnostic ondemand settings
Test iterations = 50
Action on test failure = continue until test failure limit reaches 100
Console>
```

This example show how to display the online diagnostics schedule for a specified module:

```
Console> show diagnostic schedule module 7

Current Time = Fri Apr 15 2005, 16:56:06

Diagnostic for Module 7:

Schedule #1:
        To be run daily 12:12
        Test ID(s) to be executed: 1-2.

Schedule #2:
        To be run daily 16:16
        Test ID(s) to be executed: 3.
        Port(s) to be tested: 1.

Console>
```

Related Commands

clear diagnostic
diagnostic start
diagnostic stop
set diagnostic bootup level
set diagnostic diagfail-action
set diagnostic event-log size

set diagnostic monitor
set diagnostic ondemand
set diagnostic schedule

show dot1q-all-tagged

To display the status of the dot1q tagging feature on the switch, use the **show dot1q-all-tagged** command.

show dot1q-all-tagged

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display dot1q tagging status:

```
Console> show dot1q-all-tagged
Dot1q-all-tagged feature globally disabled.
Console>
```

Related Commands

set dot1q-all-tagged

show dot1x

To display system 802.1X capabilities and information related to 802.1X users, groups, VLANs, and VLAN groups, use the **show dot1x** command.

show dot1x

show dot1x group {**all** | **authenticated** | *group_name*}

show dot1x user {**all** | *user_name*}

show dot1x vlan {**all** | *vlan_id*}

show dot1x vlan-group {**all** | *vlan_group_name*}

Syntax Description

group	Displays 802.1X user group information.
all	Displays information about all user groups.
authenticated	Displays information about authenticated user groups.
group_name	User group name.
user	Displays 802.1X user information.
all	Displays information about all authenticated users.
user_name	User name.
vlan	Displays information about 802.1X authenticated users in a VLAN.
all	Displays user information in all VLANs.
vlan_id	VLAN number.
vlan-group	Displays 802.1X VLAN group information.
all	Displays information for all 802.1X VLAN groups.
vlan_group_name	Name of the VLAN group.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the 802.1X information for the system:

```
Console> show dot1x
PAE Capability              Authenticator Only
Protocol Version            1
system-auth-control         enabled
max-req                     2
quiet-period                45 seconds
radius-accounting           disabled
```

```
radius-vlan-assignment       enabled
radius-keepalive state       enabled
re-authperiod                7200 seconds
server-timeout               30 seconds
shutdown-timeout             300 seconds
supp-timeout                 30 seconds
tx-period                    30 seconds

Console>
```

This example shows how to display information about all 802.1X user groups:

```
Console show dot1x group all
Group Manager Info

---------------------------------
Info of Group group-81
User Count  = 2
---------------------------------
User mNo    = 3
User pNo    = 20
Username    = user81
User IP     = 81.81.81.54
User VLAN   = 81
User mNo    = 3
User pNo    = 18
Username    = user81
User IP     = 81.81.81.55
User VLAN   = 81

---------------------------------
Info of Group group-82
User Count  = 1
---------------------------------
User mNo    = 3
User pNo    = 19
Username    = user82
User IP     = 81.81.82.51
User VLAN   = 82

---------------------------------
Info of Group group-83
User Count  = 0
---------------------------------

---------------------------------
Info of Group group-84
User Count  = 0
---------------------------------
Console>
```

This example shows how to display information about authenticated user groups:

```
Console> show dot1x group authenticated
Authenticated Groups Info
---------------------------------
Info of Group group-81
User Count  = 2
---------------------------------
User mNo    = 3
User pNo    = 20
Username    = user81
User IP     = 81.81.81.54
User VLAN   = 81
User mNo    = 3
User pNo    = 18
Username    = user81
User IP     = 81.81.81.55
User VLAN   = 81

---------------------------------
Info of Group group-82
User Count  = 1
---------------------------------
User mNo    = 3
User pNo    = 19
Username    = user82
User IP     = 81.81.82.51
User VLAN   = 82
Console>
```

This example shows how to display information about a specific group:

```
Console> show dot1x group group-81
---------------------------------
Info of Group group-81
User Count  = 2
---------------------------------
User mNo    = 3
User pNo    = 20
Username    = user81
User IP     = 81.81.81.54
User VLAN   = 81
User mNo    = 3
User pNo    = 18
Username    = user81
User IP     = 81.81.81.55
User VLAN   = 81
Console>
```

This example shows how to display information about all authenticated users:

```
Console> show dot1x user all
Dot1x Info for user user81
------------------------------------------
User Port                    = 3/18
User Vlan                    = 81
User count on this Vlan      = 1
User IP                      = 81.81.81.55

Dot1x Info for user user82
------------------------------------------
User Port                    = 3/19
User Vlan                    = 82
User count on this Vlan      = 1
User IP                      = 81.81.82.51

Dot1x Info for user user81
------------------------------------------
User Port                    = 3/20
User Vlan                    = 81
User count on this Vlan      = 1
User IP                      = 81.81.81.54
Console>
```

This example shows how to display information about a specific authenticated user:

```
Console> show dot1x user user81
Dot1x Info for user user81
------------------------------------------
User Port                    = 3/20
User Vlan                    = 81
User count on this Vlan      = 1
User IP                      = 81.81.81.54
Console>
```

This example shows how to display information about authenticated users in a VLAN:

```
Console> show dot1x vlan 82
Dot1x info for Vlan 81
------------------------------------------
Dot1x Info for user user81
------------------------------------------
User Port                    = 3/18
User Vlan                    = 82
User count on this Vlan      = 2
User IP                      = 81.81.82.55

Dot1x Info for user user82
------------------------------------------
User Port                    = 3/19
User Vlan                    = 82
User count on this Vlan      = 2
User IP                      = 81.81.82.51
Console>
```

This example shows how to display information about a specific VLAN group:

```
Console> show dot1x vlan-group engg-dept
Group Name       Vlans Mapped
-----------------------------------
engg-dept        3-4
Console>
```

This example shows how to display information about all VLAN groups:

```
Console> show dot1x vlan-group all
Group Name       Vlans Mapped
-----------------------------------
engg-dept        3-4
hr-dept          5-7,10
Console>
```

Related Commands

clear dot1x config
set dot1x

show dvlan statistics

To display dynamic VLAN statistics, use the **show dvlan statistics** command.

show dvlan statistics

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display dynamic VLAN statistics:

```
Console> show dvlan statistics
VMPS Client Statistics
----------------------
VQP Queries:               0
VQP Responses:             0
Vmps Changes:              0
VQP Shutdowns:             0
VQP Denied:                0
VQP Wrong Domain:          0
VQP Wrong Version:         0
VQP Insufficient Resource: 0
Console>
```

Related Commands

reconfirm vmps

8.6 EFT Copy

show environment

To display environmental, temperature, and inline power status information, use the **show environment** command.

show environment [**all** | **temperature** | **power** [*mod*] | **cooling** [*mod*] | **connector** [*mod*]]

Syntax Description

all	(Optional) Displays environmental status information (for example, power supply, fan status, and temperature information) and information about the power available to the system.
temperature	(Optional) Displays temperature information.
power	(Optional) Displays inline power status.
mod	(Optional) Number of the module to display inline power status
cooling	(Optional) Displays cooling information.
connector	(Optional) Displays connector rating information.

Defaults

If you do not enter a keyword, environmental status information (for example, power supply, fan status, and temperature information) only is displayed.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **temperature** option is not supported by the NAM.

In the output of the **show environment all** command, environmental status and temperature information for the NAM module is not supported.

In the output of the **show environment temperature** and **show environment all** commands, you will notice three slot 1 displays. The first slot 1 is the actual supervisor engine. The second slot 1 is the switching engine, which is on the supervisor engine (slot 1) and has its own Intake, Exhaust, Device 1, and Device 2 temperature outputs. The third slot 1 is the MSFC, which is also on the supervisor engine and has its own Intake, Exhaust, Device 1, and Device 2 temperature outputs.

If you see a partial-deny card status, this is an indication that some module ports are inline-powered, but not all the ports on the module are inline powered.

Examples

This example shows how to display environmental status information:

```
Console> show environment
Environmental Status (. = Pass, F = Fail, U = Unknown, N = Not Present)
  PS1:.     PS2:N     PS1 Fan:.     PS2 Fan:N
  Chassis-Ser-EEPROM:.     Fan:.
  Clock(A/B):A         Clock A:.     Clock B:.
  VTT1:.    VTT2:.    VTT3:.
Console>
```

This example shows how to display environmental status information and details about the power available to the system:

```
Console> show environment all
Environmental Status (. = Pass, F = Fail, U = Unknown, N = Not Present)
  PS1: .     PS2: N     PS1 Fan: .     PS2 Fan: N
  Chassis-Ser-EEPROM: .     Fan: .
  Clock(A/B): A         Clock A: .     Clock B: .
  VTT1: .    VTT2: .    VTT3: .

                   Intake        Exhaust       Device 1     Device 2
Slot             Temperature   Temperature   Temperature   Temperature
---------------- ------------  ------------  ------------  ------------
1                24C(50C,65C)  32C(60C,75C)  27C           32C
3                N/A           N/A           N/A           N/A
5                22C(50C,65C)  27C(60C,75C)  28C           28C
1  (Switch-Eng)  22C(50C,65C)  22C(60C,75C)  N/A           N/A
1  (MSFC)        26C(50C,65C)  30C(60C,75C)  N/A           N/A

Chassis Modules
------------------
VTT1: 25C(85C,100C)
VTT2: 24C(85C,100C)
VTT3: 25C(85C,100C)

PS1 Capacity: 1153.32 Watts (27.46 Amps @42V)
PS2 Capacity: none
PS Configuration : PS1 and PS2 in Redundant Configuration.
Total Power Available: 1153.32 Watts (27.46 Amps @42V)
Total Power Available for Line Card Usage: 1153.32 Watts (27.46 Amps @42V)
Total Power Drawn From the System: 453.18 Watts (10.79 Amps @42V)
Remaining Power in the System: 700.14 Watts (16.67 Amps @42V)
Default Inline Power allocation per port: 2.00 Watts (0.04 Amps @42V)

Slot power Requirement/Usage :

Slot Card Type           PowerRequested PowerAllocated CardStatus
                         Watts    A @42V Watts    A @42V
---- ------------------- ------- ------ ------- ------ ----------
1    WS-X6K-SUP1A-2GE    138.60   3.30  138.60   3.30  ok
2                          0.00   0.00  138.60   3.30  none
3    WS-X6380-NAM         63.00   1.50   63.00   1.50  ok
5    WS-X6248-RJ-45      112.98   2.69  112.98   2.69  ok
Console>
```

This example shows how to display temperature information:

```
Console> show environment temperature
                   Intake        Exhaust       Device 1     Device 2
Slot             Temperature   Temperature   Temperature   Temperature
---------------  ------------  ------------  ------------  ------------
1                25C(50C,65C)  34C(60C,75C)  27C           32C
3                N/A           N/A           N/A           N/A
5                24C(50C,65C)  27C(60C,75C)  28C           29C
1  (Switch-Eng)  22C(50C,65C)  22C(60C,75C)  N/A           N/A
1  (MSFC)        28C(50C,65C)  32C(60C,75C)  N/A           N/A

Chassis Modules
------------------
VTT1: 25C(85C,100C)
VTT2: 25C(85C,100C)
VTT3: 25C(85C,100C)
Console> (enable)
```

This example shows how to display the inline power for all modules:

```
Console> show environment power
PS1 Capacity:1153.32 Watts (27.46 Amps @42V)
PS2 Capacity:none
PS Configuration :PS1 and PS2 in Redundant Configuration.

Total Power Available                        :1153.32 Watts (27.46 Amps @42V)
Total Power Chassis Limit                    :3780.00 Watts (90.00 Amps @42V)
Total Power Chassis Recommended              :3780.00 Watts (90.00 Amps @42V)
Total Power Available for Line Card Usage    :1153.32 Watts (27.46 Amps @42V)
Total Power Drawn From the System            : 493.08 Watts (11.74 Amps @42V)
Total Power Drawn by the Chassis             :   0.00 Watt
Total Power Drawn by the modules             : 457.80 Watts (10.90 Amps @42V)
Total Inline Power Drawn From the System     :   0.00 Watts ( 0.00 Amps @42V)
Total Power Reserved as localpool for modules:  34.86 Watts ( 0.83 Amps @42V)
Remaining Power in the System                : 660.24 Watts (15.72 Amps @42V)
Configured Default Inline Power allocation per port:15.40 Watts ( 0.37 Amps @42V)

Slot power Requirement/Usage :

Slot Model                    PowerRequested PowerAllocated CardStatus
                            Watts    A @42V Watts    A @42V
---- ---------------------- ------- ------ ------- ------ ----------
1    WS-X6K-SUP2-2GE          128.52  3.06   128.52  3.06   ok
2    WS-X6K-SUP2-2GE          128.52  3.06   128.52  3.06   standby
5    WS-X6148-RJ45V           100.38  2.39   100.38  2.39   ok
6    WS-X6348-RJ-45           100.38  2.39   100.38  2.39   ok

Slot Inline Power Requirement/Usage :

Slot Sub-Model           Total Allocated   Max H/W Supported  Max H/W Supported
                        To Module (Watts) Per Module (Watts) Per Port (Watts)
---- ------------------- ----------------- ------------------ -----------------
5    WS-F6K-SVDB-FE      0.000             399.84             15.400
Console>
```

This example shows how to display the inline power status for a specific module:

```
Console> show environment power 9
Module 9:
Default Inline Power allocation per port: 9.500 Watts (0.22 Amps @42V)
Total inline power drawn by module 9: 0 Watt

Slot power Requirement/Usage :

Slot Card Type           PowerRequested PowerAllocated CardStatus
                         Watts   A @42V Watts   A @42V
---- ------------------- ------- ------ ------- ------ ----------
9    WS-X6348            123.06   2.93  123.06   2.93  ok

Default Inline Power allocation per port: 9.500 Watts (0.22 Amps @42V)
Port      InlinePowered     PowerAllocated
      Admin Oper   Detected mWatt mA @42V
----- ----- ------ -------- ----- --------
 9/1  auto  off    no       0     0
 9/2  auto  off    no       0     0
 9/3  auto  off    no       0     0
 9/4  auto  off    no       0     0
 9/5  auto  off    no       0     0
.
.
.
Console>
```

This example shows how to display cooling information:

```
Console> show environment cooling

Chassis per slot cooling capacity : 84 cfm


Fan tray(s) cooling capacity :

Fan  Model               Ver Cooling  Ambient FanStatus
                             capacity temp
---- ------------------- --- -------- ------- ---------
1    FAN-MOD-9             2  690 cfm     55C ok
2    FAN-MOD-9             2  690 cfm     55C ok

Slot cooling requirement :

Slot CardType            Cooling
---- ------------------- -------
3    WS-X6724-SFP         30 cfm
6    WS-X6K-SUP3-BASE     70 cfm
7    FI_WS_X6348_RJ45     30 cfm
9    WS-X6704-10GE        70 cfm
Console>
```

This example shows how to display connector rating information:

```
Console> show environment connector
Chassis connector rating : 756.00  Watts (18.00  Amps @42V)

Slot connector rating :

Slot CardType            ConnectorRating
                         Watts    A @42V
---- ------------------- -------- ------
3    WS-X6724-SFP        693.00   16.50
6    WS-X6K-SUP3-BASE    693.00   16.50
7    FI_WS_X6348_RJ45    693.00   16.50
9    WS-X6704-10GE       756.00   18.00
Console>
```

Table 2-33 describes the fields in the **show environment** output.

Table 2-33 show environment Command Output Fields

Field	Description
Environmental Status[1]	
PS1: and PS2:	Power supply status.
PS1 Fan: and PS2 Fan:	Power supply fan status.
Chassis-Ser-EEPROM:	Chassis serial EEPROM status.
Fan:	Fan status.
Clock A: and Clock B:	Clock A and B status.
VTT1:, VTT2:, and VTT3:	VTT module status. VTT modules are power monitors for the chassis backplane. A minor system alarm is signalled when one of the three VTTs fails, and a major alarm is signalled when two or more VTTs fail.
Intake Temperature and Exhaust Temperature	Temperature of the air flow as it enters, goes over the modules, and exits the chassis. The current temperature is listed first, with the minor and major alarm temperatures listed in parentheses.
Device 1 Temperature and Device 2 Temperature	The devices are additional temperature sensors measuring the internal temperature on each module indicated. The current temperature is listed first, with the warning and critical alarm temperatures listed in parentheses.
Chassis Modules	
VTT1:, VTT2:, and VTT3:	Temperature of the VTT modules. The current temperature is listed first, with the minor and major alarm temperature settings listed in parentheses.
PS1 Capacity: and PS2 Capacity:	Power supply capacity.
PS Configuration:	Power supply configuration.
Total Power Available:	Total available power.
Total Power Available for Line Card Usage:	Total power available for module use.
Total Power Drawn From the System:	Total power drawn from the system.
Remaining Power in the System:	Remaining power in the system.
Configured Default Inline Power allocation per port:	Configured default inline power allocation per port.

Table 2-33 show environment Command Output Fields (continued)

Field	Description
Slot power Requirement/Usage	
Power Requested	Module power requested.
Power Allocated	Module power allocation.
Card Status	Module status (no, ok, partial-deny[2], unknown, power-bad, and power-deny).
Slot Inline Power Requirement/Usage	
Total Allocated to Module	Inline power in Watts already allocated to the specified module.
Max H/W Supported Per Module	Maximum hardware supported per module in Watts.
Max H/W Supported Per Port	Maximum hardware supported per port in Watts.
Total inline power drawn	Total inline power drawn from the system.
InlinePowered—Admin	Inline power management status—auto, on, and off.
InlinePowered—Oper	Inline power status—on indicates power is being supplied by that port, off indicates power is not being supplied by the port, denied indicates there is not have enough power available to provide to the port.
InlinePowered—Detected	Status of whether or not inline power is detected.

[1] Environmental status indications are the following: . = Pass, F = Fail, U = Unknown, and N = Not Present.

[2] The partial-deny state indicates that some ports but not all ports in the module are inline powered.

Related Commands

set inlinepower
show port inlinepower

8.6 EFT Copy

show eou

To display Extensible Authentication Protocol over User Datagram Protocol (EoU) information, use the **show eou** command.

show eou all

show eou authentication {**clientless** | **eap** | **static**}

show eou config

show eou ip-address *ip_addr*

show eou mac-address *mac_addr*

show eou posture-token *posture_token*

Syntax Description

all	Displays a summary of the LAN port IP state on all EoU-enabled ports.
authentication	Displays EoU authentication-related information.
clientless	Displays all clientless ports.
eap	Displays all ports with EAP authentication.
static	Displays all hosts in an exception list.
config	Displays the EoU global configuration.
ip-address *ip_addr*	Displays EoU information for a host with the specified IP address.
mac-address *mac_addr*	Displays EoU information for a host with the specified MAC address.
posture-token *posture_token*	Displays EoU results on a posture-token basis.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display a summary of the LAN port IP state on all LAN port IP-enabled ports:

```
Console> show eou all
Eou Summary
-----------
Eou Global State = disabled

mNo/pNo   Host Ip           Nac_Token   Host_Fsm_State   Username
-------   ----------------  ---------   --------------   --------
Console>
```

This example shows how to display the EOU configuration:

```
Console> show eou config
Eou Protocol Version = 1
Eou Global Config
-----------------
Eou Global Enable          = Disabled
Eou Clientless             = Disabled
Eou Logging                = Enabled
Eou MaxRetry               = 3
Eou AAA timeout            = 60
Eou Hold timeout           = 180
Eou Retransmit timeout     = 30
Eou Revalidation timeout   = 3600
Eou Status Query timeout   = 300
List of hosts in IP Exception list.
------------------------------------

List of hosts in Mac Exception list.
-------------------------------------

Exception Hosts Policy
----------------------

Console>
```

Related Commands

clear eou
set eou
set port eou
set security acl ip
show port eou

show errdisable-timeout

To display the configuration and status of the errdisable timeout, use the **show errdisable-timeout** command.

show errdisable-timeout

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If your system is configured with a Supervisor Engine 2, the crossbar-fallback error may be displayed in the ErrDisable Reason field.

Examples

This example shows how to display the errdisable timeout configuration and status:

```
Console> show errdisable-timeout
ErrDisable Reason      Timeout Status
---------------------- --------------
aarp-inspection                         enable
bcast-suppression                       enable
bpdu-guard                              enable
cam-monitor                             enable
channel-misconfig                       enable
crossbar-fallback                       enable
duplex-mismatch                         enable
gl2pt-ingress-loop                      enable
gl2pt-threshold-exceed                  enable
gl2pt-cdp-threshold-exceed              enable
gl2pt-stp-threshold-exceed              enable
gl2pt-vtp-threshold-exceed              enable
link-rxcrc                              enable
link-txcrc                              enable
udld                                    enable
other                                   enable
Interval: 300 seconds

Ports that will be enabled at the next timeout:
Port  Errdisable Reason  Port ErrDisableTimeout  Action on Timeout
----  -----------------  ----------------------  -----------------
3/3   udld               Disable                 Remain Disabled
3/4   udld               Enable                  Enabled
3/5   other              Disable                 Remain Disabled (PRBS)
Console>(enable)
```

Related Commands

set errdisable-timeout

show errordetection

To display error detection settings, use the **show errordetection** command.

show errordetection

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the error detection settings:

```
Console> show errordetection
Inband error detection:                     disabled
Memory error detection:                     disabled
Packet buffer error detection:              errdisable
Port counter error detection:               disabled
Port link-errors detection:                 disabled
Port link-errors action:                    port-failover
Port link-errors interval:                  30 seconds
Port link-errors threshold inerrors high:   1001 packets
Port link-errors threshold inerrors low:    1000 packets
Port link-errors threshold rxcrc high:      1001 packets
Port link-errors threshold rxcrc low:       1000 packets
Port link-errors threshold txcrc high:      1001 packets
Port link-errors threshold txcrc low:       1000 packets
Port link-errors sampling:                  3
Console>
```

Related Commands

set errordetection
set port errordetection
show port errordetection

show ethernet-cfm continuity-check statistics

To display continuity-check message statistics, use the **show ethernet-cfm continuity-check statistics** command.

show ethernet-cfm continuity-check statistics {**level** *level* | **domain** *domain_name*}

Syntax Description

level *level*	Displays statistics for maintenance points at a specific level; valid values are from 0 to 7.
domain *domain_name*	Displays statistics for maintenance points in a specific domain.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This output for this command displays remote MPIDs, mod/port numbers, number of received packets, number of packets discarded because of cross-connected CSIs, number of packets discarded because of duplicate CSIDs, and the number of packets discarded because of out-of-order transaction IDs.

Examples

This example displays statistics for all the maintenance points on the switch with a maintenance level 1:

```
Console> show ethernet-cfm continuity-check statistics level 1
---------------------------------------------------------------------
Remote MPID  Port  Rcvd  Cross-connect  Duplicate  out-of-order
---------------------------------------------------------------------
3033         4/11  13756             0          0             0
3031         4/13   4329             0          0             0
3033         4/11  11438             0          0             0
3031         4/13   4329             0          0             0
3033         4/11  11438             0          0             0
3031         4/13   4329             0          0             0
3033         4/11  11438             0          0             0
3031         4/13   4329             0          0             0
3033         4/11  11438             0          0             0
3031         4/13   4329             0          0             0
3033         4/11  11438             0          0             0
3031         4/13   4329             0          0             0
3033         4/11  11438             0          0             0
3031         4/13   4329             0          0             0
3033         4/11  11438             0          0             0
3031         4/13   4329             0          0             0
3033         4/11  11438             0          0             0
3031         4/13   4329             0          0             0
3033         4/11  11438             0          0             0
3031         4/13   4329             0
Console>
```

show ethernet-cfm domain

To display all the configured CFM domains, use the **show ethernet-cfm domain** command.

show ethernet-cfm domain [*domain_name*]

Syntax Description

domain_name	(Optional) Domain name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *domain_name* argument, all domains, their maintenance levels, and their total services are displayed.

Examples

This example displays information on all the domains on the switch:

```
Console> show ethernet-cfm domain
------------------------------------------
Domain Name                Level  Services
------------------------------------------
sjlabf1                        1        99
sjlabg3                        3        99
sjlabg4                        4        50
Console>
```

This example displays information on only the sjlabf1 domain:

```
Console> show ethernet-cfm domain sjlabf1
Domain Name : sjlabf1
Level : 1
archive time : 0
Total Services : 99
Console>
```

show ethernet-cfm errors

To display the the CFM error conditions logged since the last reload, use the **show ethernet-cfm errors** command.

show ethernet-cfm errors [**level** *level*]

Syntax Description

level *level*	(Optional) Display CFM error conditions for maintenance points with a specific maintenance level; valid values are from 0 to 7.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a maintenance level, errors for all levels are displayed.

Examples

[Need example.]

show ethernet-cfm maintenance-point

To display all the local or remote maintenance points, use the **show ethernet-cfm maintenance-point** command.

show ethernet-cfm maintenance-point {**local** | **remote**} [**level** *level*]

Syntax Description

local	Displays all local maintenance points on the switch.
remote	Displays all remote maintenance points on the switch.
level *level*	(Optional) Displays all maintenance points at a specified maintenance level; valid values are from 0 to 7.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

For remote maintenance points, this command displays the module and port number, the VLAN number, the MPID, whether the maintenance point is a MIP or a MEP, the maintenance level, the MAC address, and the CSID. For local maintenance points, this command displays the module and port number, the MPID, whether the maintenance point is a MIP or a MEP, the level, the domain name, the status of the continuity check, and the VLAN number or range of VLANs.

If you do not enter a maintenance level, all levels are displayed.

Examples

This example displays remote maintenance points:

```
Console> show ethernet-cfm maintenance-point remote
-------------------------------------------------------------------------------
Ing-Port  Vlan  MPID  Type  Level            mac-addr                 CSID
-------------------------------------------------------------------------------
4/11        1   3033   MEP      1   00-50-3e-8f-8f-fb              custA1
4/13        1   3031   MEP      1   00-d0-00-b3-6b-fb              custA1
4/11        2   3033   MEP      1   00-50-3e-8f-8f-fb              custA2
4/13        2   3031   MEP      1   00-d0-00-b3-6b-fb              custA2
4/11        3   3033   MEP      1   00-50-3e-8f-8f-fb              custA3
4/13        3   3031   MEP      1   00-d0-00-b3-6b-fb              custA3
4/11        4   3033   MEP      1   00-50-3e-8f-8f-fb              custA4
4/13        4   3031   MEP      1   00-d0-00-b3-6b-fb              custA4
4/11        5   3033   MEP      1   00-50-3e-8f-8f-fb              custA5
4/13        5   3031   MEP      1   00-d0-00-b3-6b-fb              custA5
Console>
```

This example displays local maintenance points:

```
Console> show ethernet-cfm maintenance-point local
------------------------------------------------------------------------
Port  MPID  Type  Level         DomainName  CC-stat    Vlans
------------------------------------------------------------------------
4/37  3033   MEP      1            sjlabf1   enable    1-100
4/37  4040   MEP      3            sjlabg3   enable    1-100
Console>
```

This example displays remote maintenance points at level 3:

```
Console> show ethernet-cfm maintenance-point remote level 3
---------------------------------------------------------------------------
Ing-Port  Vlan  MPID  Type  Level            mac-addr                 CSID
---------------------------------------------------------------------------
4/11        1  4040   MEP      3   00-50-3e-8f-8f-fb               custA1
4/13        1  4020   MEP      3   00-d0-00-b3-6b-fb               custA1
4/11        2  4040   MEP      3   00-50-3e-8f-8f-fb               custA2
4/13        2  4020   MEP      3   00-d0-00-b3-6b-fb               custA2
4/11        3  4040   MEP      3   00-50-3e-8f-8f-fb               custA3
4/13        3  4020   MEP      3   00-d0-00-b3-6b-fb               custA3
4/11        4  4040   MEP      3   00-50-3e-8f-8f-fb               custA4
4/13        4  4020   MEP      3   00-d0-00-b3-6b-fb               custA4
4/11        5  4040   MEP      3   00-50-3e-8f-8f-fb               custA5
4/13        5  4020   MEP      3   00-d0-00-b3-6b-fb               custA5
4/11        6  4040   MEP      3   00-50-3e-8f-8f-fb               custA6
4/13        6  4020   MEP      3   00-d0-00-b3-6b-fb               custA6
4/11        7  4040   MEP      3   00-50-3e-8f-8f-fb               custA7
4/13        7  4020   MEP      3   00-d0-00-b3-6b-fb               custA7
4/11        8  4040   MEP      3   00-50-3e-8f-8f-fb               custA8
4/13        8  4020   MEP      3   00-d0-00-b3-6b-fb               custA8
4/11        9  4040   MEP      3   00-50-3e-8f-8f-fb               custA9
4/13        9  4020   MEP      3   00-d0-00-b3-6b-fb               custA9
Console>
```

show ethernet-cfm status

To display the global CFM status, maximum configured maintenance level and bridge brain MAC address, use the **show ethernet-cfm status** command.

show ethernet-cfm status

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

For all maintenance points configured on the switch, this command displays the type of CFM configured, the maximum MEP and MIP maintenance level, and the bridge brain MAC address. “Bridge brain” means that all the Maintenance Points have the same MAC address. [Could I get clarification on the meaning of “bridge brain”?]

Examples

This example displays the CFM status:

```
Console> show ethernet-cfm status
Ethernet CFM is enabled on the switch.
Max configured MEP level is 4.
Bridge Brain Mac Address is 00-90-6f-96-23-fb.
Console>
```

show fabric channel

To display Switch Fabric Module information, use the **show fabric channel** command.

show fabric channel counters {*mod* | **all**} [**hex**]

show fabric channel utilization

show fabric channel switchmode [*mod*]

Syntax Description

counters	Displays fabric channel counter information.
mod	Number of the fabric-enabled module.
all	Displays counters for all fabric-enabled modules.
hex	(Optional) Displays counters in hexadecimal format.
utilization	Displays fabric channel utilization information.
switchmode	Displays switch mode and fabric channel status.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The term “CEF720” refers to any module that has a part number that conforms to WS-X67*xx-xxx* (such as WS-X6724-SFP). These modules connect to the integrated 720-Gbps switch fabric on the Supervisor Engine 720 and to the 32-Gbps switching bus.

Note The integrated 720-Gbps switch fabric is supported only on Supervisor Engine 720.

The term “CEF256” refers to any module that has a part number that conforms to WS-X65*xx-xxx* (such as WS-X6548-GE-TX), the Optical Services Modules, the enhanced FlexWAN module, and most service modules (such as the FWSM, the SSLM, the VPNSM, the NAM-1, the NAM-2, the IDSM-2, the CSG, and the CMM). These modules connect to either the integrated 720-Gbps switch fabric on the Supervisor Engine 720 or to the external 256-Gbps Switch Fabric Modules that are supported by the Supervisor Engine 2, and these modules connect to the 32-Gbps switching bus.

Note The external Switch Fabric Modules are supported only with Supervisor Engine 2 in the Catalyst 6500 series switch.

A non-fabric-enabled module is not included in the CEF720 or CEF256 categories. These modules have no fabric connections and connect only to the 32-Gbps switching bus.

The CEF256/CEF720 modules operate in one of three modes when using centralized forwarding:

- Compact mode—Operational mode when all modules in the system are CEF256 or CEF720 (no non-fabric-enabled modules can be present for this mode).

  In this mode, the CEF256 or CEF720 modules send a “compact” 32-byte header for each frame to the supervisor engine over the switching bus. Once a forwarding decision is made, the CEF256 or CEF720 modules send the entire frame through the switch fabric to the egress module.

- Truncated mode—Operational mode when at least one non-fabric-enabled module is present in the system.

  In this mode, the CEF256 or CEF720 modules send the first 64 bytes of each frame to the supervisor engine over the switching bus. Once a forwarding decision is made, the CEF256 or CEF720 modules send the entire frame through the switch fabric to the egress module.

- Flow-through mode—Operational mode for the CEF256 modules when there is no switch fabric present.

  In this mode, the CEF256 modules send the entire packet to the supervisor engine over the switching bus. This mode is not applicable for the CEF720 modules, which require the presence of the switch fabric.

Examples

This example shows how to display fabric channel counter information for a specific module:

```
Console> show fabric channel counters 2
Channel 0 counters:
0 rxErrors                           =                    0
1 txErrors                           =                    0
2 txDropped                          =                    0
Console>
```

This example shows how to display fabric channel utilization information:

```
Console> show fabric channel utilization
Fab Chan Input Output
-------- ----- ------
       0    0%     0%
       1    0%     0%
       2    0%     0%
       3    0%     0%
.
.
.
      15    0%     0%
      16    0%     0%
      17    0%     0%
Console>
```

This example shows how to display switch mode and fabric channel status:

```
Console> show fabric channel switchmode
Global switching mode: flow through
Module Num Fab Chan Fab Chan Switch Mode  Channel Status
------ ------------ -------- ------------ --------------
     2            1   0, 1   flow through ok
     3            0   n/a    n/a          n/a
     5           18   0, 0   n/a          unknown
     5           18   1, 1   n/a          ok
.
.
.
     5           18  15, 15  n/a          unknown
     5           18  16, 16  n/a          unknown
     5           18  17, 17  n/a          unknown
    16            0 n/a      n/a          n/a
Console>
```

This example shows how to display the counters for all fabric-enabled modules:

```
Console> show fabric channel counters all
Counters for module 1
------------------------
Channel 0 counters:
0  rxErrors =                     0/0/0
1  txErrors  =                     0/0/0
2  txDropped  =                     0/0/0
Counters for module 4
------------------------
Channel 0 counters:
0  rxErrors =                     0/0/0
1  txErrors =                     0/0/0
2  txDropped =                     0/0/0
Counters for module 8
------------------------
Channel 0 counters:
0  rxErrors =                     0/0/0
1  txErrors =                     0/0/0
2  txDropped =                     0/0/0
Console>
```

This example shows how to display switch mode and fabric channel status on a Supervisor Engine 720 and on other fabric-enabled modules in the chassis:

```
Console> show fabric channel switchmode
Global switching mode: truncated
Fabric status : Online

Module Num Fab Chan Fab Chan Switch Mode  Channel Status
------ ------------ -------- ------------ --------------
     4            1   0, 3   truncated    ok
     6            1   0, 4   flow-through ok
     6           18   0, 0   n/a          ok
     6           18   1, 1   n/a          unused
     6           18   2, 2   n/a          unused
     6           18   3, 3   n/a          ok
     6           18   4, 4   n/a          unused
     6           18   5, 5   n/a          unused
     6           18   6, 6   n/a          unused
     6           18   7, 7   n/a          ok
     6           18   8, 8   n/a          unused
     6           18   9, 9   n/a          unused
     6           18  10, 10  n/a          unused
     6           18  11, 11  n/a          unused
     6           18  12, 12  n/a          unused
     6           18  13, 13  n/a          unused
     6           18  14, 14  n/a          unused
     6           18  15, 15  n/a          unused
     6           18  16, 16  n/a          unused
     6           18  17, 17  n/a          unused
     7            0    n/a   n/a          n/a
     8            1   0, 7   truncated    ok
Console>
```

This example shows how to display fabric channel utilization information on a system that uses a Supervisor Engine 720:

```
Console> show fabric channel utilization
Fab Chan Speed Input Output
-------- ----- ----- ------
       0   n/a    0%     0%
       1   n/a    0%     0%
       2   n/a    0%     0%
       3   n/a    0%     0%
       4   20G    0%     0%
       5   n/a    0%     0%
       6   n/a    0%     0%
       7   20G    0%     0%
       8    8G    0%     0%
       9   n/a    0%     0%
      10   n/a    0%     0%
      11   n/a    0%     0%
      12   n/a    0%     0%
      13   n/a    0%     0%
      14   n/a    0%     0%
      15   n/a    0%     0%
      16   20G    0%     0%
      17   n/a    0%     0%
Console>
```

Table 2-34 describes the fields in the **show fabric channel** output.

Table 2-34 show fabric channel Command Output Fields

Field	Description
rxErrors	Number of received errors.
txErrors	Number of transmitted errors.
txDropped	Number of dropped transmitted packets.
Input	Percentage of input traffic utilization.
Output	Percentage of output traffic utilization.
Num Fab Chan	Number of fabric channels associated with the module.
Global switching mode	Global switching mode of the switch (flow through, truncated, and compact).
Fab Chan	Fabric channel number; see the "Usage Guidelines" section for additional information.
Switch Mode	Channel switch mode type (flow through, truncated, and compact).
Channel Status	Channel status (ok, sync error, CRC error, heartbeat error, buffer error, timeout error, or unknown).

Table 2-34 show fabric channel Command Output Fields (continued)

Field	Description
Speed	Speed of the fabric link (8 Gbps or 20 Gbps).
Input	Percentages of input traffic utilization.
Output	Percentages of output traffic utilization.

Related Commands

switch fabric

show fabric errors

To display the fabric error counters on one or all modules, use the **show fabric errors** command.

show fabric errors {*mod* | **all**}

Syntax Description

mod	Number of the module.
all	Displays fabric error counters for all modules.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

```
Console> show fabric errors all
Module errors:
 slot    channel        crc       hbeat        sync   DDR sync
    3          0          0           0           0          0
    3          1          0           0           0          0
    5          0          0           0           0          0

Fabric errors:
 slot    channel       sync      buffer     timeout
    3          0          0           0           0
    3          1          0           0           0
    5          0          0           0           0
Console>
```

Table 2-36 describes the fields in the **show fabric errors** output.

Table 2-35 show fabric errors Command Output Fields

Field	Description
slot	Module number.
channel	Fabric channel number that is associated with the module.
crc	Cyclic redundancy check errors.
hbeat	Heartbeat errors.
sync	Synchronization errors on the module side.
DDR sync	Double Data Rate synchronization errors.
sync	Synchronization errors on the fabric side.
buffer	Buffer errors.
timeout	Timeout errors.

Related Commands

show fabric channel
show fabric status

show fabric status

To display the integrated switch fabric status and forwarding speed, use the **show fabric status** command.

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The integrated 720 Gbps switch fabric is supported only on the Supervisor Engine 720.

Note For software release 8.3(4) and later releases, the **show fabric status** command will not indicate the fabric speed.

Examples

```
Console> show fabric status
Mod Speed  Fabric
           status
--- ----- -------
  5   20G  active
Console> (enable)
```

Related Commands

set system crossbar-fallback
set system switchmode allow
show fabric channel

show file

To display the contents of a file that have been saved to Flash memory, use the **show file** command.

show file [*device*:]*filename* [**dump**]

Syntax Description

device:	(Optional) Device where the Flash memory resides.
filename	Name of the configuration file.
dump	(Optional) Shows the hexadecimal dump of the file.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

Examples

This example shows how to display the contents of the configuration file saved to Flash memory:

```
Console> (enable) show file slot0:cfgfile
begin
!
#version 5.4
!
set password $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set enablepass $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set prompt Console>
set length 24 default
!
#system
set system baud  9600
set system modem disable
...
Console> (enable)
```

This example shows how to display the hexadecimal dump from a file:

```
Console> (enable) show file slot:cfgfile dump
8099d140  0A626567 696E0A21 0A237665 7273696F   .begin.!.#versio
8099d150  6E20352E 3328302E 31312942 4F552D45   n 5.3(0.11)BOU-E
8099d160  6E670A21 0A736574 20706173 73776F72   ng.!.set passwor
8099d170  64202431 24464D46 51244866 5A523544   n $1$FMFQ$HfZR5D
8099d180  55737A56 48495268 727A3468 36563730   UszVHIRhrz4h6V70
8099d190  0A736574 20656E61 626C6570 61737320   .set enablepass
8099d1a0  24312446 4D465124 48665A52 35445573   $1$FMFQ$HfZR5DUs
8099d1b0  7A564849 5268727A 34683656 37300A73   zVHIRhrz4h6V70.s
...
```

show firewall

To display the parameters that are configured for a Firewall Services Module (FWSM), use the **show firewall** command.

show firewall multiple-vlan-interfaces

Syntax Description

multiple-vlan-interfaces	Displays the status of the multiple VLAN interface feature.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the status of the multiple VLAN interface feature on the FWSM:

```
Console> show firewall multiple-vlan-interfaces
multiple-vlan-interface feature disabled for firewall modules
Console>
```

Related Commands

set firewall

show flash

To list bootflash or Flash PC card information, including file code names, version numbers, volume ID, status, and sizes, use the **show flash** command.

show flash devices

show flash [[*m/*]*device*:] [**all** | **chips** | **filesys**]

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
device:	(Optional) Valid devices are **bootflash** and **slot0**.
all	(Optional) Lists deleted files, undeleted files, and files with errors on a Flash memory device.
chips	(Optional) Shows information about the Flash chip.
filesys	(Optional) Shows the Device Info Block, the Status Info, the Usage Info, and the volume ID.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

A colon (:) is required after the specified device.

Examples

This example shows how to list the Flash files:

```
Console> show flash devices
slot0, bootflash, tftp
Console>
```

These examples show how to list supervisor engine Flash information:

```
Console> show flash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
  1 .. ffffffff fec05d7a  4b3a4c   25  4667849 Mar 03 2000 08:52:09 cat6000-sup.
5-3-4-CSX.bin
  2 .. ffffffff 4e5efc31  c0fadc   30  7716879 May 19 2000 06:50:55 cat6000-sup-
d.6-1-0-83-ORL.bin

3605796 bytes available (12384988 bytes used)
Console>
Console> show flash chips
******** Intel Series 2+ Status/Register Dump ********

ATTRIBUTE MEMORY REGISTERS:
  Config Option Reg (4000): 2
  Config Status Reg (4002): 0
  Card Status   Reg (4100): 1
  Write Protect Reg (4104): 4
  Voltage Cntrl Reg (410C): 0
  Rdy/Busy Mode Reg (4140): 2
COMMON MEMORY REGISTERS: Bank 0
  Intelligent ID Code   : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    8  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    16 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    24 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0

COMMON MEMORY REGISTERS: Bank 1
  Intelligent ID Code   : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    8  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    16 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    24 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0

COMMON MEMORY REGISTERS: Bank 2
  Intelligent ID Code   : FF00FF
    IID Not Intel -- assuming bank not populated

COMMON MEMORY REGISTERS: Bank 3
Console>

Console> show flash all
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
  1 .. ffffffff fec05d7a  4b3a4c   25  4667849 Mar 03 2000 08:52:09 cat6000-sup.
5-3-4-CSX.bin
  2 .. ffffffff 4e5efc31  c0fadc   30  7716879 May 19 2000 06:50:55 cat6000-sup-
d.6-1-0-83-ORL.bin

3605796 bytes available (12384988 bytes used)

-------- F I L E   S Y S T E M   S T A T U S --------
  Device Number = 0
DEVICE INFO BLOCK:
  Magic Number          = 6887635   File System Vers = 10000    (1.0)
  Length                = 800000    Sector Size      = 20000
  Programming Algorithm = 4         Erased State     = FFFFFFFF
  File System Offset    = 20000     Length = 7A0000
  MONLIB Offset         = 100       Length = C730
  Bad Sector Map Offset = 1FFF8     Length = 8
  Squeeze Log Offset    = 7C0000    Length = 20000
  Squeeze Buffer Offset = 7E0000    Length = 20000
  Num Spare Sectors     = 0
    Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
```

```
USAGE INFO:
  Bytes Used     = 201D9B  Bytes Available = 5FE265
  Bad Sectors    = 0       Spared Sectors  = 0
  OK Files       = 1       Bytes = 100FC0
  Deleted Files  = 1       Bytes = 100DDB
  Files w/Errors = 0       Bytes = 0

******** Intel Series 2+ Status/Register Dump ********

ATTRIBUTE MEMORY REGISTERS:
  Config Option Reg (4000): 2
  Config Status Reg (4002): 0
  Card Status   Reg (4100): 1
  Write Protect Reg (4104): 4
  Voltage Cntrl Reg (410C): 0
  Rdy/Busy Mode Reg (4140): 2

COMMON MEMORY REGISTERS: Bank 0
  Intelligent ID Code  : 8989A0A0
  Compatible Status Reg: 8080
  Global     Status Reg: B0B0
  Block Status Regs:
    0  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    8  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    16 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    24 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0

COMMON MEMORY REGISTERS: Bank 1
  Intelligent ID Code  : 8989A0A0
  Compatible Status Reg: 8080
  Global     Status Reg: B0B0
  Block Status Regs:
    0  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    8  :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    16 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0
    24 :  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0  B0B0

COMMON MEMORY REGISTERS: Bank 2
  Intelligent ID Code  : FF00FF
    IID Not Intel -- assuming bank not populated

COMMON MEMORY REGISTERS: Bank 3
  Intelligent ID Code  : FF00FF
    IID Not Intel -- assuming bank not populated

COMMON MEMORY REGISTERS: Bank 4
  Intelligent ID Code  : FF00FF
    IID Not Intel -- assuming bank not populated
Console>
```

Related Commands

download
reset—switch

show ftp

To display the parameters configured for File Transfer Protocol (FTP), use the **show ftp** command.

show ftp

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the parameters configured for FTP:

```
Console> (enable) show ftp
FTP username set to: ski
FTP password for user 'ski' is configured
FTP passive mode : disabled
Console> (enable)
```

Related Commands

clear ftp
set ftp

show garp timer

To display all the values of the General Attribute Registration Protocol (GARP) timers, use the **show garp timer** command.

show garp timer

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You must maintain the following *relationship* for the various timer values:

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.

Caution Set the same GARP application (for example, GMRP and GVRP) timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP applications will not operate successfully.

Note The modified timer values are applied to all GARP application (for example, GMRP and GVRP) timer values.

Examples

This example shows how to display all the values of the GARP timers:

```
Console> (enable) show garp timer
Timer     Timer Value (milliseconds)
--------  --------------------------
Join      200
Leave     600
LeaveAll  10000
Console> (enable)
```

Related Commands

set garp timer
set gmrp timer
set gvrp timer

show gmrp configuration

To display complete GMRP-related configuration information, use the **show gmrp configuration** command.

show gmrp configuration

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If the port list exceeds the available line spaces, the list wraps to the next line.

Examples

This example shows how to display GMRP-related configuration information:

```
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
GMRP-Status Registration ForwardAll Port(s)
----------- ------------ ---------- --------------------------------------------
Enabled     Normal       Disabled   1/1-2
                                    2/1-48
                                    15/1
Console> (enable)
```

Related Commands

set gmrp registration

8.6 EFT Copy

show gmrp statistics

To display all the GMRP-related statistics for a specified VLAN, use the **show gmrp statistics** command.

show gmrp statistics [*vlan*]

Syntax Description

vlan	(Optional) VLAN for which to show GMRP statistics; valid values are from 1 to 4094.

Defaults

The default is that if you do not specify a VLAN, statistics for VLAN 1 are shown.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display all the GMRP-related statistics for VLAN 23:

```
Console> show gmrp statistics 23
GMRP Statistics for vlan <23>:
Total valid GMRP Packets Received:                          500
Join Empties:                                               200
Join INs:                                                   250
Leaves:                                                     10
Leave Alls:                                                 35
Empties:                                                    5
Fwd Alls:                                                   0
Fwd Unregistered:                                           0
Total valid GMRP Packets Transmitted:                       600
Join Empties:                                               200
Join INs:                                                   150
Leaves:                                                     45
Leave Alls:                                                 200
Empties:                                                    5
Fwd Alls:                                                   0
Fwd Unregistered:                                           0
Total valid GMRP Packets Received:                          0
Total GMRP packets dropped:                                 0
Total GMRP Registrations Failed:                            0
Console>
```

Related Commands

clear gmrp statistics
set gmrp

8.6 EFT Copy

show gmrp timer

To display all the values of the GMRP timers, use the **show gmrp timer** command.

show gmrp timer

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display all the values of the GMRP timers:

```
Console> (enable) show gmrp timer
Timer                Timer Value(milliseconds)
---------------------------------------------
Join                 200
Leave                600
Leave All            10000
Console> (enable)
```

Related Commands

set garp timer
set gmrp timer
set gvrp timer
show gmrp configuration

show gvrp configuration

To display GVRP configuration information, including timer values, whether or not GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP, use the **show gvrp configuration** command.

show gvrp configuration

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If the port list exceeds the available line spaces, the list wraps to the next line.

If no ports are GVRP participants, the message output changes from:

```
GVRP Participants running on port_list
```

to:

```
GVRP Participants running on no ports.
```

Examples

This example shows how to display GVRP configuration information:

```
Console> show gvrp configuration

Global GVRP Configuration:
GVRP Feature is currently enabled on the switch.
GVRP dynamic VLAN creation is enabled.
GVRP Timers(milliseconds)
Join = 200
Leave = 600
LeaveAll = 10000

Port based GVRP Configuration:
GVRP-Status Registration Applicant Port(s)
----------- ------------ --------- -------------------------------------------
Enabled.   Normal      Normal   2/1
Enabled.   Normal      Active   4/4
Enabled.   Fixed       Normal   4/9
Enabled.   Fixed       Active   4/11
Enabled.   Forbidden   Normal   4/10
Enabled.   Forbidden   Active   4/5
Disabled   Normal      Normal   2/2
                                4/12-24
                                5/1-8
Disabled   Normal      Active   4/1,4/8
Disabled   Fixed       Normal   4/2
Disabled   Fixed       Active   4/7
Disbled    Forbidden   Normal   4/3
Disbled    Forbidden   Active   4/6

GVRP Participants running on no ports.
Console>
```

Related Commands

clear gvrp statistics
set gvrp
set gvrp dynamic-vlan-creation
set gvrp registration
set gvrp timer
show gvrp statistics

8.6 EFT Copy

show gvrp statistics

To view GVRP statistics for a port, use the **show gvrp statistics** command.

show gvrp statistics [*mod/port*]

Syntax Description

mod/port	(Optional) Number of the module and port on the module.

Defaults

The default is, that if you do not specify a VLAN, statistics for VLAN 1 are shown.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display GVRP statistics for module 2, port 1:

```
Console> show gvrp statistics 2/1
GVRP enabled

GVRP statistics for port 2/1:
Total valid pkts rcvd:          18951
Total invalid pkts recvd        0
General Queries recvd           377
Group Specific Queries recvd    0
MAC-Based General Queries recvd 0
Leaves recvd                    14
Reports recvd                   16741
Queries  Xmitted                0
GS Queries Xmitted              16
Reports Xmitted                 0
Leaves Xmitted                  0
Failures to add GDA to EARL     0
Topology Notifications rcvd     10
GVRP packets dropped            0
Console>
```

Table 2-36 describes the fields in the **show gvrp statistics** output.

Table 2-36 show gvrp statistics Command Output Fields

Field	Description
GVRP Enabled	Status of whether or not GVRP is enabled or disabled.
Total valid pkts rcvd	Total number of valid GVRP packets received.
Total invalid pkts recvd	Total number of invalid GVRP packets received.
General Queries recvd	Total number of GVRP general queries received.
Group Specific Queries recvd	Total number of GVRP group-specific queries received.

Table 2-36 show gvrp statistics Command Output Fields (continued)

Field	Description
MAC-Based General Queries recvd	Total number of MAC-based general queries received.
Leaves recvd	Total number of GVRP leaves received.
Reports recvd	Total number of GVRP reports received.
Queries Xmitted	Total number of GVRP general queries transmitted by the switch.
GS Queries Xmitted	Total number of GVRP group specific-equivalent queries transmitted by the switch.
Reports Xmitted	Total number of GVRP reports transmitted by the switch.
Leaves Xmitted	Total number of GVRP leaves transmitted by the switch.
Failures to add GDA to EARL	Total number of times the switch failed to add a multicast entry (GDA) to the EARL table.
Topology Notifications rcvd	Total number of topology change notifications received by the switch.
GVRP packets dropped	Total number of GVRP packets dropped by the switch.

Related Commands

clear gvrp statistics
set gvrp
set gvrp dynamic-vlan-creation
set gvrp registration
set gvrp timer
show gvrp configuration

show ifindex

To display the information of the specific ifIndex, use the **show ifindex** command.

show ifindex *number*

Syntax Description

number	Number of the ifIndex.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can designate multiple ifIndex numbers by separating each number with a comma. To specify a range of numbers, use a dash (-) between the low and high numbers.

Examples

This example shows how to display ifIndex information:

```
Console> show ifindex 1,2,3,4-15,40-45
 Ifindex 1 is mapped to interface sc0.
 Ifindex 2 is mapped to interface sl0.
 Ifindex 3 is mapped to port 1/1.
 Ifindex 4 is mapped to port 1/2.
 Ifindex 5 is mapped to port 1/3.
 Ifindex 6 is mapped to port 1/4.
 Ifindex 7 is mapped to vlan 1.
 Ifindex 8 is mapped to vlan 1002.
 Ifindex 9 is mapped to vlan 1004.
 Ifindex 10 is mapped to vlan 1005.
 Ifindex 11 is mapped to vlan 1003.
 Ifindex 12 is mapped to port 9/1.
 Ifindex 13 is mapped to port 9/2.
 Ifindex 14 is mapped to port 9/3.
 Ifindex 15 is mapped to port 9/4.
 Ifindex 40 is mapped to port 8/5.
 Ifindex 41 is mapped to port 8/6.
 Ifindex 42 is mapped to port 8/7.
 Ifindex 43 is mapped to port 8/8.
 Ifindex 44 is mapped to port 8/9.
 Ifindex 45 is mapped to FEC-1/1-2.
Console>
```

show igmp flooding

To display whether the IGMP flooding feature is enabled or disabled, use the **show igmp flooding** command.

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Using the IGMP flooding feature, you can activate or prevent the flooding of multicast traffic after the last host leaves a multicast group.

For more information about IGMP flooding, refer to the "Understanding How IGMP Snooping Works" section of the "Configuring Multicast Services" chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example show how to display the status of the IGMP flooding feature:

```
Console> show igmp flooding
Mcast flooding disabled
Console>
```

Related Commands

set igmp flooding

show igmp gda_status

To display the active multicast groups that are included in a Group Destination Address (GDA) in a particular VLAN for which there is a Layer 2 CAM entry created, use the **show igmp gda_status** command.

show igmp gda_status *vlan mac_addr*

Syntax Description

vlan	Number of the VLAN that forms the Layer 2 CAM entry.
mac_addr	MAC address of the GDA.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal mode.

Examples

This example shows how to display the active group IP addresses in VLAN 1 and the GDA with the specified MAC address:

```
Console> show igmp gda_status 1 01-00-5e-0a-0a-0a
Multicast-Groups active under this GDA are:
    232.10.10.10
Console>
```

This example shows how to display the active group IP addresses in VLAN 100 and the GDA with the specified MAC address:

```
Console> show igmp gda_status 100 01-00-5e-00-01-28
Multicast-Groups active under this GDA are:
    224.0.1.40
Console>
```

Related Commands

show multicast group

show igmp leave-query-type

To display the type of query to be sent when a port receives a leave message, use the **show igmp leave-query-type** command.

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the type of IGMP query that is sent when a port receives a leave message:

```
Console> show igmp leave-query-type
IGMP Leave Query Type : Mac based General Query
Console>
```

Related Commands

set igmp leave-query-type

show igmp mode

To display the IGMP mode on the switch, use the **show igmp mode** command.

show igmp mode

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The switch dynamically chooses either IGMP-only or IGMP-CGMP mode, depending on the traffic present on the network. IGMP-only mode is used in networks with no CGMP devices. IGMP-CGMP mode is used in networks with both IGMP and CGMP devices.

The **show igmp mode** command output includes three fields:

- IGMP Mode—Possible values are auto, igmp-only, and igmp-cgmp.
- IGMP-Operational-Mode—Possible values are igmp-only and igmp-cgmp.
- IGMP Address Aliasing Mode—Possible values are normal and fallback.

Examples

This example shows how to display the IGMP mode:

```
Console> show igmp mode
IGMP Mode:                  auto
IGMP Operational Mode:      igmp-only
IGMP Address Aliasing Mode: normal
Console>
```

Related Commands

set igmp mode

show igmp querier information

To display querier information specific to a configured VLAN, use the **show igmp querier information** command.

show igmp querier information [*vlan*]

Syntax Description

vlan	(Optional) Number of the VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a VLAN number, IGMP querier information is displayed for all configured VLANs.

Examples

This example shows how to display querier information for VLAN 1:

```
Console> show igmp querier information 1
VLAN Querier State         Query Tx Count QI (seconds) OQI (seconds)
---- --------------------- -------------- ------------ -------------
1    QUERIER               26             125          300
Console>
```

Related Commands

set igmp querier

show igmp statistics

To view IGMP statistics for a particular VLAN, use the **show igmp statistics** command.

show igmp statistics [*vlan_id*]

Syntax Description

vlan_id	(Optional) VLAN for which to show IGMP statistics; valid values are from 1 to 4094.

Defaults

The default is that if you do not specify a VLAN, statistics for VLAN 1 are shown.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to view IGMP statistics for VLAN 1:

```
Console> show igmp statistics 1
IGMP enabled

IGMP statistics for vlan 1:
Total valid pkts rcvd:           18951
Total invalid pkts recvd         0
General Queries recvd            377
Group Specific Queries recvd     0
MAC-Based General Queries recvd  0
Leaves recvd                     14
Reports recvd                    16741
Queries  Xmitted                 0
GS Queries Xmitted               16
Reports Xmitted                  0
Leaves Xmitted                   0
Failures to add GDA to EARL      0
Topology Notifications rcvd      10
IGMP packets dropped             0
Console>
```

Table 2-37 describes the fields in the **show igmp statistics** output.

Table 2-37 show igmp statistics Command Output Fields

Field	Description
IGMP enabled	Status of whether IGMP snooping is enabled or disabled.
Total valid pkts rcvd	Number of valid IGMP packets received.
Total invalid pkts recvd	Number of invalid IGMP packets received.
General Queries recvd	Number of IGMP general queries received.
Group Specific Queries recvd	Number of IGMP group-specific queries received.

Table 2-37 show igmp statistics Command Output Fields (continued)

Field	Description
MAC-Based General Queries recvd	Number of MAC-based general queries received.
Leaves recvd	Number of IGMP leaves received.
Reports recvd	Number of IGMP reports received.
Queries Xmitted	Number of IGMP general queries transmitted by the switch.
GS Queries Xmitted	Number of IGMP group-specific equivalent queries transmitted by the switch.
Reports Xmitted	Number of IGMP reports transmitted by the switch.
Leaves Xmitted	Number of IGMP leaves transmitted by the switch.
Failures to add GDA to EARL	Number of times the switch failed to add a multicast entry (GDA) to the EARL table.
Topology Notifications rcvd	Number of topology change notifications received by the switch.
IGMP packets dropped	Number of IGMP packets dropped by the switch.

Related Commands

clear igmp statistics
clear multicast router
set igmp
set multicast router
show multicast group
show multicast router

show imagemib

To display image information provided in the CISCO-IMAGE-MIB for a particular image, use the **show imagemib** command.

show imagemib *filename*

Syntax Description

filename	Name of the Flash device on the supervisor engine.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display CISCO-IMAGE-MIB information for the Flash image:

```
Console> (enable) show imagemib bootflash:cat6000-sup.6-1-1.bin
show mib info for file bootflash:cn50
CW_BEGIN$cat6000-WS-X6K-SUP1$
CW_IMAGE$bootflash:at6000-sup.5-5-1.bin$
CW_FAMILY$Catalyst 6000 Switch$
CW_MODULE$Catalyst Supervisor Module$
CW_VERSION$5.5.1$
CW_MIN_DRAM$ 32 MB$
CW_MIN_BOOTFLASH$  8 MB$
CW_MIN_NVRAM$ 512 KB$
CW_BUILDTIME$  Mar 24 2000 00:32:33$
CW_SYSDESCR$Catalyst Operating System$
CW_END$cat6000-WS-X6K-SUP1$
Console>
```

show image-verification

To display the status of the image verification feature, use the **show image-verifcation** command.

show image-verification

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command shows whether or not the integrity of the image will be verified when the system is booting, after the image has been copied, or before a system resets.

Examples

This example shows how to display the status of the image verification feature:

```
Console> show image-verification
Image Verification Status:
Boot:  Enable
Copy:  Disable
Reset: Disable
Console> (enable)
```

show inlinepower

To display status of inline power for all modules, use the **show inlinepower** command.

show inlinepower

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the inline power for all modules that are configured for inline power:

```
Console> show inlinepower
Configured Default Inline Power allocation per port:15.40 Watts ( 0.37 Amps @42V)

Mod         Ports        Notify-Thld    Inline Power (Watts)   Usage Status
    on deny errdis off  (% of Max)   Max     Thld    Admin
---  -- ---- ------ ---  -----------  ------- ------- ------- ------------
4    1  0    0      95   99           800.10  792.09  7.07     Ok
6    0  0    0      48   99           378.00  374.22  0.00     Ok

(*) "errdis" ports are static ports with insufficient power

Console>
```

Table 2-38 describes the fields in the **show inlinepower** output.

Table 2-38 show inlinepower Command Output Fields

Field	Description
Mod	Module number.
Ports on	Number of ports that are operational.
Ports deny	Number of ports that are denied power.
Ports errdis	Number of ports that are static and that have insufficient power.
Ports off	Number of ports that are not operational.
Notify-Thld (% of Max)	Percentage of power usage that must be reached before a syslog notification goes out.
Inline Power Max	Maximum wattage that is allocated to the module.
Inline Power Thld	Wattage that must be reached before a syslong notification goes out.

Table 2-38 show inlinepower Command Output Fields (continued)

Field	Description
Inline Power Admin	Total power that is allocated to the ports on the module.
Usage Status	Status of the inline power on the module: • OK—The module is below the inline power threshold. • Over-Thld—The module is over the inline power threshold. • OFF—The module is not operational.

Related Commands

set inlinepower
set port inlinepower
show port inlinepower

show interface

To display information on network interfaces, use the **show interface** command.

show interface

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display sl0 and sc0:

```
Console> show interface
sl0: flags=51<UP,POINTOPOINT,RUNNING>
        slip 0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
        vlan 1 inet 172.20.52.19 netmask 255.255.255.224 broadcast 172.20.52.31
sc1: flags=63<UP,BROADCAST,RUNNING>
        vlan 2 inet 0.0.0.0 netmask 255.0.0.0 broadcast 0.255.255.255
dhcp server: 174.44.67.201
Console>
```

Table 2-39 describes the fields in the **show interface** command output.

Table 2-39 show interface Command Output Fields

Field	Description
sl0	Information on the SLIP interface.
flags	Flags indicating the interface state (decoded in the subsequent field).
<UP, POINTOPOINT, RUNNING>	Interface state (UP, DOWN, BROADCAST, LOOPBACK, POINTOPOINT, or RUNNING).
slip	IP address of the SLIP interface.

Table 2-39 show interface Command Output Fields (continued)

Field	Description
dest	IP address of the host to which the console port will be connected.
sc0	Information on the sc0 in-band interface.
vlan	Number of the VLAN to which the sc0 interface has been assigned (known as the management VLAN).
inet	IP address of the interface.
netmask	Network mask for the interface.
broadcast	Broadcast address for the interface.
sc1	Information on the sc1 in-band interface.
dhcp server	IP address of the DHCP server.

Related Commands

set interface

show inventory

To display the product inventory listing of all Cisco products that are installed in a networking device, use the **show inventory** command.

show inventory [*entity*]

Syntax Description

entity	(Optional) Name of a Cisco entity (for example, chassis, backplane, module, or slot).

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **show inventory** command retrieves and displays inventory information about each Cisco product in the form of a Cisco Unique Device Indentifier (UDI). The UDI is a combination of three separate data elements: a product identifier (PID), a version identifier (VID), and the serial number (SN).

The PID is the name by which the product can be ordered and is also called the "Product Name" or "Part Number." You can use this identifier to order an exact replacement part. The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The SN is the vendor-unique serialization of the product. Each manufactured product carries a unique serial number assigned at the factory; this number identifies a specific instance of a product. This number cannot be changed in the field.

The UDI refers to each product as an entity. Some entities, such as a chassis, have subentities, such as slots. Each entity displays on a separate line.

Examples

The following is sample output from the **show inventory** command without any arguments.

```
Console> show inventory
NAME: "Chassis", DESCR: "Cisco Systems WS-C6509 9 slot switch"
PID: WS-C6509          , VID:    , SN: SCA034401LQ

NAME: "Clock 1", DESCR: "Clock"
PID: WS-C6000-CL       , VID:    , SN: SMT03462479

NAME: "Clock 2", DESCR: "Clock"
PID: WS-C6000-CL       , VID:    , SN: SMT03462480

NAME: "VTT 1", DESCR: "VTT"
PID: WS-C6000-VTT      , VID:    , SN: SMT03460976

NAME: "VTT 2", DESCR: "VTT"
PID: WS-C6000-VTT      , VID:    , SN: SMT03460843

NAME: "VTT 3", DESCR: "VTT"
```

```
PID: WS-C6000-VTT      , VID:    , SN: SMT03461008

NAME: "2", DESCR: "1000BaseX Supervisor 2 port WS-X6K-SUP2-2GE Rev. 1.1"
PID: WS-X6K-SUP2-2GE   , VID:    , SN: SAD04450LF1

NAME: "submodule 2/1", DESCR: "L3 Switching Engine II"
PID: WS-F6K-PFC2       , VID:    , SN: SAD04440HVU

NAME: "3", DESCR: "10/100BaseTX Ethernet 48 port WS-X6248-RJ-45 Rev. 1.0"
PID: WS-X6248-RJ-45    , VID:    , SN: SAD03181468

NAME: "5", DESCR: "Switch Fabric Module 0 port WS-C6500-SFM Rev. 1.0"
PID: WS-C6500-SFM      , VID:    , SN: SAD04420JR5

NAME: "7", DESCR: "Network Analysis Module 2 port WS-X6380-NAM Rev. 0.201"
PID: WS-X6380-NAM      , VID:    , SN: JAB0343055Y

NAME: "8", DESCR: "1000BaseX Ethernet 8 port WS-X6408-GBIC Rev. 0.202"
PID: WS-X6408-GBIC     , VID:    , SN: SAD02430406

NAME: "PS 1", DESCR: "1300 watt supply AC"
PID: WS-CAC-1300W      , VID:    , SN: ACP03380477

NAME: "Fan 1", DESCR: "Fan 1"
PID: WS-C6K-9SLOT-FAN  , VID:    , SN:

Console>
```

Table 2-40 describes the fields in the **show inventory** command output.

Table 2-40 show inventory Command Output Fields

Field	Description
NAME	Physical name (text string) assigned to the Cisco entity. For example, console or a simple component number (port or module number), such as “1,” depending on the physical component naming syntax of the device. Equivalent to the entPhysicalName MIB variable in RFC 2737.
DESCR	Physical description of the Cisco entity that characterizes the object. Equivalent to the entPhysicalDesc MIB variable in RFC 2737.
PID	Entity product identifier. Equivalent to the entPhysicalModelName MIB variable in RFC 2737.
VID	Entity version identifier. Equivalent to the entPhysicalHardwareRev MIB variable in RFC 2737.
SN	Entity serial number. Equivalent to the entPhysicalSerialNum MIB variable in RFC 2737.

show ip alias

To show a listing of defined IP aliases, use the **show ip alias** command.

show ip alias [*name*]

Syntax Description

name	(Optional) Alias for a specific host.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display a listing of all IP aliases:

```
Console> show ip alias
default         0.0.0.0
sparc20         192.168.10.69
cat6000-1       172.16.169.16
cat6000-2       172.16.169.20
Console>
```

Related Commands

clear ip alias
set ip alias

show ip dns

To show the DNS name servers and the default DNS domain name, use the **show ip dns** command.

show ip dns

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the DNS name servers and the default DNS domain name:

```
Console> show ip dns
DNS is currently enabled.
The default DNS domain name is: cisco.com

DNS name server            status
---------------            -------
172.16.30.32
192.168.2.132              primary
172.31.128.70
Console>
```

Table 2-41 describes the fields in the **show ip dns** command output.

Table 2-41 show ip dns Command Output Fields

Field	Description
DNS is currently enabled	Status of whether DNS is enabled or disabled.
default DNS domain name	Default DNS domain name.
DNS name server	IP addresses or IP aliases of the configured DNS servers.
status	Primary DNS server.

Related Commands

clear ip dns domain
clear ip dns server
set ip dns
set ip dns domain
set ip dns server

show ip http

To view the HTTP configuration and the switch web interface information, use the **show ip http** command.

show ip http

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the HTTP configuration and web interface information if the web interface is supported:

```
Console> show ip http
HTTP Configuration Information:
----------------
HTTP Server: enabled
HTTP port: 80
Web Interface: Supported

Switch Information:
------------------
File:  applet.html
       size: 912 bytes
       version: 5.0(0.26)
       date: 10/9/99
File:  cvembopt.jar
       size: 3500000 bytes
       version: 5.0(0.26)
       date: 10/9/99

Active Web Interface Session: 1
-----------------------------
Client IP Address: 192.20.20.45
Request Type: GET
Request URI: /all-engine.jar
Console>
```

This example shows the HTTP configuration and web interface information if the web interface is not supported:

```
Console> show ip http
HTTP Configuration Information:
----------------
HTTP Server: disabled
HTTP port: 80
Web Interface: Not Supported
Console>
```

Related Commands

set ip http port
set ip http server

show ip permit

To display the IP permit list information, use the **show ip permit** command.

show ip permit [**noalias**]

Syntax Description

noalias	(Optional) Forces the display to show IP addresses, not IP aliases.

Defaults

This command has no default value.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the IP permit list information:

```
Console> (enable) show ip permit
Telnet permit list feature enabled.
Ssh permit list enabled.
Snmp permit list feature disabled.

Permit List          Mask               Access-Type
----------------     ---------------    ---------------
172.16.0.0         255.255.0.0          telnet
172.20.52.3                             snmp telnet
172.20.52.32       255.255.255.224      snmp

Denied IP Address   Last Accessed Time Type
-----------------   ------------------ ------
172.100.101.104     01/20/97,07:45:20  SNMP
172.187.206.222     01/21/97,14:23:05  Telnet

Console> (enable)
```

Table 2-42 describes the fields in the **show ip permit** command output.

Table 2-42 show ip permit Command Output Fields

Field	Description
IP permit list feature enabled	Status of whether the IP permit list feature is enabled or disabled.
Permit List	IP addresses and IP aliases that are allowed to access the switch.
Mask	Subnet masks of permitted IP addresses.
Denied IP Address	IP addresses and IP aliases that are not allowed to access the switch.

Table 2-42 show ip permit Command Output Fields (continued)

Field	Description
Last Accessed Time	Date and time of the last attempt to log in to the switch from the address.
Type	Login-attempt type.

Related Commands

clear ip permit
set ip permit
set snmp trap

show ip route

To display IP routing table entries, use the **show ip route** command.

show ip route [**noalias**]

Syntax Description

noalias	(Optional) Forces the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the IP route table:

```
Console> show ip route
Fragmentation   Redirect   Unreachable
-------------   --------   -----------
enabled         enabled    enabled

Destination      Gateway          RouteMask    Flags   Use       Interface
---------------  ---------------  ----------   -----   --------  ---------
172.20.0.0       172.20.26.70     0xffff0000   U       8          sc0
default          default          0xff000000   UH      0          sl0
Console>
```

Table 2-43 describes the fields in the **show ip route** command output.

Table 2-43 show ip route Command Output Fields

Field	Description
Fragmentation	Current setting of IP fragmentation.
Redirect	Current setting of ICMP redirect.
Unreachable	Current setting of ICMP unreachable messages.
Destination	Destination address IP route mask.
Gateway	IP address or IP alias of the gateway router.
RouteMask	Determines which path is closer to the destination.
Flags	Route status; possible values are U=up, G=route to a Gateway, H=route to a Host, and D=Dynamically created by a redirect.
Use	Number of times a route entry was used to route packets.
Interface	Type of interface.

Related Commands

clear ip route
set ip route

show ip telnet

To display whether the Telnet server is enabled or disabled, use the **show ip telnet** command.

show ip telnet

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows to display the status of the Telnet server:

```
Console> (enable) show ip telnet
Telnet Server :   enabled
Console> (enable)
```

Related Commands

set ip telnet server

show kerberos

To display the Kerberos configuration information, use the **show kerberos** command.

show kerberos [**creds**]

Syntax Description

creds	(Optional) Displays credential information only.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display Kerberos configuration information:

```
Console> (enable) show kerberos
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM,  Server:187.0.2.1,  Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com,  Realm:CISCO.COM

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Enabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Srvtab Entry 1:host/niners.cisco.com@CISCO.COM 0 932423923 1 1 8 01;;8>00>50;0=0=0
Console> (enable)
```

Table 2-44 describes the fields in the **show kerberos** command output.

Table 2-44 show kerberos Command Output Fields

Field	Description
Kerberos Local Realm	Status of whether or not the local realm is configured.
Kerberos server entries	Status of servers entered into the switch.
Kerberos Domain<->Realm entries	Kerberos domain and realm entries.
Kerberos Clients NOT Mandatory	Status of whether or not Kerberos has been configured as mandatory on the clients.

Table 2-44 show kerberos Command Output Fields (continued)

Field	Description
Kerberos Credentials Forwarding Disabled	Status of whether credentials forwarding is enabled or disabled.
Kerberos Pre Authentication Method	Status of whether preauthentication is enabled or disabled.
Kerberos config key	Status of whether or not a 3DES key has been configured.
Kerberos SRVTAB entries	SRVTAB entries.

Related Commands

clear kerberos clients mandatory
clear kerberos credentials forward
clear kerberos realm
clear kerberos server
clear key config-key
set kerberos clients mandatory
set kerberos credentials forward
set kerberos local-realm
set kerberos realm
set kerberos srvtab entry
set kerberos srvtab remote
set key config-key

show l2protocol-tunnel statistics

To display Layer 2 protocol tunneling statistics for a port or range or ports, use the **show l2protocol-tunnel statistic**s command.

show l2protocol-tunnel statistics [*mod*[*/port*]]

show l2protocol-tunnel statistics *mod/port* **vlan** *vlan*

Syntax Description

mod[*/port*]	(Optional) Number of the module and the number of the port or range of ports on the module. See the “Usage Guidelines” section for more information.
vlan	Displays Layer 2 protocol tunneling statistics on a VLAN. See the “Usage Guidelines” section for more information.
vlan	VLAN number.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a module and a port or range of ports, Layer 2 protocol tunneling statistics are displayed for all tunneling ports. If you only specify a module, Layer 2 protocol tunneling statistics are displayed for all tunneling ports on the module.

If you want to specify a VLAN, you must also specify a module number and a port number.

Examples

This example shows how to display Layer 2 protocol tunneling statistics for a range of ports:

```
Console> show l2protocol-tunnel statistics 7/1-2
Tunneling CoS is set to 5.

Port                     CDP Frames Encap     CDP Frames De-encap
------------------------ -------------------- --------------------
 7/1                                        2                    2
 7/2                                        2                    2

Port                     STP Frames Encap     STP Frames De-encap
------------------------ -------------------- --------------------
 7/1                                        0                    0
 7/2                                        0                    0

Port                     VTP Frames Encap     VTP Frames De-encap
------------------------ -------------------- --------------------
 7/1                                        0                    0
 7/2                                        0                    0
```

```
Port                     EOAM Frames Encap    EOAM Frames De-encap
------------------------ -------------------- --------------------
 7/1                                        0                    0
 7/2                                        0                    0
Console>
```

This example shows how to display Layer 2 protocol tunneling statistics for a port:

```
Console> show l2protocol-tunnel statistics 7/1
Tunneling CoS is set to 5.

Port                     CDP Frames Encap     CDP Frames De-encap
------------------------ -------------------- --------------------
 7/1                                        2                    2

Port                     STP Frames Encap     STP Frames De-encap
------------------------ -------------------- --------------------
 7/1                                        0                    0

Port                     VTP Frames Encap     VTP Frames De-encap
------------------------ -------------------- --------------------
 7/1                                        0                    0

Port                     EOAM Frames Encap    EOAM Frames De-encap
------------------------ -------------------- --------------------
 7/1                                        0                    0
Console>
```

Related Commands

clear l2protocol-tunnel cos
clear l2protocol-tunnel statistics
set l2protocol-tunnel cos
set port l2protocol-tunnel
show port l2protocol-tunnel

show lacp-channel

To display information about the Link Aggregation Control Protocol (LACP) channel, use the **show lacp-channel** command.

show lacp-channel

show lacp-channel sys-id

show lacp-channel group [*admin-key*] [**info** [*type*] | **statistics**]

show lacp-channel [*channel_id*] [**info** [*type*] | **statistics** | **mac**]

show lacp-channel hash *channel_id* {{*src_ip_addr* [*dest_ip_addr*]} | *dest_ip_addr* | {*src_mac_addr* [*dest_mac_addr*]} | *dest_mac_addr* | {*src_port dest_port*} | *dest_port*}

show lacp-channel traffic [*channel_id*]

Syntax Description

sys-id	Displays the system identifier adopted by LACP.
group	Displays all the ports that belong to a channel.
admin-key	(Optional) Number of the administrative key; valid values are from 1 to 65535.
info	(Optional) Displays detailed LACP channel information.
type	(Optional) Name of the feature-related parameter; valid values are **auxiliaryvlan**, **cops**, **dot1qtunnel**, **gmrp**, **gvrp**, **jumbo**, **protocol**, **qos**, **rsvp**, **spantree**, **trunk**.
statistics	(Optional) Displays LACP statistics.
channel_id	(Optional) Number of the channel; valid values are from 769 to 896.
mac	(Optional) Specifies MAC information about the channel.
hash	Displays the outgoing port used in a channel for a specific address or Layer 4 port number.
src_ip_addr	Source IP address.
dest_ip_addr	(Optional) Destination IP address.
src_mac_addr	Source MAC address.
dest_mac_addr	(Optional) Destination MAC address.
src_port	Number of the source port; valid values are from 0 to 65535.
dest_port	Number of the destination port; valid values are from 0 to 65535.
traffic	Displays traffic utilization on channel ports.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify the *admin-key* value, information about all LACP channels is displayed.

If you do not specify the *channel_id* value, information about all LACP channels is displayed.

For differences between PAgP and LACP, refer to the “Guidelines for Port Configuration” section of the “Configuring EtherChannel” chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example shows how to display information about all LACP channels:

```
Console> show lacp-channel group
Admin Key    Ports
-----------  ------
69           4/1-2
70           4/5-6
143          2/1-2
151          4/3-4
152          4/7-8
Console>
```

This example shows how to display limited information about ports that are assigned to administrative key 152:

```
Console> show lacp-channel group 152
Port  Channel   Admin Ch   Partner Oper                         Partner
      Mode      Key    id  Sys ID                               Port
----- --------- ----- ---- --------------------------------- -------
 4/7   active     152   770  8000,AC-12-24-56-78-90           4/3
 4/8   active     152   770  8000,AC-12-24-56-78-90           4/4
Console>
```

This example shows how to display detailed information about ports that are assigned to administrative key 152:

```
Console> show lacp-channel group 152 info
I = Isolated Port.  C = Channeling Port.  N = Not Connected.
H = Hot Stand-by Port.  S = Suspended Port.

Port  LACP Port Port  Speed Duplex VLANs  Trunk status Port  STP Port PortSecurity/
      Priority  Status                                Cost  Priority Dynamic Port
----- --------- ----- ----- ------ ------- ------------ ----- -------- ------------
 4/7  130       C      1000  full   1-1005 not-trunking    4      32
 4/8  131       C      1000  full   1-1005 not-trunking    4      32

Port  Admin Channel if-   Partner Oper              Partner     Partner   Partner
       Key  id      Index Sys ID                    Port Prior  Port      Oper Key
----- ----- ------- ----- ------------------------- ----------  --------  ----------
 4/7  152   770     31    800,AC-12-24-56-78-90     248          4/3       15768
 4/8  152   770     31    800,AC-12-24-56-78-90     249          4/4       15768
Console>
```

This example shows how to display LACP Tx and Rx statistics for ports that are assigned to administrative key 152:

```
Console> show lacp-channel group 152 statistics
Port  Admin    LACP Pkts  LACP Pkts Marker Pkts Marker Pkts LACP Pkts
       Key    Transmitted Received  Transmitted   Received    Errors
----- ------- ----------- --------- ----------- ----------- ---------
 4/7    152           0        92         0         0         0
 4/8    152           0         0         0         0         0
Console>
```

This example shows how to display all ports that are assigned to an administrative key:

```
Console> show lacp-channel group info
I = Isolated Port.  C = Channeling Port.  N = Not Connected.
H = Hot Stand-by Port.  S = Suspended Port.

Port  LACP Port Port  Speed Duplex VLANs  Trunk status Port  STP Port PortSecurity/
      Priority  Status                                 Cost  Priority Dynamic Port
----- --------- ----- ----- ------ ------ ------------ ----- -------- ------------
 4/1  50        I     1000  full   1-1005 not-trunking     4       32
 4/2  51        I     1000  full   1-1005 not-trunking     4       32
 4/5  27        I     1000  full   1-1005 not-trunking     4       32
 4/6  28         I    1000  full   1-1005  not-trunking     4      32
 2/1  133       C     1000  full   1-1005 not-trunking     4       32
 2/2  134       C     1000  full   1-1005 not-trunking     4       32
 4/3  200       C     1000  full   1-1005 not-trunking     4       32
 4/4  201       C     1000  full   1-1005 not-trunking     4       32
 4/7  130       C     1000  full   1-1005 not-trunking     4       32
 4/8  131       C     1000  full   1-1005 not-trunking     4       32

Port  Admin   Channel if-   Partner Oper                Partner    Partner  Partner
       Key    id      Index Sys ID                      Port Prior Port     Oper Key
----- ------- ------- ----- -------------------------- ----------- ------- --------
 4/1  69      0       -     0,00-00-00-00-00-00         0          3/1     0
 4/2  69      0       -     0,00-00-00-00-00-00         0          4/5     0
 4/5  70      0       -     0,00-00-00-00-00-00         0          7/3     0
 4/6  70      0       -     0,00-00-00-00-00-00         0          7/4     0
 2/1  143     768     29    1276,45-12-24-AC-78-90      34         5/1     5658
 2/2  143     768     29    1276,45-12-24-AC-78-90      35         5/2     5658
 4/3  151     769     30    13459,89-BC-24-56-78-90     200        1/1     9768
 4/4  151     769     30    13459,89-BC-24-56-78-90     201        1/2     9768
 4/7  152     770     31    8000,AC-12-24-56-78-90      248        4/3     15678
 4/8  152     770     31    8000,AC-12-24-56-78-90      249        4/4     15768
Console>
```

This example shows how to display Tx and Rx statistics for all ports that are assigned to an administrative key:

```
Console> show lacp-channel group statistics
Port  Admin    LACP Pkts  LACP Pkts Marker Pkts Marker Pkts LACP Pkts
       Key    Transmitted Received  Transmitted   Received    Errors
----- ------- ----------- --------- ----------- ----------- ---------
 4/1       69           0         0         0         0         0
 4/2       69           0         0         0         0         0
 4/5       70           0         0         0         0         0
 4/6       70           0         0         0         0         0
 2/1      143           0         0         0         0         0
 2/2      143           0         0         0         0         0
 4/3      151           0         0         0         0         0
 4/4      151           0         0         0         0         0
 4/7      152           0        92         0         0         0
 4/8      152           0         0         0         0         0
Console>
```

This example shows how to display the outgoing port for the specified source and destination IP addresses:

```
Console> (enable) show lacp-channel hash 808 172.20.32.10 172.20.32.66
Selected channel port:2/17
Console> (enable)
```

This example shows how to display traffic utilization on channel ports:

```
Console> (enable) show lacp-channel traffic
ChanId Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ ----- ------- ------- ------- ------- ------- -------
   808  2/16   0.00%   0.00%  50.00%  75.75%   0.00%   0.00%
   808  2/17   0.00%   0.00%  50.00%  25.25%   0.00%   0.00%
   816  2/31   0.00%   0.00%  25.25%  50.50%   0.00%   0.00%
   816  2/32   0.00%   0.00%  75.75%  50.50%   0.00%   0.00%
Console> (enable)
```

Related Commands

clear lacp-channel statistics
set channelprotocol
set lacp-channel system-priority
set port lacp-channel
set spantree channelcost
set spantree channelvlancost
show port lacp-channel

show lcperroraction

To display how your system handles LCP errors when a module reports an ASIC problem to the Network Management Processor (NMP), use the **show lcperroraction** command.

show lcperroraction

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the action that handles an LCP error:

```
Console> (enable) show lcperroraction
LCP action level is: system
Console> (enable)
```

Related Commands

set lcperroraction

show lda

To display the ASLB configuration information, use the **show lda** command.

show lda [**committed** | **uncommitted**]

show lda mls entry

show lda mls entry [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*] [**short** | **long**]

show lda mls statistics count

show lda mls statistics entry

show lda mls statistics entry [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*]

Syntax Description

committed	(Optional) Views committed configuration information.
uncommitted	(Optional) Views configuration information that has not been committed.
mls entry	Displays the ASLB MLS entries.
destination *ip_addr_spec*	(Optional) Full destination IP address or a subnet address in these formats: *ip_addr*, *ip_addr/netmask,* or *ip_addr/maskbit*.
source *ip_addr_spec*	(Optional) Full source IP address or a subnet address in these formats: *ip_addr, ip_addr/netmask,* or *ip_addr/maskbit*.
protocol *protocol*	(Optional) Specifies additional flow information (protocol family and protocol port pair) to be matched; valid values include **tcp**, **udp**, **icmp**, or a decimal number for other protocol families.
src-port *src_port*	(Optional) Specifies the number of the TCP/UDP source port (decimal). Used with **dst-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates "do not care."
dst-port *dst_port*	(Optional) Specifies the number of the TCP/UDP destination port (decimal). Used with **src-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates "do not care."
short | **long**	(Optional) Specifies the width of the display.
count	Displays the number of active ASLB MLS entries.
mls statistics entry	Displays statistics information.

Defaults

The default displays MLS entry information in long format.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported only on switches configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card).

Entering the **destination** keyword specifies the entries matching the destination IP address specification, entering the **source** keyword specifies the entries matching the source IP address specification, and entering an *ip_addr_spec* can specify a full IP address or a subnet address. If you do not specify a keyword, it is treated as a wildcard, and all entries are displayed.

When entering the *ip_addr_spec* value, use the full IP address or a subnet address in one of the following formats: *ip_addr*, *ip_addr/netmask,* or *ip_addr/maskbit*.

Entering the **destination** keyword specifies the entries matching the destination IP address specification, entering the **source** keyword specifies the entries matching the source IP address specification, and entering an *ip_addr_spec* can specify a full IP address or a subnet address. If you do not specify a keyword, it is treated as a wildcard, and all entries are displayed.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the short subnet address format. The trailing decimal number 00 in an IP address YY.YY.YY.00 specifies the boundary for an IP subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 173.24.00.00/255.255.0.0). However, this format can identify only a subnet address with a length of 8, 16, or 24 bits.
- *ip_addr/subnet_mask*—This is the long subnet address format. For example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip_addr* value is allowed to be a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip_addr* value is allowed to be a full host address, such as 172.22.254.1/22, which has the same subnet address as 172.22.252.00/72.

If you have disabled the ASLB feature, you can view the last configuration using the **show lda uncommitted** command.

The **short | long** options give the flexibility to display the output in regular (80 characters in width) or wide screen.

If you enter the **show lda mls entry** or the **show lda mls statistics entry** command with no keywords or variables, all entries are displayed.

Examples

This example shows how to display committed ASLB information:

```
Console> (enable) show lda committed
Status:Committed

Local Director Flow:10.0.0.8/ (TCP port 8)
Router MAC:
00-02-03-04-05-06
00-04-56-67-04-05
00-03-32-02-03-03

LD MAC:00-02-03-04-05-06
LD Router Side:
---------------
Router and LD are on VLAN 110
LD is connected to switch port 4/26 on VLAN 110
LD Server Side:
---------------
Server(s) and LD are on VLAN 105
LD is connected to switch port 4/40 on VLAN 105
Console> (enable)
```

This example shows how to display uncommitted ASLB information:

```
Console> (enable) show lda uncommitted
Status:Not Committed.

Router MAC:
00-02-03-04-05-06
00-04-56-67-04-05
00-03-32-02-03-03

LD MAC:00-02-03-04-05-06

LD Router Side:
----------------

LD Server Side:
----------------
Console> (enable)
```

Note The examples shown for the **show lda mls entry** commands are displayed in short format. The display in the long form exceeds the page width and cannot be shown.

This example shows how to display ASLB MLS entries in short format:

```
Console> (enable) show lda mls entry short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan
--------------- --------------- ----- ------ ------ ----------------- ----
EDst ESrc DPort  SPort  Stat-Pkts  Stat-Bytes  Uptime   Age
---- ---- ------ ------ ---------- ----------- -------- --------
10.0.0.8        172.20.20.10    TCP  8      64     00-33-66-99-22-44 105
ARPA ARPA -      4/25   0          0          00:00:02 00:00:05

10.0.0.8        172.20.20.11    TCP  8      64     00-33-66-99-22-44 105
ARPA ARPA -      4/25   0          0          00:00:05 00:00:08
Console> (enable)
```

This example shows how to display ASLB information for the source IP address in short format:

```
Console> (enable) show lda mls entry source 172.20.20.11 short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan
--------------- --------------- ----- ------ ------ ----------------- ----
EDst ESrc DPort  SPort  Stat-Pkts  Stat-Bytes  Uptime   Age
---- ---- ------ ------ ---------- ----------- -------- --------
10.0.0.8        172.20.20.11    TCP  8      64     00-33-66-99-22-44 105
ARPA ARPA -      4/25   0          0          00:00:05 00:00:08
Console> (enable)
```

This example shows how to display the number of active ASLB MLS entries:

```
Console> (enable) show lda mls statistics count
LDA active shortcuts:20
Console> (enable)
```

This example shows how to display all ASLB MLS entry statistics:

```
Console> (enable) show lda mls statistics entry
                                  Last    Used
Destination IP  Source IP       Prot DstPrt SrcPrt Stat-Pkts  Stat-Bytes
--------------- --------------- ---- ------ ------ ---------- ---------------
10.0.0.8        172.20.20.10    TCP  WWW    64     636        29256
10.0.0.8        172.20.22.10    TCP  WWW    64     0          0
Console> (enable)
```

This example shows how to display the statistics for a specific destination IP address:

```
Console> (enable) show lda mls statistics entry destination 172.20.22.14
                Last Used         Last    Used
Destination IP  Source IP       Prot DstPrt SrcPrt Stat-Pkts  Stat-Bytes
--------------- --------------- ---- ------ ------ ---------- ---------------
172.20.22.14    172.20.25.10    6    50648  80     3152       347854
Console> (enable)
```

Related Commands

clear lda
commit lda
set lda

show localuser

To display the local user accounts for a switch, use the **show localuser** command.

show localuser [*name*]

Syntax Description

name	(Optional) Specifies the local user account.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display all local user accounts:

```
Console> (enable) show localuser
Local User Authentication: enabled
Username                        Privilege Level
---------                        -------------
picard                             15
number1                            0
worf                               15
troy                               0
Console> (enable)
```

This example shows how to display a specific local user account:

```
Console> (enable) show localuser troy
Local User Authentication: enabled
Username                        Privilege Level
---------                        -------------
troy                               0
Console> (enable)
```

Related Commands

clear localuser
set localuser

show log

To display the error log for the system or a specific module, use the **show log** command.

show log [*mod*]

show log dump [**-***count*]

Syntax Description

mod	(Optional) Number of the module for which the log is displayed.
dump	Displays dump log information.
-*count*	(Optional) Number of dump log entries to display.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

To display the contents of ASIC error messages as soon as they are received from SLCP or LCP, see the **set logging server** command.

You can use the **dump** keyword to display log dump information generated when certain events occur, such as memory corruption.

Examples

This example shows a partial display of the output from the **show log** command:

```
Console> show log

Network Management Processor (ACTIVE NMP) Log:
  Reset count:   10
  Re-boot History:   Mar 22 2000 10:34:09 0, Mar 17 2000 15:35:11 0
                     Mar 13 2000 17:40:16 0, Mar 13 2000 13:14:08 0
                     Mar 13 2000 11:57:30 0, Feb 24 2000 10:04:18 0
  Bootrom Checksum Failures:      0   UART Failures:                  0
  Flash Checksum Failures:        0   Flash Program Failures:         0
  Power Supply 1 Failures:        0   Power Supply 2 Failures:        0
  Swapped to CLKA:                0   Swapped to CLKB:                0
  Swapped to Processor 1:         0   Swapped to Processor 2:         0
  DRAM Failures:                  0

  Exceptions:                     0

  Last software reset by user: 3/13/2000,17:39:00

  EOBC Exceptions/Hang:            0

Heap Memory Log:
Corrupted Block = none
```

```
NVRAM log:

01. 1/25/2000,17:39:10: convertCiscoMIB:PreSac(0) checksum failed: 0xFFFF(0xE507
)

Module 3 Log:
  Reset Count:   14
  Reset History: Wed Mar 22 2000, 10:35:54
                 Fri Mar 17 2000, 15:36:57
                 Wed Mar 15 2000, 16:54:59
                 Tue Mar 14 2000, 16:02:19

<<<<output truncated >>>>
```

This example shows how to display dump log information:

```
Console> (enable) show log dump
Total logs: 1
Console> (enable)
```

Table 2-45 describes the possible fields in the output from the **show log** command.

Table 2-45 show log Command Output Fields

Field	Description
Network Management Processor (ACTIVE NMP) Log	Log that applies to the NMP on the supervisor engine.
Reset Count	Number of times the system has reset.
Re-boot History	Date and times the system has rebooted.
Bootrom Checksum Failures	Number of bootrom checksum failures.
UART Failures	Number of times the UART has failed.
Flash Checksum Failures	Number of times the Flash Checksum has failed.
Flash Program Failures	Number of times the Flash Program has failed.
Power Supply 1 Failures	Number of times Power Supply 1 has failed.
Power Supply 2 Failures	Number of times Power Supply 2 has failed.
Swapped to CLKA	Number of times a switchover to clock A has occurred.
Swapped to CLKB	Number of times a switchover to clock B has occurred.
Swapped to Processor 1	Number of times a switchover to processor 1 has occurred.
Swapped to Processor 2	Number of times a switchover to processor 2 has occurred.
DRAM Failures	Number of times the DRAM has failed.
Exceptions:	Exceptions log.
Last software reset by user	Date of the last time the software was reset.
NVRAM log	Number of times NVRAM errors have occurred.
Reset Count	Number of times the system has reset.
Reset History	Date and times the system has reset.
Total log	Number of entries.

Related Commands

clear log

show log command

To display the command log entries, use the **show log command** command.

show log command [*mod*]

Syntax Description

mod	(Optional) Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The command log entry table is a history log of commands input to the switch from the console, Telnet or SSH.

Examples

This example shows how to display the command log for a specific module:

```
Console> show log command
Active Command Log
001. Jul 19 13:49:44 Pid = 174 set logg cons ena
Session Type = Console TTY = 0 Username = Location =
002. Jul 19 13:49:51 Pid = 174 en engineer
Session Type = Console TTY = 0 Username = Location =
003. Jul 19 13:50:13 Pid = 174 start_op_console
Session Type = Telnet TTY = 22542919 Username = Location=172.20.16.10
004. Jul 19 13:50:15 Pid = 174 sh int
Session Type = Telnet TTY = 22542919 Username = Location = 172.20.16.10
005. Jul 19 13:50:16 Pid = 174 ena
Session Type = SSH TTY = 2254347796 Username = cisco Location = 10.5.7.62
006. Jul 19 13:50:18 Pid = 174 sh int
Session Type = Console TTY = 0 Username = Location =
007. Jul 19 13:51:55 Pid = 174 sh log comm
Session Type = SSH TTY = 2254347796 Username = Location = 10.5.7.62
008. Jul 19 13:52:09 Pid = 174 en eng
Session Type = Telnet TTY = 22542919 Username = cisco Location = 172.20.16.10
009. Jul 19 13:52:24 Pid = 174 set feature log-command disabl
Session Type = Console TTY = 0 Username = cisco Location =
010. Jul 19 13:52:42 Pid = 174 sh log command
Session Type = Console TTY = 0 Username = Location =
011. Jul 19 13:52:55 Pid = 174 sh log comma
Session Type = Telnet TTY = 22542919 Username = cisco Location = 172.20.16.10

Console>
```

Related Commands

clear log command

show logging

To display the system message log information, use the **show logging** command.

show logging [**noalias**]

Syntax Description

noalias	(Optional) Forces the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the default system message log configuration:

```
Console> show logging

Logging buffer size:          500
        timestamp option:     enabled
Logging history
Logging history
           size:                 1
           severity:             notifications(5)
Logging console:              enabled
Logging telnet:               enabled
Logging server:               disabled
        server facility:      LOCAL7
        server severity:      warnings(4)


Facility             Default Severity         Current Session Severity
-------------        -----------------------  ------------------------
acl                  7                        7
cdp                  6                        6
cops                 7                        7
dtp                  7                        7
dvlan                7                        7
earl                 7                        7
ethc                 7                        7
filesys              7                        7
gvrp                 7                        7
ip                   7                        7
kernel               7                        7
ld                   7                        7
mcast                7                        7
mgmt                 7                        7
mls                  7                        7
protfilt             7                        7
pruning              7                        7
privatevlan          7                        7
```

```
qos                 7                        7
radius              7                        7
rsvp                7                        7
security            7                        7
snmp                7                        7
spantree            7                        7
sys                 7                        7
tac                 7                        7
tcp                 7                        7
telnet              7                        7
tftp                7                        7
udld                7                        7
vmps                7                        7
vtp                 7                        7


0(emergencies)        1(alerts)             2(critical)
3(errors)             4(warnings)           5(notifications)
6(information)        7(debugging)
Console> (enable)
```

Table 2-46 describes the fields in the **show logging** command output.

Table 2-46 show logging Command Output Fields

Field	Description
Logging buffered size	Size of the logging buffer.
timestamp option	Status of whether the timestamp option is enabled or disabled.
Logging history size	Size of the logging history buffer.
Logging history severity	Severity level at which point errors are logged to the history table.
Logging console	Status of whether logging to the console is enabled or disabled.
Logging telnet	Status of whether logging to the Telnet session is enabled or disabled.
Logging server	Status of whether logging to the logging server is enabled or disabled.
Facility	Name of the facility to be logged.
Server/Severity	Severity level at which point an error from that facility is logged.
Current Session Severity	Severity level at which point an error from that facility is logged during the current session.
0 (emergencies), 1 (alerts)...	Key to the numeric severity level codes.

Related Commands

clear logging server
set logging console
set logging history
set logging level
set logging server
set logging session
show logging buffer

show logging buffer

To display system messages from the internal buffer, use the **show logging buffer** command.

show logging buffer [**–**] [*number_of_messages*]

Syntax Description

–	(Optional) Forces the display to show system messages starting from the end of the buffer.
number_of_messages	(Optional) Number of system messages to be displayed; valid values are from 1 to 1023.

Defaults

The default is –20 messages.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not enter the **–** keyword, system messages are displayed from the beginning of the buffer. If you do not specify the *number_of_messages*, all messages in the buffer are displayed.

Examples

This example shows how to display the first four system messages from the internal buffer:

```
Console> (enable) show logging buffer 4

1999 Dec 28 15:18:21 %SYS-1-SYS_NORMPWRMGMT:System in normal power management on
1999 Dec 28 15:18:24 %SYS-5-MOD_PWRON:Module 2 powered up
1999 Dec 28 15:18:31 %MLS-5-NDEDISABLED:Netflow Data Export disabled
1999 Dec 28 15:18:32 %MLS-5-MCAST_STATUS:IP Multicast Multilayer Switching is ed
Console> (enable)
```

This example shows how to display the last four system messages from the internal buffer:

```
Console> (enable) show logging buffer -4
1999 Dec 28 15:18:32 %MLS-5-MCAST_STATUS:IP Multicast Multilayer Switching is ed
1999 Dec 28 15:18:32 %SYS-5-MOD_OK:Module 1 is online
1999 Dec 28 15:19:07 %SYS-5-MOD_OK:Module 2 is online
1999 Dec 28 15:19:27 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
Console> (enable)
```

Related Commands

clear logging buffer
set logging buffer

show logging callhome

To display the configured CallHome settings, use the **show logging callhome** command.

show logging callhome

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the configured CallHome settings:

```
Console> (enable) show logging callhome
Callhome Functionality:       enabled
Callhome Severity:            LOG_ERR(3)
SMTP Server
-----------
172.20.8.16
Destination Address                                             Message Size
-------------------                                             ------------
adminboss@cisco.com                                             No Fragmentation
adminjane@cisco.com                                             No Fragmentation
adminjoe@epage.cisco                                            128 bytes
From: adminjoe@cisco.com
Reply-To: adminjane@cisco.com
0(emergencies)         1(alerts)              2(critical)
3(errors)              4(warnings)            5(notifications)
6(information)         7(debugging)
Console> (enable)
```

Table 2-47 describes the fields in the **show logging callhome** command output.

Table 2-47 show logging callhome Command Output Fields

Field	Description
CallHome functionality	Current setting of CallHome.
CallHome Severity	Severity level at which point syslog messages are sent to specified destination addresses.
SMTP Server	IP address of SMTP server(s) specified for CallHome.
Destination Address	E-mail or pager e-mail addresses for all recipients set to receive syslog messages.
Message Size	Message fragment size specified for each Destination Address.

Table 2-47 show logging callhome Command Output Fields (continued)

Field	Description
From:	E-mail address set to display as From address in the syslog messages sent.
Reply-To:	E-mail address set to display as the Reply-to address in the syslog messages sent.
0 (emergencies), 1 (alerts)...	Key to the numeric severity level codes.

Related Commands

clear logging callhome
clear logging callhome from
clear logging callhome reply-to
show logging callhome severity
clear logging callhome smtp-server
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome severity
set logging callhome smtp-server
show logging callhome destination
show logging callhome from
show logging callhome reply-to
show logging callhome severity
show logging callhome smtp-server

show logging callhome destination

To display the addresses set to receive CallHome syslog messages, use the **show logging callhome destination** command.

show logging callhome destination

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the destination addresses set to receive CallHome syslog messages:

```
Console> (enable) show logging callhome destination
Destination Address                                                Message Size
-------------------                                                ------------
adminboss@cisco.com                                                No Fragmentation
adminjane@cisco.com                                                No Fragmentation
adminjoe@epage.cisco                                               128 bytes
Console> (enable)
```

Table 2-48 describes the fields in the **show logging callhome destination** command output.

Table 2-48 show logging callhome destination Command Output Fields

Field	Description
Destination Address	E-mail or pager e-mail addresses for all recipients set to receive syslog messages.
Message Size	Message fragment size specified for each Destination Address.

Related Commands

clear logging callhome
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome severity
set logging callhome smtp-server
show logging
show logging callhome
show logging callhome from
show logging callhome reply-to
show logging callhome severity
show logging callhome smtp-server

8.6 EFT Copy

show logging callhome from

To display the From address in the CallHome syslog messages, use the **show logging callhome from** command.

show logging callhome from

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the From address in the CallHome syslog messages:

```
Console> (enable) show logging callhome from
From: adminjoe@cisco.com
Console> (enable)
```

Related Commands

clear logging callhome from
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome severity
set logging callhome smtp-server
show logging callhome
show logging callhome destination
show logging callhome reply-to
show logging callhome severity
show logging callhome smtp-server

show logging callhome reply-to

To display the Reply-to address in the CallHome syslog messages, use the **show logging callhome reply-to** command.

show logging callhome reply-to

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the Reply-to address in the CallHome syslog messages:

```
Console> (enable) show logging callhome reply-to
Reply-To: adminjane@cisco.com
Console> (enable)
```

Related Commands

clear logging callhome reply-to
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome severity
set logging callhome smtp-server
show logging callhome
show logging callhome destination
show logging callhome from
show logging callhome severity
show logging callhome smtp-server

show logging callhome severity

To display the severity level at which point syslog messages are sent to specified destination addresses, use the **show logging callhome severity** command.

show logging callhome severity

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the severity level at which point syslog messages are sent to specified destination addresses:

```
Console> (enable) show logging callhome
Callhome Severity:           LOG_ERR(3)
Console> (enable)
```

Related Commands

clear logging callhome severity
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome severity
show logging callhome
show logging callhome destination
show logging callhome from
show logging callhome reply-to
show logging callhome smtp-server

show logging callhome smtp-server

To display the SMTP servers set for CallHome to use when routing messages, use the **show logging callhome smtp-server** command.

show logging callhome smtp-server

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the SMTP servers set for CallHome to use when routing messages:

```
Console> (enable) show logging callhome smtp-server
SMTP Server
-----------
172.20.8.16
Console> (enable)
```

Related Commands

clear logging callhome smtp-server
set logging callhome
set logging callhome destination
set logging callhome from
set logging callhome reply-to
set logging callhome severity
set logging callhome smtp-server
show logging callhome
show logging callhome destination
show logging callhome from
show logging callhome reply-to
show logging callhome severity

show mac

To display MAC counters, use the **show mac** command.

show mac [**utilization**] [*mod*[/*port*]]

Syntax Description

utilization	(Optional) Displays approximated packet and byte rates.
mod/[/*port*]	(Optional) Number of the module and optionally, the number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **utilization** keyword is not supported on ATM ports.

If you do not specify a module number, all modules are shown. If you do not specify a port number, all ports are shown.

The Out-Discards field displays the number of outbound packets chosen to be discarded even though no errors had been detected to prevent being transmitted. For example, an outbound link is overwhelmed by switch traffic. Packets dropped are the ones destined for that port, but the port could not accept those packets due to XMT buffer overflow.

The Xmit-Packet-Rate, Xmit-Octet-Rate, Rcv-Packet-Rate, and Rcv-Octet-Rate fields display approximated average utilization rates rather than exact values. The approximated average is based on the previous approximation values, the last counter values read from hardware, the load time interval (fixed at 5 minutes), and the polling interval.

Examples

This example shows how to display MAC information for port 4 on module 3:

```
Console> show mac 3/4
MAC      Rcv-Frms   Xmit-Frms  Rcv-Multi  Xmit-Multi Rcv-Broad  Xmit-Broad
-------- ---------- ---------- ---------- ---------- ---------- ----------
3/4               0          0          0          0          0          0

MAC      Dely-Exced MTU-Exced  In-Discard Out-Discard
-------- ---------- ---------- ---------- -----------
3/4               0          0          0          0

MAC     SMT-Address       Curr-Path  TReq     TNeg     TMax     TVX
------- ----------------- ---------- -------- -------- -------- --------
3/4     00:06:7c:b3:bc:98 primary      165000   165000   165004     2509
        00-60-3e-cd-3d-19
```

```
MAC     SMT-Address       Curr-Path  TReq     TNeg     TMax     TVX
------- ----------------- ---------- -------- -------- -------- --------
3/4     00:06:7c:b3:bc:98 primary      165000   165000   165004     2509
        00-60-3e-cd-3d-19

MAC     Upstream-Nbr      Downstream-Nbr    Old-Upstrm-Nbr    Old-Downstrm-Nbr
------- ----------------- ----------------- ----------------- -----------------
3/4 00:00:1f:00:00:00 00:00:1f:00:00:00 00:00:1f:00:00:00 00:00:1f:00:00:00
        00-00-f8-00-00-00 00-00-f8-00-00-00 00-00-f8-00-00-00 00-00-f8-00-00-00

MAC     Rcv-Smt    Xmit-Smt   Rcv-llc    Xmit-llc   Tvx-Exp-Ct RingOp-Ct
------- ---------- ---------- ---------- ---------- ---------- ----------
3/4                  0             0            1           61             0            1

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
3/4                         0                    0                    0
Port     Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
3/4                         0                    0                    0
Port     Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------
3/4                         0                    0

MAC      Last-Time-Cleared
-------- --------------------------
5/40    Tue Mar 21 2000, 19:19:03
Console>
```

This command shows how to display approximated packet and byte rates:

```
Console> (enable) show mac utilization 1
5 min input/output port rates:

Port  Xmit-Packet-Rate     Xmit-Octet-Rate
----- -------------------- --------------------
1/1                  1343               123432
1/2                  2342               232343
Port  Rcv-Packet-Rate      Rcv-Octet-Rate
----- -------------------- --------------------
1/1                  1324               143253
1/2                  2234               253234
Console> (enable)
```

Table 2-49 describes the possible fields in the **show mac** command output.

Table 2-49 show mac Command Output Fields

Field	Description
MAC	Module and port.
Rcv-Frms	Frames received on the port.
Xmit-Frms	Frames transmitted on the port.
Rcv-Broad	Broadcast frames received on the port.
Xmit-Broad	Broadcast frames transmitted on the port.
Dely-Exced	Total transmit frames aborted due to excessive deferral.
MTU-Exced	Frames for which the MTU size was exceeded.

Table 2-49 show mac Command Output Fields (continued)

Field	Description
In-Discard	Incoming frames that were discarded because the frame did not need to be switched.
Out-Discard	Number of outbound packets chosen to be discarded even though no errors had been detected to prevent their being transmitted.
Curr-Path	Current path used (primary or secondary).
TVX	Value of the valid transmission timer.
Upstream-Nbr	MAC address of the current upstream neighbor.
Downstream-Nbr	MAC address of the current downstream neighbor.
Old-Upstrm-Nbr	MAC address of the previous upstream neighbor.
Old-Downstrm-Nbr	MAC address of the previous downstream neighbor.
Rcv-Smt	Number of SMT frames received by the port.
Xmit-Smt	Number of SMT frames transmitted by the port.
Rcv-llc	Number of NLLC frames received by the port.
Xmit-llc	Number of LLC frames transmitted by the port.
Rcv-Octet	Number of octet frames received on the port.
Xmit-Octet	Number of octet frames transmitted on the port.
Rcv-Unicast	Number of unicast frames received on the port.
Rcv-Broadcast	Number of broadcast frames received on the port.
Xmit-Unicast	Number of unicast frames transmitted on the port.
Xmit-Broadcast	Number of broadcast frames transmitted on the port.
Tvx-Exp-Ct	Number of times the TVX timer expired.
MAC Last-Time-Cleared	Module and port number and the date and time of the last time the software counters are cleared on this MAC.
Xmit-Packet-Rate	Number of packets transmitted.
Xmit-Octet-Rate	Number of bytes transmitted.
Rcv-Packet-Rate	Number of packets received.
Rcv-Octet-Rate	Number of bytes received.

show mac-auth-bypass

To display information about the MAC address authentication bypass feature for all ports that have the feature enabled or for a port with the specific MAC address, use the **show mac-auth-bypass** command.

show mac-auth-bypass config

show mac-auth-bypass {*mac_addr* | **all**}

Syntax Description

config	Displays the global settings for the MAC address authentication bypass feature, including the timer values, the violation mode, and the global reauthentication mode.
mac_addr	MAC address for the port.
all	Displays information for all ports that have the MAC address authentication bypass feature enabled.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display MAC address authentication bypass global configuration settings:

```
Console> show mac-auth-bypass config
Mac-Auth-Bypass Global Config
-----------------------------
Mac-Auth-Bypass Status      = Enabled
AuthFail Timeout            = 60
RadiusAccounting            = Enabled
Reauthentication            = Disabled
Reauth Timeout              = 3600
Shutdown Timeout            = 60
Violation mode              = Shutdown
Console>
```

This example shows how to display MAC address authentication bypass information for all ports in the switch that have the feature enabled:

```
Console> show mac-auth-bypass all

Port  Mac-Auth-Bypass State MAC Address       Auth-State     Vlan
----- --------------------- ----------------- -------------- -----
 5/1  Disabled              -                 -              1
 5/2  Enabled               00-00-00-00-00-00 waiting        1
 5/3  Enabled               00-00-00-00-00-00 waiting        1
 5/4  Enabled               00-00-00-00-00-00 waiting        1
 5/5  Enabled               00-00-00-00-00-00 waiting        1
 5/6  Enabled               00-00-00-00-00-00 waiting        1
 5/7  Enabled              00-00-00-00-00-00 waiting        1
 5/8  Enabled              00-00-00-00-00-00 waiting        1
.
.
.
Port  Termination action Session Timeout Shutdown/Time-Left
----- ------------------ --------------- ------------------
 5/1  -                  3600            -        -
 5/2  reauthenticate     3600            NO       -
 5/3  reauthenticate     3600            NO       -
 5/4  reauthenticate     3600            NO       -
 5/5  reauthenticate     3600            NO       -
 5/6  reauthenticate     3600            NO       -
 5/7  reauthenticate     3600            NO       -
 5/8  reauthenticate     3600            NO       -
.
.
.
Console> (enable)
```

Related Commands

set mac-auth-bypass
set port mac-auth-bypass
show port mac-auth-bypass

8.6 EFT Copy

show macro

To display user-defined SmartPorts macros and macro variables, use the **show macro** command.

show macro all

show macro name *macro_name* [**variables** [*mod/port*]]

show macro variable {**all** | **name** *variable_name* [*mod/port*]}

show macro map {**all** | **name** *macro_name* | **port** *mod/port*}

Syntax Description

all	Displays the names of all user-defined macros.
name	Displays the definition of a specific macro.
macro_name	Name of the macro.
variables	Displays variables in a user-defined macro.
mod/port	(Optional) Number of the module and the port on the module.
variable	Displays user-defined macro variables.
all	Displays all variables.
name	Displays a specific variable.
variable_name	Name of the variable.
map	Displays user-defined macros and their port mappings.
all	Displays all macros and port mappings.
name	Displays a specific macro and its port mappings.
port	Displays a specific port and its macros.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The macro and variable definitions are stored in NVRAM and can be displayed using the **show config** command.

If there is a macro inside a macro definition and if the root macro is applied on a port, the root macro is displayed using the **show macro map** command.

For more information about macros, including root macros, see the "Configuring a VoIP Network" chapter of the *Catalyst 6500 Series Software Configuration Guide*.

Examples

This example shows how to display the names of all the macros in the switch:

```
Console> show macro all
Macro Names
-----------
fileserver
videophone
Console>
```

This example shows how to display the definition of a specific macro:

```
Console> show macro name videophone

The macro definition for videophone is:

set port enable #MODPORT
set vlan $DATAVLAN #MODPORT
set port auxiliaryvlan #MODPORT $AUXVLAN
Console>
```

This example shows how to display all the macro variables in the switch:

```
Console> show macro variable all

Variable                 Port            Value           Type
--------                 ----            -----           ------
DATAVLAN                 3/2              3                Per-port
DATAVLAN                 3/3              5                Per-port
DATAVLAN                 NA               99               Global
AUXVLAN                  3/2              4                Per-port
AUXVLAN                  3/7              77               Per-port
CDPVER                   NA               v2               Global
Console>
```

This example shows how to display a specific macro variable and all of the ports to which it is applied:

```
Console> show macro variable name $DATAVLAN

Variable                 Port            Value           Type
--------                 ----            -----           ------
DATAVLAN                 3/2              3                Per-port
DATAVLAN                 3/3              5                Per-portGlobal
DATAVLAN                 NA               99               Global
Console>
```

This example shows how to display an individual macro variable and a specific port to which it is applied:

```
Console> show macro variable name $DATAVLAN 3/2

Variable                 Port            Value           Type
--------                 ----            -----           ------
DATAVLAN                 3/2              3                Per-port
Console>
```

This example shows how to display macro variables by entering the macro name:

```
Console> show macro variables name videophone 3/2

Variable-Name                    Variable Value          Port
-------------                    --------------          -----
DATAVLAN                         3                       3/2
AUXVLAN                          4                       3/2
Console>
```

This example shows how to display all macro port mappings:

```
Console> show macro map all

Port                    Macro
-----                   -----
3/2                       videophone
3/7                       videophone
Console>
```

This example shows how to display the macro port mappings for a specific macro:

```
Console> show macro map name videophone

Port                    Macro
-----                   -----
3/2                       videophone
3/7                       videophone
Console>
```

This example shows how to display the macro port mappings for a specific port:

```
Console> show macro map port 3/2

Port                    Macro
-----                   -----
3/2                     videophone
Console>
```

Related Commands

clear macro
set macro
set port macro
show config

show microcode

To display the version of the microcode and the module version information, use the **show microcode** command.

show microcode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the **show microcode** output for a supervisor engine:

```
Console> show microcode
Bundled Images  Version              Size    Built
--------------- -------------------- ------- -----------------
LCP SLCP        4.2(0.24)VAI58        302506 12/03/98 03:51:46
LCP LX1000      4.2(0.24)VAI58        288508 12/03/98 03:53:12
LCP LX10100     4.2(0.24)VAI58        379810 12/03/98 03:52:33
```

Table 2-50 describes possible fields in the **show microcode** command output.

Table 2-50 show microcode Command Output Fields

Field	Description
Bundled Images	Name of the bundled image.
Version	Version of the image.
Size	Size of the image.
Built	Date image was built.

8.6 EFT Copy

show mls

To display MLS Layer 3 packet information in the MLS-based Catalyst 6500 series switches, use the **show mls** command.

show mls

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you place the MSFC on a supervisor engine installed in slot 1, then the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16.

This command is not supported on switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2).

Examples

These examples show the display if you enter the **show mls** commands on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC:

```
Console> show mls
Total Active MLS entries = 0
Total packets switched = 0
IP Multilayer switching enabled
IP Multilayer switching aging time = 256 seconds
IP Multilayer switching fast aging time = 0 seconds, packet threshold = 0
IP Flow mask: Full Flow
Configured flow mask is Destination flow
Active IP MLS entries = 0
Netflow Data Export version: 8
Netflow Data Export disabled
Netflow Data Export port/host is not configured
Total packets exported = 0
MSFC ID         Module XTAG MAC               Vlans
--------------- ------ ---- ----------------- --------------------
52.0.03         15     1    01-10-29-8a-0c-00 1,10,123,434,121
                                              222,666,959
IPX Multilayer switching enabled
IPX Multilayer switching aging time = 256 seconds
IPX Flow mask: Full Flow
Active IPX MLS entries = 0
```

```
MSFC ID         Module XTAG MAC               Vlans
--------------- ------ ---- ----------------- --------------------
52.0.0.3        16     1    00-10-29-8a-0c-00 1,10

Console>
```

This example shows the display if you enter the **show mls** command on a switch with a Supervisor Engine 720 with a PFC2A:

```
Console> show mls
Total packets switched = 0
Total bytes switched = 0
Total routes = 16

Total flows in the Netflow table = 0
Total forwarding entries in the Netflow table = 0
Statistics flows normal aging time = 64 seconds
Statistics flows long-duration aging time = 8 seconds
Statistics flows fast aging time = 0 seconds, packet threshold = 0
Statistics flows session aging time = 2 seconds
Netflow Data Export version: 7
Netflow Data Export disabled
Netflow Data Export port/host is not configured.
Total packets exported = 0
Destination Ifindex export is enabled
Source Ifindex export is enabled

Module 16: Physical MAC-Address 00-b0-c2-3b-db-fd
Module 16 is the designated RP for installing CEF entries

Rate limiting is turned off, packets are bridged to router
Load balancing hash is based on source and destination IP addresses
Per-prefix Stats for ALL FIB entries is Enabled
Console>
```

Related Commands

clear mls statistics entry
set mls agingtime
set mls exclude protocol
set mls nde
set mls statistics protocol

show mls acl-route

To display summaries from ACL for routing in the MLS-based Catalyst 6500 series switches, use the **show mls acl-route** command.

show mls acl-route

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6500 series switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

If you enter any of the **show mls** commands on Catalyst 6500 series switches without IP or IPX MLS, one of these warning messages display:

```
Multilayer switching not supported on feature card.
```

or

```
IPX Multilayer switching not supported on feature card.
```

Examples

This example shows how to display summaries from ACL for routing:

```
Console> show mls acl-route
Total L3 packets forwarded      0
Total L3 octets forwarded       0
Total routed VLANs              0
Total used adjacency entries    0
Console>
```

Related Commands

show mls

show mls cef exact-route

To show the exact path that is taken from a specific IP source address to a specific IP destination address, use the **show mls cef exact-route** command.

show mls cef exact-route {*src_IP*} {*dst_IP*} [{*src_port*} {*dst_port*}]

Syntax Description

src_IP	Source IP address.
dst_IP	Destination IP address.
src_port	(Optional) Layer 4 source port number; valid values are from 0 to 65535. See the "Usage Guidelines" section for more information.
dst_port	(Optional) Layer 4 destination port number; valid values are from 0 to 65535. See the "Usage Guidelines" section for more information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If load sharing is in full mode (using a load balancing algorithm to include Layer 4 ports), you must include Layer 4 source and destination port numbers when entering this command. If load sharing is not in full mode, you do not need to include Layer 4 port numbers.

After you access the CLI on the MSFC, you can configure the load sharing mode by entering the **mls ip cef load-sharing full** command for full mode or by entering the **no mls ip cef load-sharing full** command for non-full mode. For more information about accessing the CLI on the MSFC, refer to the "Command Line Interface" chapter of the *Catalyst 6500 Series MSFC Cisco IOS Command Reference, 12.2SX*.

Examples

This example shows how to display the exact path when load sharing is not in full mode:

```
Console> show mls cef exact-route 90.0.0.1 100.0.0.1
Next Hop:52.0.0.2 Vlan:2, Destination Mac:00:00:00:00:30:01
Console>
```

This example shows how to display the exact path when load sharing is in full mode:

```
Console> show mls cef exact-route 90.0.0.1 100.0.0.1 20000 10000
Next Hop:53.0.0.2 Vlan:3, Destination Mac:00:00:00:00:40:01
Console>
```

Related Commands

show mls entry cef ip

show mls cef interface

To display MSFC VLAN information, use the **show mls cef interface** command.

show mls cef interface [*vlan*]

Syntax Description

vlan	(Optional) Number of the VLAN; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6500 series switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to display Cisco Express Forwarding (CEF) interfaces:

```
Console> (enable) show mls cef interface
Module 16: vlan 1, IP Address 21.0.0.194, Netmask 255.0.0.0
  MTU = 1500, State = up, ICMP-Unreach = enabled, ICMP-Redirect = enabled
  Unicast RPF = disabled
Module 16: vlan 43, IP Address 43.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = down, ICMP-Unreach = disabled, ICMP-Redirect = disabled
  Unicast RPF = disabled
Module 16: vlan 44, IP Address 44.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = down, ICMP-Unreach = disabled, ICMP-Redirect = disabled
  Unicast RPF = disabled
Module 16: vlan 45, IP Address 45.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = up, ICMP-Unreach = enabled, ICMP-Redirect = enabled
  Unicast RPF = disabled
Module 16: vlan 46, IP Address 46.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = up, ICMP-Unreach = enabled, ICMP-Redirect = enabled
  Unicast RPF = disabled
Module 16: vlan 47, IP Address 47.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = down, ICMP-Unreach = disabled, ICMP-Redirect = disabled
  Unicast RPF = disabled
Module 16: vlan 48, IP Address 48.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = down, ICMP-Unreach = disabled, ICMP-Redirect = disabled
  Unicast RPF = disabled
Module 16: vlan 49, IP Address 0.0.0.0, Netmask 0.0.0.0
  MTU = 1500, State = down, ICMP-Unreach = disabled, ICMP-Redirect = disabled
  Unicast RPF = disabled

Console> (enable)
```

This example show how to display information for a specific CEF VLAN:

```
Console> (enable) show mls cef interface 46
Module 16: vlan 46, IP Address 46.0.0.99, Netmask 255.0.0.0
  MTU = 1500, State = up, ICMP-Unreach = enabled, ICMP-Redirect = enabled
  Unicast RPF = disabled

Console> (enable)
```

Table 2-51 describes the possible fields in the **show mls cef interface** command output.

Table 2-51 show mls cef interface Command Output Fields

Field	Description
Vlan	VLAN associated with the interface.
IP Address	IP address associated with the interface.
Netmask	IP network mask associated with the interface.
MTU	IP MTU associated with the interface.
State	Interface state (up or down).
ICMP-Unreach	Status of whether denied Layer 3 packets will be bridged to MSFC to generate ICMP unreachable.
ICMP-Redirect	Status of whether Layer 3 packets whose destination VLAN is equal to the source VLAN should be redirected to the MSFC to generate ICMP redirect.
Unicast RPF	Unicast RPF enable/disable.

Related Commands

clear mls cef
show mls cef mac
show mls cef summary
show mls entry cef

show mls cef mac

To display bottom interface adapter (BIA) physical MACs and HSRP active virtual MACs associated with the designated MSFC2, use the **show mls cef mac** command.

show mls cef mac

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6500 series switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

If the MSFC2 has any HSRP MAC addresses configured on one or more VLANs and these interfaces are HSRP ACTIVE (for example, not standby), these will also be displayed in the command output. For example:

```
Console> show mls cef mac
Module 16:Physical MAC-Address 00-01-97-34-2b-fd
Vlan Virtual MAC-Address(es)
---- -----------------------
   1 00-00-0c-07-ac-00
  20 00-00-0c-07-ac-00
```

You will only see the virtual MAC addresses if those interfaces on the designated MSFC2 that have HSRP configured are HSRP ACTIVE and not STANDBY.

Examples

This example shows how to display the MAC address associated with the designated MSFC2:

```
Console> (enable) show mls cef mac
Module 16: Physical MAC-Address 00-01-97-36-1b-fd

Console> (enable)
```

Related Commands

clear mls cef
show mls cef interface
show mls cef summary
show mls entry cef

show mls cef maximum-routes

To display the maximum number of routes that are configured for each MLS protocol, use the **show mls cef maximum-routes** command.

show mls cef maximum-routes

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is only available on the Supervisor Engine 720.

If the maximum number of routes is not set for an MLS protocol, a system-determined default value is shown. The default value for a protocol might not be fixed, as the system tries to assign the remaining space to the unassigned protocols. If the maximum-routes configuration is changed after bootup, this command displays two kinds of information: one for the current (bootup) configuration and the other for the new configuration that takes effect after reboot.

Use the **set mls cef maximum-routes** command to set the values for the maximum number of routes. The values do not take effect until after you reboot the system.

Examples

This example shows how to display the maximum number of routes that are configured for each MLS protocol. The user-configured values do not take effect until after reboot.

```
Console> (enable) show mls cef maximum-routes
Current:
    IPv4           :192k (default)
    IPv4 multicast : 32k (default)

User configured:(effective after reboot)
    IPv4           :220k
    IPv4 multicast : 16k (adjusted default)
Console> (enable)
```

Related Commands

set mls cef maximum-routes

show mls cef rpf

To display reverse path forwarding (RPF) mode information, statistics, and VLAN table content, use the **show mls cef rpf** command.

show mls cef rpf {**mode** | **statistics** | **vlan-table**}

Syntax Description

mode	Displays the RPF mode.
statistics	Displays the number of packets and bytes that failed the hardware RPF check.
vlan-table	Displays the RPF VLAN table.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Types

Normal.

Usage Guidelines

The **show mls cef rpf vlan-table** command displays the content of the RPF VLAN table, which you configure by entering the **mls ip cef rpf interface-group** command after you access the CLI on the MSFC. For more information about accessing the CLI on the MSFC, refer to the “Command Line Interface” chapter of the *Catalyst 6500 Series MSFC Cisco IOS Command Reference, 12.2SX*.

Examples

This example shows how to display RPF mode information:

```
Console> show mls cef rpf mode
Number of active and RPF enabled VLANs:1
Packets failing hardware RPF check are dropped
RPF check mode:source reachable-via rx
RPF multipath mode:punt
Console>
```

This example shows how to display RPF statistics:

```
Console> show mls cef rpf statistics
Total packets failing hardware RPF check:                   0
Total octets  failing hardware RPF check:                   0
Console>
```

This example shows how to display RPF VLAN table content:

```
Console> show mls cef rpf vlan-table
Index         VLANs
-----   -------------------
  0        1    2    3
  1     unused
  2     unused
  3     unused
Console>
```

Related Commands

clear mls cef rpf statistics

show mls cef summary

To display a summary of CEF table information, use the **show mls cef summary** command.

show mls cef summary

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6500 series switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to display CEF information:

```
Console> show mls cef summary
Total L3 packets switched:                     0
Total L3 octets switched:                      0
Total route entries:                          10
   IP route entries:                            9
   IPX route entries:                           1
   IPM route entries:                           0
IP load sharing entries:                       0
IPX load sharing entries:                      0
Forwarding entries:                            1
Bridge entries:                                6
Drop entries:                                  3
Console>
```

Table 2-52 describes the possible fields in the **show mls cef summary** command output.

Table 2-52 show mls cef summary Command Output Fields

Field	Description
Total L3 packets forwarded	Number of Layer 3 packets forwarded by the CEF engine.
Total L3 octets forwarded	Number of Layer 3 octets forwarded by the CEF engine.
Total route entries	Number of route entries.
IP route entries	Number of IP route entries.

Table 2-52 show mls cef summary Command Output Fields (continued)

Field	Description
IPX route entries	Number of IPX route entries.
IP load sharing entries	Number of IP load-sharing entries.
IPX load sharing entries	Number of IPX load-sharing entries.
Forwarding entries	Number of forwarding entries.
Bridge entries	Number of bridge entries.
Drop entries	Number of incomplete entries (no adjacency information).

Related Commands

clear mls cef
show mls cef interface
show mls cef mac
show mls entry cef

show mls entry

To display state information in the MLS-based Catalyst 6500 series switches, use the **show mls entry** command.

show mls entry [*mod*] [**short** | **long**]

show mls entry ip [*mod*] [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*] [**short** | **long**]

show mls entry ipx [*mod*] [**destination** *ipx_addr_spec*] [**short** | **long**]

show mls entry qos [**short** | **long**]

Syntax Description

mod	(Optional) MSFC module number; valid values are **15** or **16**.
short	(Optional) Displays the output with carriage returns.
long	(Optional) Displays the output on one line.
ip	Specifies IP MLS.
destination	(Optional) Specifies the destination IP or IPX address.
ip_addr_spec	(Optional) Full IP address or a subnet address.
source	(Optional) Specifies the source IP or IPX address.
protocol	(Optional) Specifies the protocol type.
protocol	(Optional) Protocol type; valid values can be **0**, **tcp**, **udp**, **icmp**, or a decimal number for other protocol families. **0** indicates “do not care.”
src-port *src_port*	(Optional) Specifies the number of the TCP/UDP source port (decimal). Used with **dst-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates “do not care.”
dst-port *dst_port*	(Optional) Specifies the number of the TCP/UDP destination port (decimal). Used with **src-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates “do not care.”
ipx	Specifies IPX MLS.
ipx_addr_spec	(Optional) Full IPX address or a subnet address.
qos	Specifies QoS.

Defaults

The default displays MLS information in long format.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

On switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2), the display contains summaries derived from three forwarding sources: FIB for routing, the NetFlow table for statistics, and ACL TCAM for policy-based routing.

The *mod* variable and the **ip**, **ipx**, **long**, and **short** keywords are not supported on switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2).

If you use the **ip** keyword, you are specifying a command for IP MLS. If you use the **ipx** keyword, you are specifying a command for IPX MLS.

When entering the *ip_addr_spec*, use the full IP address or a subnet address in one of the following formats: *ip_addr*, *ip_addr/netmask,* or *ip_addr/maskbit*.

When entering the *ipx_addr_spec*, use the full IP address or a subnet address in one of the following formats: *src_net/*[*mask*], *dest_net.dest_node,* or *dest_net/mask*.

If you enter any **show mls** command on Catalyst 6500 series switches without IP MLS, this warning message is displayed:

```
Multilayer switching not supported on feature card.
```

If you enter any **show mls** command on Catalyst 6500 series switches without IPX MLS, this warning message is displayed:

```
IPX Multilayer switching not supported on feature card.
```

If you enter the **show mls** command with no arguments, general IP MLS information and all IP MLS-RP information is displayed.

A value 0 for *src_port* and *dst_port* means “don’t care.”

Entering the **destination** keyword specifies the entries matching the destination IP address specification, entering the **source** keyword specifies the entries matching the source IP address specification, and entering an *ip_addr_spec* can specify a full IP address or a subnet address. If you do not specify a keyword, it is treated as a wildcard, and all entries are displayed.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the short subnet address format. The trailing decimal number 00 in an IP address YY.YY.YY.00 specifies the boundary for an IP subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 173.24.00.00/255.255.0.0). However, this format can identify only a subnet address with a length of 8, 16, or 24 bits.
- *ip_addr/subnet_mask*—This is the long subnet address format. For example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip_addr* is allowed to be a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip_addr* is allowed to be a full host address, such as 172.22.254.1/22, which has the same subnet address as 172.22.252.00/72.

The [**long** | **short**] option gives the flexibility to display the output in regular (80 characters in width) or wide screen.

Dashes may be displayed for some fields if the fields are not applicable to the type of flow mask.

If you place the MSFC on a supervisor engine installed in slot 1, then the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16.

The **show mls entry** command displays bridged flows on a Supervisor Engine 1 when bridged flow statistics is enabled. The **show mls statistics entry** command displays bridged flows on a Supervisor Engine 2 when bridged flow statistics is enabled. To enable or disable bridged flow statistics, enter the **set mls bridged-flow-statistics** command.

Examples

Note The examples shown for the **show mls entry** commands are displayed in short format. The display in the long form exceeds the page width and cannot be shown.

These examples show the display if you enter the **show mls entry** commands on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC:

```
Console> (enable) show mls entry short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan ---------------
--------------- ----- ------ ------ ----------------- ----
 ESrc EDst SPort DPort Stat-Pkts Stat-Byte   Uptime   Age
 ---- ---- ----- ----- --------------------- -------- --------
171.69.200.234  171.69.192.41   TCP*  6000   59181  00-60-70-6c-fc-22 4
 ARPA SNAP 5/8    11/1  3152      347854       09:01:19 09:08:20
171.69.1.133    171.69.192.42   UDP   2049   41636  00-60-70-6c-fc-23 2
 SNAP ARPA 5/8    1/1   2345      123456       09:03:32 09:08:12

Total IP entries: 2

Destination-IPX           Source-IPX-net Destination-Mac   Vlan Port
------------------------- -------------- ----------------- ---- -----
 Stat-Pkts Stat-Bytes
 --------- -----------
BABE.0000.0000.0001       -             00-a0-c9-0a-89-1d 211  13/37 30230     1510775
201.00A0.2451.7423        -              00-a0-24-51-74-23 201  14/33
 30256     31795084
501.0000.3100.0501        -              31-00-05-01-00-00 501  9/37
 12121     323232
401.0000.0000.0401        -              00-00-04-01-00-00 401  3/1
 4633      38676

Total IPX entries: 4
Console> (enable)
```

For full flow:

```
Console> (enable) show mls entry ip short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac
Vlan --------------- --------------- ----- ------ ------
----------------- ----
EDst ESrc DPort SPort Stat-Pkts Stat-Byte   Uptime   Age
---- ---- ----- ----- --------------------- -------- --------
MSFC 127.0.0.24 (module 16):
171.69.200.234  171.69.192.41   TCP*  6000   59181  00-60-70-6c-fc-22 4
ARPA SNAP 5/8   11/1  3152 347854       09:01:19 09:08:20
171.69.1.133    171.69.192.42   UDP   2049   41636  00-60-70-6c-fc-23 2
SNAP ARPA 5/8   1/1   2345 123456       09:03:32 09:08:12

Total Entries:2
* indicates TCP flow has ended
Console> (enable)
```

For destination-only flow:

```
Console> (enable) show mls entry ip short
Destination-IP  Source-IP      Prot  DstPrt SrcPrt Destination-Mac   Vlan ---------------
--------------- ----- ------ ------ ----------------- ----
 ESrc EDst SPort DPort Stat-Pkts Stat-Byte   Uptime   Age
 ---- ---- ----- ----- --------------------- -------- --------
MSFC 127.0.0.24 (module 16):
171.69.200.234  -               -     -      -      00-60-70-6c-fc-22 4
 ARPA SNAP 5/8   11/1  3152 347854       09:01:19 09:08:20
171.69.1.133    -               -     -      -      00-60-70-6c-fc-23 2
 SNAP ARPA 5/8   1/1   2345 123456       09:03:32 09:08:12

Total Entries: 2
* indicates TCP flow has ended
Console> (enable)
```

For destination-source flow:

```
Console> (enable) show mls entry ip 16 short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan ESrc EDst
Destination-IP  Source-IP      Prot  DstPrt SrcPrt Destination-Mac   Vlan ---------------
--------------- ----- ------ ------ ----------------- ----
 ESrc EDst SPort DPort Stat-Pkts Stat-Byte   Uptime   Age
 ---- ---- ----- ----- --------------------- -------- --------
MSFC 127.0.0.24 (module 16):
171.69.200.234  171.69.192.41   -     -      -      00-60-70-6c-fc-22 4
 ARPA SNAP 5/8   11/1  3152      347854       09:01:19 09:08:20
171.69.1.133    171.69.192.42   -     -      -      00-60-70-6c-fc-23 2
 SNAP ARPA 5/8   1/1   2345      123456       09:03:32 09:08:12

Total Entries: 2
* indicates TCP flow has ended
Console> (enable)
```

For destination-source:

```
Console> (enable) show mls entry ipx short
Destination-IPX           Source-IPX-net Destination-Mac   Vlan Port
------------------------- -------------- ----------------- ---- -----
 Stat-Pkts Stat-Bytes
 --------- -----------
MSFC 127.0.0.22 (Module 15):
201.00A0.2451.7423        1.0002         00-a0-24-51-74-23 201  14/33
 30256     31795084
501.0000.3100.0501        1.0003         31-00-05-01-00-00 501  9/37
 12121     323232

Total entries: 0
Console> (enable)
```

Destination-only flow:

```
Console> (enable) show mls entry ipx short
Destination-IPX           Source-IPX-net Destination-Mac   Vlan Port
------------------------- -------------- ----------------- ---- -----
 Stat-Pkts Stat-Bytes
 --------- -----------
MSFC 127.0.0.24 (module 16):
BABE.0000.0000.0001       -              00-a0-c9-0a-89-1d 211  13/37
 30230     1510775
201.00A0.2451.7423        -              00-a0-24-51-74-23 201  14/33
 30256     31795084
501.0000.3100.0501        -              31-00-05-01-00-00 501  9/37
 12121     323232
```

```
401.0000.0000.0401        -              00-00-04-01-00-00 401  3/1
 4633      38676

Total entries: 4
Console> (enable)

Console> (enable) show mls entry ipx 16 short
Destination-IPX           Source-IPX-net Destination-Mac   Vlan Port
------------------------- -------------- ----------------- ---- -----
 Stat-Pkts Stat-Bytes
 --------- -----------
MSFC 127.0.0.22 (Module 16):
501.0000.3100.0501        -              31-00-05-01-00-00 501  9/37
 12121     323232
401.0000.0000.0401        -              00-00-04-01-00-00 401  3/1
 4633      38676
Console> (enable)
```

These examples show the display if you enter the **show mls entry** commands on a switch configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> (enable) show mls entry
Mod FIB-Type  Destination-IP  Destination-Mask NextHop-IP      Weight
--- --------- --------------- ---------------- --------------- ------
 15 receive   0.0.0.0         255.255.255.255
 15 receive   255.255.255.255 255.255.255.255
 15 receive   127.0.0.12      255.255.255.255
 16 receive   127.0.0.0       255.255.255.255
 16 receive   127.255.255.255 255.255.255.255
 15 resolved  127.0.0.11      255.255.255.255  127.0.0.11           1
 15 receive   21.2.0.4        255.255.255.255
 16 receive   21.0.0.0        255.255.255.255
 16 receive   21.255.255.255  255.255.255.255
 15 receive   44.0.0.1        255.255.255.255
 16 receive   44.0.0.0        255.255.255.255
 16 receive   44.255.255.255  255.255.255.255
 15 receive   42.0.0.1        255.255.255.255
 16 receive   42.0.0.0        255.255.255.255
 16 receive   42.255.255.255  255.255.255.255
 15 receive   43.0.0.99       255.255.255.255
 15 receive   43.0.0.0        255.255.255.255
 15 receive   43.255.255.255  255.255.255.255
 15 receive   192.20.20.20    255.255.255.255
 16 receive   21.2.0.5        255.255.255.255
 16 receive   42.0.0.20       255.255.255.255
 15 connected 43.0.0.0        255.0.0.0
 15 drop      224.0.0.0       240.0.0.0
 15 wildcard  0.0.0.0         0.0.0.0

Mod FIB-Type  Dest-IPX-net NextHop-IPX               Weight
--- --------- ------------ ------------------------- ------
 15 connected 21
 15 connected 44
 15 connected 42
 15 resolved  450          42.0050.3EA9.ABFD              1
 15 resolved  480          42.0050.3EA9.ABFD              1
 15 wildcard  0

Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan EDst Stat-Pkts  Stat-Bytes  Uptime
Age      TcpDltSeq TcpDltAck
--------------- --------------- ----- ------ ------ ----------------- ---- ---- ---------- -----------
-------- -------- --------- ---------
0.0.0.5         0.0.0.5         5     204    104    cc-cc-cc-cc-cc-cc 5    ARPA 0          0
01:03:18 01:00:51 cccccccc  cccccccc
```

```
0.0.0.2         0.0.0.2         2      201    101    cc-cc-cc-cc-cc-cc 2    ARPA 0          0
01:03:21 01:00:51 cccccccc  cccccccc
0.0.0.4         0.0.0.4         4      203    X      cc-cc-cc-cc-cc-cc 4    ARPA 0          0
01:03:19 01:00:51 cccccccc  cccccccc
0.0.0.1         0.0.0.1         ICMP   200    100    cc-cc-cc-cc-cc-cc 1    ARPA 0          0
01:03:25 01:00:52 cccccccc  cccccccc
0.0.0.3         0.0.0.3         3      202    102    cc-cc-cc-cc-cc-cc 3    ARPA 0          0
01:03:20 01:00:52 cccccccc  cccccccc
0.0.0.6         0.0.0.6         TCP    205    105    cc-cc-cc-cc-cc-cc 6    ARPA 0          0
01:03:18 01:00:52 cccccccc  cccccccc
Console> (enable)

Console> (enable) show mls entry qos
Warning: QoS is disabled.
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Stat-Pkts  Stat-Bytes  Excd-
Pkts  Stat-Bkts  Uptime   Age
--------------- --------------- ----- ------ ------ ---------- ----------- -----
----- ---------- -------- --------
MSFC 0.0.0.0 (Module 16):

Console> (enable)
```

Related Commands

clear mls statistics entry

show mls entry cef

To display CEF and adjacency entries (and Tx statistics) for IP resolved entries and IPX resolved or connected entries, use the **show mls entry cef** command.

show mls entry cef [**adjacency**]

show mls entry cef [**short** | **long**]

show mls entry cef ip [[*ip_addr/*]*mask_len*] [**adjacency** | **short** | **long**]

show mls entry cef ipx [[*ipx_addr/*]*mask_len*] [**adjacency** | **short** | **long**]

Syntax Description

adjacency	(Optional) Displays adjacency information.
short	(Optional) Displays the output with carriage returns.
long	(Optional) Displays the output on one line.
ip	Specifies IP entries.
ipx	Specifies IPX entries.
ip_addr/	(Optional) IP address of the entry.
mask_len	(Optional) Mask length associated with the IP or IPX address of the entry; valid values are from 0 to 32.
ipx_addr/	(Optional) IPX address of the entry.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6500 series switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

In the NextHop-IP field, the ouput may actually be set to “point2point” if the next hop is a point-to-point WAN interface.

When you enter the **show mls entry cef adjacency** command, only adjacency information for those IP or IPX CEF entries that are of type resolved, wildcard, or default are displayed.

Examples

This example shows how to display information for all CEF entries:

```
Console> (enable) show mls entry cef
Mod FIB-Type  Destination-IP  Destination-Mask NextHop-IP      Weight
--- --------- --------------- ---------------- --------------- ------
 16 receive   0.0.0.0         255.255.255.255
 16 receive   255.255.255.255 255.255.255.255
 16 resolved  127.0.0.21      255.255.255.255  127.0.0.21           1
 16 receive   21.0.0.194      255.255.255.255
 16 receive   45.0.0.99       255.255.255.255
 16 receive   46.0.0.99       255.255.255.255
 16 resolved  46.0.0.10       255.255.255.255  46.0.0.10            1
 16 resolved  46.0.0.9        255.255.255.255  46.0.0.9             1
 16 resolved  46.0.0.4        255.255.255.255  46.0.0.4             1
 16 resolved  46.0.0.1        255.255.255.255  46.0.0.1             1
 16 resolved  46.0.0.2        255.255.255.255  46.0.0.2             1
 16 resolved  46.0.0.3        255.255.255.255  46.0.0.3             1
 16 resolved  46.0.0.5        255.255.255.255  46.0.0.5             1
 16 resolved  46.0.0.6        255.255.255.255  46.0.0.6             1
 16 resolved  46.0.0.7        255.255.255.255  46.0.0.7             1
 16 resolved  46.0.0.8        255.255.255.255  46.0.0.8             1
 16 receive   224.0.0.0       255.255.255.0
 16 connected 21.0.0.0        255.0.0.0
 16 connected 45.0.0.0        255.0.0.0
 16 connected 46.0.0.0        255.0.0.0
 16 drop      224.0.0.0       240.0.0.0
 16 wildcard  0.0.0.0         0.0.0.0

Mod FIB-Type  Dest-IPX-net NextHop-IPX               Weight
--- --------- ------------ ------------------------- ------
 16 connected abcd
 16 connected defa
 16 resolved  fade         defa.000A.0203.0405            1
 16 wildcard  0
Console> (enable)
```

These examples show how to display information for a specific entry type:

```
Console> (enable) show mls entry cef ip
Mod FIB-Type  Destination-IP  Destination-Mask NextHop-IP      Weight
--- --------- --------------- ---------------- --------------- ------
 16 receive   0.0.0.0         255.255.255.255
 16 receive   255.255.255.255 255.255.255.255
 16 receive   127.0.0.22      255.255.255.255
 16 receive   127.0.0.0       255.255.255.255
 16 receive   127.255.255.255 255.255.255.255
 16 resolved  21.0.0.1        255.255.255.255  21.0.0.1             1
 16 receive   21.0.0.194      255.255.255.255
 16 receive   21.0.0.0        255.255.255.255
 16 receive   21.255.255.255  255.255.255.255
 16 resolved  127.0.0.21      255.255.255.255  127.0.0.21           1
 16 receive   224.0.0.0       255.255.255.0
.
.
.
Console> (enable) show mls entry cef ipx
Mod FIB-Type  Dest-IPX-net NextHop-IPX               Weight
--- --------- ------------ ------------------------- ------
 16 connected fadeface
 16 resolved  abcd         fadeface.0001.0203.0405        1
 16 wildcard  0
```

This example shows how to display adjacency information:

```
Console> (enable) show mls entry cef ip adjacency
Mod:                 16
Destination-IP:      127.0.0.21         Destination-Mask:   255.255.255.255
FIB-Type:            resolved

AdjType  NextHop-IP      NextHop-Mac       Vlan Encp Tx-Packets   Tx-Octets
-------- --------------- ----------------- ---- ---- ------------ -------------
connect  127.0.0.21      00-00-12-00-00-00    0 ARPA            0             0

Mod:                 16
Destination-IP:      46.0.0.10          Destination-Mask:   255.255.255.255
FIB-Type:            resolved

AdjType  NextHop-IP      NextHop-Mac       Vlan Encp Tx-Packets   Tx-Octets
-------- --------------- ----------------- ---- ---- ------------ -------------
connect  46.0.0.10       00-00-0c-42-00-0a   46 ARPA      4889030     224895380
Console> (enable)
```

Table 2-53 describes the possible fields in the **show mls entry cef** command output.

Table 2-53 show mls entry cef Command Output Fields

Field	Description
Mod	MSFC module number
Destination-IP Destination-IPX	Destination address (IP address or IPX network)
Destination-Mask	Destination mask
FIB-Type	FIB entry types are as follows: • receive—Prefix associated with an MSFC interface • connected—Prefix associated with a connected network • resolved—Prefix associated with a valid next-hop address • drop—Drop packets associated with this prefix • wildcard—Match-all entry (drop or MSFC redirect) • default—Default route (wildcard will point to default route)
NextHop-IP NextHop-IPX	Next-hop address (IP address or IPX network)
Weight	Next-hop load-sharing weight
AdjType	Adjacency types are as follows: • connect—Complete rewrite information • drop, null, loopbk—Drop adjacency • frc drp—Drop adjacency due to ARP throttling • punt—Redirect to MSFC for further processing • no r/w—Redirect to MSFC because rewrite is incomplete
NextHop-Mac	Next-hop destination MAC address
Vlan	Next-hop destination VLAN

Table 2-53 show mls entry cef Command Output Fields (continued)

Field	Description
Encp	Next-hop destination encapsulation type (ARPA, RAW, SAP, and SNAP)
Tx-Packets	Number of packets transmitted to this adjacency
Tx-Octets	Number of bytes transmitted to this adjacency

Related Commands

clear mls cef
clear mls entry cef
show mls cef interface
show mls cef mac
show mls cef summary

show mls entry netflow-route

To display shortcut information in the MLS-based Catalyst 6500 series switches, use the **show mls entry netflow-route** command.

show mls entry netflow-route [**short** | **long**]

show mls entry netflow-route ip [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol*] [**src-port** *src_port*] [**dst-port** *dst_port*] [**short** | **long**]

Syntax Description

short	(Optional) Displays the output with carriage returns.
long	(Optional) Displays the output on one line.
ip	Specifies IP MLS.
destination	(Optional) Specifies the destination IP or IPX address.
ip_addr_spec	(Optional) Full IP address or a subnet address.
source	(Optional) Specifies the source IP or IPX address.
protocol	(Optional) Specifies the protocol type.
protocol	(Optional) Protocol number or type; valid values can be from 0 to 255, **ip, ipinip, icmp, igmp, tcp**, or **udp**. **0** indicates "do not care."
src-port *src_port*	(Optional) Specifies the number of the TCP/UDP source port (decimal). Used with **dst-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates "do not care."
dst-port *dst_port*	(Optional) Specifies the number of the TCP/UDP destination port (decimal). Used with **src-port** to specify the port pair if the protocol is **tcp** or **udp**. **0** indicates "do not care."

Defaults

The default displays MLS information in long format.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6500 series switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

The **show mls entry netflow-route** command output displays software-installed NetFlow forwarding entries (these are used for features such as TCP intercept or reflexive ACL), but does not display flow statistics for flows that are switched through CEF entries.

If you use the **ip** keyword, you are specifying a command for IP MLS.

When entering the *ip_addr_spec*, use the full IP address or a subnet address in one of the following formats: *ip_addr*, *ip_addr/netmask,* or *ip_addr/maskbit*.

Entering the **destination** keyword specifies the entries matching the destination IP address specification, entering the **source** keyword specifies the entries matching the source IP address specification, and entering an *ip_addr_spec* can specify a full IP address or a subnet address. If you do not specify a keyword, it is treated as a wildcard, and all entries are displayed.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the short subnet address format. The trailing decimal number 00 in an IP address YY.YY.YY.00 specifies the boundary for an IP subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 173.24.00.00/255.255.0.0). However, this format can identify only a subnet address with a length of 8, 16, or 24 bits.
- *ip_addr/subnet_mask*—This is the long subnet address format. For example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip_addr* is allowed to be a full host address, such as 172.22.253.1/255.255.252.00.
- *ip_addr/maskbits*—This is the simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip_addr* is allowed to be a full host address, such as 172.22.254.1/22, which has the same subnet address as 172.22.252.00/72.

The [**long** | **short**] option gives the flexibility to display the output in regular (80 characters in width) or wide screen.

Dashes may be displayed for some fields if the fields are not applicable to the type of flow mask.

If you place the MSFC on a supervisor engine installed in slot 1, then the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16.

Examples

Note The example below is displayed in short format. The display in the long form exceeds the page width and cannot be shown.

```
Console> show mls entry netflow-route short
Destination-IP  Source-IP       Prot  DstPrt SrcPrt Destination-Mac   Vlan
--------------- --------------- ----- ------ ------ ----------------- ----
 EDst Stat-Pkts  Stat-Bytes  Uptime   Age      TcpDltSeq TcpDltAck

 ---- ---------- ----------- -------- -------- --------- ---------
0.0.0.8         0.0.0.8         8     207    107    cc-cc-cc-cc-cc-cc 8
 ARPA 0          0          00:07:07 00:21:08 cccccccc  cccccccc
0.0.0.7         0.0.0.7         7     206    106    cc-cc-cc-cc-cc-cc 7
 ARPA 0          0          00:07:09 00:21:08 cccccccc  cccccccc
0.0.0.10        0.0.0.10        10    209    109    cc-cc-cc-cc-cc-cc 10
 ARPA 0          0          00:07:06 00:21:08 cccccccc  cccccccc
0.0.0.9         0.0.0.9         9     208    108    cc-cc-cc-cc-cc-cc 9
 ARPA 0          0          00:07:07 00:21:08 cccccccc  cccccccc
0.0.0.6         0.0.0.6         TCP   205    105    cc-cc-cc-cc-cc-cc 6
 ARPA 0          0          00:07:12 00:21:08 cccccccc  cccccccc

Total entries displayed:5
Console>
```

show mls exclude protocol

To display excluded protocols on TCP or UDP from being shortcuts, use the **show mls exclude protocol** command.

show mls exclude protocol

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you enter the **show mls exclude protocol** command on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC, MLS exclusion only works in full-flow mode.

These guidelines apply to switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

- The **show mls exclude protocol** displays the Layer 4 protocols that will not cause a NetFlow entry to be created automatically but can still be forwarded if a FIB hit occurs.
- MLS exclusion works regardless of the configured flow mask.

Examples

This example shows how to display excluded protocols on TCP or UDP from being shortcuts:

```
Console> (enable) show mls exclude protocol
Protocol-Port Excluded-From
------------- -------------
89            TCP UDP
5             TCP
10            TCP UDP
122           UDP
Note: MLS exclusion only works in full flow mode.
Console> (enable)
```

Related Commands

clear mls multicast statistics
set mls exclude protocol

show mls flowmask

To display the MLS flow mask configuration, use the **set mls flowmask** command.

show mls flowmask

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

In software release 8.5(1), multiple flow masks are supported.

Examples

These examples show output with various configurations when no features are configured on the route processor:

```
Console> show mls flowmask
Netflow Data Export is enabled
NDE Flowmask is configured to use atleast Null flowmask
Console>

Console> show mls flowmask
Netflow Data Export is enabled and is using Full flowmask
NDE Flowmask is configured to use atleast Full flowmask
Console>

Console> show mls flowmask
Netflow Data Export is disabled
NDE Flowmask is configured to use atleast Full flowmask
Console>
```

This example shows output when NAT is configured on the RP:

```
Console> show mls flowmask
The MSFC features are using NotVlanFullFlow and VlanFullFlowOnly flow mask on vlan(s)
10-11,50-51,90-91.
Netflow Data Export is disabled
NDE Flowmask is configured to atleast the Null flowmask
Console>
```

These examples show output with various configurations when the Reflexive ACL feature is configured on the RP:

```
Console> show mls flowmask
The MSFC features are using VlanFullFlowOnly flow mask on vlan(s) 13.
Netflow Data Export is disabled
NDE Flowmask is configured to use atleast Null flowmask
Console>

Console> show mls flowmask
The MSFC features are using VlanFullFlowOnly flow mask on vlan(s) 13.
Netflow Data Export is enabled and is using Full-Vlan flowmask
NDE Flowmask is configured to use atleast Full-Vlan flowmask
Console>
```

Related Commands

set mls flow
set mls nde

show mls multicast

To display IP multicast MLS information, use the **show mls multicast** command.

show mls multicast

show mls multicast entry {[*mod*] [**vlan** *vlan_id*] [**group** *ip_addr*]} [**source** *ip_addr*] [**long** | **short**]

show mls multicast entry {[**all**] [**short** | **long**]}

show mls multicast statistics {*mod*}

Syntax Description

entry	Specifies the IP multicast MLS packet entry.
mod	(Optional) Number of the MSFC; valid values are **15** and **16**.
vlan *vlan_id*	(Optional) Specifies a VLAN.
group *ip_addr*	(Optional) Specifies a multicast group address.
source *ip_addr*	(Optional) Specifies a multicast traffic source.
all	(Optional) Specifies all IP multicast MLS entries on the switch.
long	(Optional) Specifies an output appropriate for terminals that support output 80-characters wide.
short	(Optional) Specifies an output appropriate for terminals that support output less than 80-characters wide.
statistics	Displays statistics for an MSFC.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you enter the **show mls multicast** commands on Catalyst 6500 series switches without MLS, this warning message is displayed:

```
This feature is not supported on this device.
```

If you enter the **show mls multicast entry** command with no arguments, all the MLS entries for multicast are displayed. Each row in the **show mls multicast entry** command corresponds to a flow.

These guidelines apply to switches configured with the Supervisor 2 with Layer 3 Switching Engine II (PFC2):

- If you enter the **show mls multicast entry** command and an asterisk appears in the Source IP column, this indicates that any source is used.
- If you specify source 0, all * (asterisk) entries are displayed.

If you disable DNS, no name can be specified or shown.

A warning message is displayed if you disable the Layer 2 multicast protocol when the multicast multilayer switching (MMLS) feature is running.

If you place the MSFC on a supervisor engine installed in slot 1, then the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16.

Examples

This example shows how to display global information about the IP MMLS entries on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine (WS-F6K-PFC):

```
Console> (enable) show mls multicast
Admin Status: Enabled
Operational Status: Inactive
Configured flow mask is {Source-Destination-Vlan} flow
Active Entries = 0
MSFC (Module 15): 0.0.0.0
Console> (enable)
```

This example shows how to display global information about the IP MMLS entries on a switch configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> (enable) show mls multicast
Admin Status       : Enabled
 Operational Status : Active
 Total Entries      : 104
 MSFC (Module 15)   :
     IP Address     : 1.1.1.1
     Complete Flows : 30
     Partial Flows  : 10
 MSFC (Module 16)   :
     IP Address     : 2.2.2.2
     Complete Flows : 50
     Partial Flows  : 14
Console> (enable)
```

Table 2-54 describes the fields in the **show mls multicast** command output.

Table 2-54 show mls multicast Command Output Fields

Field	Description
Admin Status	Status of whether MMLS feature has been administratively enabled or not.
Operational Status	Actual operational status of the MMLS feature.
Total Entries	Number of shortcut entries that are currently installed.
MSFC	Information about the internal RP connected to the supervisor engine.
IP Address	IP address of the RP.
Complete Flows	Total number of complete flows installed by this RP.
Partial Flows	Total number of partial flows installed by this RP.

This example shows how to display statistical information on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine (WS-F6K-PFC):

```
Console> (enable) show mls multicast statistics
Router IP          Router Name        Router MAC
---------------    ------------------ -----------------
0.0.0.0            default            00-00-00-00-00-00
Transmit:
                     Feature Notifications: 0
            Feature Notification Responses: 0
           Shortcut Notification Responses: 0
                      Delete Notifications: 0
                          Acknowledgements: 0
                           Flow Statistics: 0
                   Total Transmit Failures: 0

Receive:
                     Feature Notifications: 0
                         Shortcut Messages: 0
               Duplicate Shortcut Messages: 0
                      Shortcut Install TLV: 0
                      Selective Delete TLV: 0
                          Group Delete TLV: 0
                                Update TLV: 0
                     Input VLAN Delete TLV: 0
                    Output VLAN Delete TLV: 0
                         Global Delete TLV: 0
                           MFD Install TLV: 0
                            MFD Delete TLV: 0
                     Global MFD Delete TLV: 0
                               Invalid TLV: 0
Console> (enable)
```

This example shows how to display statistical information on a switch configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> (enable) show mls multicast statistics
Router IP          Router Name        Router MAC
---------------    ------------------ -----------------
0.0.0.0            default            00-00-00-00-00-00
Transmit:
                     Feature Notifications: 0
            Feature Notification Responses: 0
           Shortcut Notification Responses: 0
                      Delete Notifications: 0
                          Acknowledgements: 0
                           Flow Statistics: 0
                   Total Transmit Failures: 0
Receive:
                     Feature Notifications: 0
                         Shortcut Messages: 0
               Duplicate Shortcut Messages: 0
                      Shortcut Install TLV: 0
                      Selective Delete TLV: 0
                          Group Delete TLV: 0
                                Update TLV: 0
                     Input VLAN Delete TLV: 0
                    Output VLAN Delete TLV: 0
                         Global Delete TLV: 0
                           MFD Install TLV: 0
                            MFD Delete TLV: 0
                     Global MFD Delete TLV: 0
                               Invalid TLV: 0
Console> (enable)
```

This example shows how to display IP MMLS entry information on a switch configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC:

```
Console> (enable) show mls multicast entry
Router IP       Dest IP         Source IP       Pkts       Bytes       InVlan  OutVlans
--------------- --------------- --------------- ---------- ----------- ------- --------
1.1.5.252       224.1.1.1       1.1.11.1        15870      2761380     20
1.1.9.254       224.1.1.1       1.1.12.3        473220     82340280    12
1.1.5.252       224.1.1.1       1.1.12.3        15759      2742066     20
1.1.9.254       224.1.1.1       1.1.11.1        473670     82418580    11
1.1.5.252       224.1.1.1       1.1.11.3        15810      2750940     20
1.1.9.254       224.1.1.1       1.1.12.1        473220     82340280    12
1.1.5.252       224.1.1.1       1.1.13.1        15840      2756160     20
Total Entries: 7
Console> (enable)
```

Note The display for the **show mls multicast entry** command has been modified to fit the page.

This example shows how to display IP MMLS entry information on a switch configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> (enable) show mls multicast entry
 Router-IP       Dest-IP         Source-IP       Pkts                 Bytes                InVlan Type
OutVlans
 --------------- --------------- --------------- -------------------- -------------------- ------ ----
----------
 33.0.33.26      224.2.2.3       10.0.0.1        595                  59500                50      C    13,
12
 33.0.33.26      224.2.2.3       *               2                    200                  50      P    13,
12

 Total Entries: 2 (1 of which type 'C' = Complete Flow/s, 'P' = Partial Flow/s)
Console> (enable)
```

Table 2-55 describes the fields in the **show mls multicast entry** command output.

Table 2-55 show mls multicast entry Command Output Fields

Field	Description
Router-IP	IP address of the RP that installed the flow.
Dest-IP	Multicast destination IP address for this flow.
Source-IP	IP address of the source that corresponds to this flow.
Pkts	Number of packets switched using this flow.
Bytes	Number of bytes switched using this flow.
InVlan	RPF interface for the packets corresponding to this flow.
Type	Shortcut Type (C = a complete shortcut and P = a partial shortcut).
OutVlans	Output VLANs on which the packets are replicated for this flow.
Total Entries	Number of shortcut entries currently installed.

Related Commands

clear mls multicast statistics

show mls nde

To display NetFlow Data Export information, use the **show mls nde** command.

show mls nde

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display NetFlow Data Export information:

```
Console> show mls nde
Netflow Data Export version: 5
Netflow Data Export disabled
Netflow Data Export configured for port 9000 on host 10.6.1.10
Secondary Data Export configured for port 9111 on host 10.6.1.10
Total packets exported = 30872
Total Secondary packets exported = 1412
Destination Ifindex export is enabled
Source Ifindex export is enabled
Bridged flow statistics is disabled on vlan(s) 1,11-12,46.
Console>
```

Related Commands

clear mls nde
set mls bridged-flow-statistics
set mls nde

show mls netflow-route

To display summaries from NetFlow for routing in the MLS-based Catalyst 6500 series switches, use the **show mls netflow-route** command.

show mls netflow-route [**ip** | **ipx**]

Syntax Description

ip	(Optional) Specifies IP MLS.
ipx	(Optional) Specifies IPX MLS.

Defaults

The default displays both IP and IPX MLS information.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is supported on Catalyst 6500 series switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Examples

This example shows how to display summaries from NetFlow for routing:

```
Console> show mls netflow-route
Total packets switched = 0
Total bytes switched = 0

Software installed aging time = 0
IP flows aging time = 256 seconds
IP flows fast aging time = 0 seconds, packet threshold = 0
IP Current flow mask is Full flow
Total netflow forwarding entries = 4
Netflow Data Export version:7
Netflow Data Export disabled
Netflow Data Export port/host is not configured.
Total packets exported = 0


IPX flows aging time = 256 seconds
IPX flow mask is Destination flow
IPX max hop is 15
Console>
```

show mls pbr-route

To display statistics about policy-based routing (PBR) traffic, use the **show mls pbr-route** command.

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal mode.

Usage Guidelines

Because PBR occurs in the hardware, PBR-related statistics on the MSFC do not reflect the volume of traffic being policy routed.

Examples

This example shows how to display PBR traffic statistics:

```
Console> show mls pbr-route
Total L3 packets forwarded      9789802
Total L3 octets forwarded       541243304
Total routed VLANs              1
Total adjacency entries         1
Console>
```

Table 2-56 describes the possible fields in the **show mls pbr-route** command output.

Table 2-56 show mls pbr-route Command Output Fields

Field	Description
Total L3 packets forwarded	Number of Layer 3 packets forwarded in hardware.
Total L3 octets forwarded	Number of Layer 3 octets forwarded in hardware.
Total routed VLANs	Number of VLANs with PBR configured.
Total adjacency entries	Number of policy-routing adjacencies programmed.

show mls statistics

To display MLS statistics information in the MLS-based Catalyst 6500 series switches, use the **show mls statistics** command.

show mls statistics protocol

show mls statistics entry [*mod*]

show mls statistics entry ip [*mod*] [**destination** *ip_addr_spec*] [**source** *ip_addr_spec*] [**protocol** *protocol* [**src-port** *src_port*] [**dst-port** *dst_port*]]

show mls statistics entry ip top-talkers [*num_of_top_talkers*]

show mls statistics entry ipx [*mod*] [**destination** *ipx_addr_spec*] [**source** *ipx_addr_spec*]

show mls statistics entry uptime

Syntax Description

protocol	Specifies a route processor.
entry	Specifies the entry type.
mod	(Optional) Number of the MSFC; valid values are **15** or **16**.
entry	Displays statistics based on the specified option.
ip	Specifies IP MLS.
destination	(Optional) Specifies the destination IP address.
ip_addr_spec	(Optional) Full IP address or a subnet address in the following formats: ip_addr, ip_addr/netmask, or ip_addr/maskbit.
source	(Optional) Specifies the source IP address.
protocol *protocol*	(Optional) Specifies additional flow information (protocol family and protocol port pair) to be matched; valid values are from 1 to 255, **ip**, **ipinip**, **icmp**, **igmp**, **tcp**, and **udp**.
src-port *src_port*	(Optional) Specifies the source port IP address.
dst-port *dst_port*	(Optional) Specifies the destination port IP address.
top-talkers	Displays the NetFlows with the maximum network usage.
num_of_top_talkers	(Optional) Number of NetFlows to be displayed; valid values are from 1 to 32.
ipx	Specifies IPX MLS.
ipx_addr_spec	(Optional) Full IPX address or a subnet address in one of the following formats: *src_net/*[*mask*], *dest_net.dest_node,* or *dest_net/mask*.
uptime	Displays up time and aging time.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If your system is configured with the Supervisor Engine 2 with Switching Engine II (PFC2), the **show mls statistics entry** command output displays per flow statistics as per the configured flow mask. You can enter this command to display per-flow statistics for flows that are CEF switched (in hardware) or switched through software-installed shortcuts in the NetFlow table.

You can enter the **show mls statistics entry** command to display NetFlow forwarding entries on systems configured with a Supervisor Engine 2. If your system is configured with a Supervisor Engine 1, enter the **show mls entry** command.

When specifying the **ip** | **ipx** keyword, if you specify **ip** or do not enter a keyword, this means that the command is for IP MLS. If you specify **ipx**, this means the command is for IPX only.

When entering the IPX address syntax, use the following format:

- IPX net address—1...FFFFFFFE
- IPX node address—x.x.x where x is 0...FFFF
- IPX address—ipx_net.ipx_node (for example 3.0034.1245.AB45, A43.0000.0000.0001)

If you enter any of the **show mls statistics protocol** commands on a Catalyst 6500 series switch without MLS, this warning message is displayed:

```
Feature not supported in hardware.
```

If you enter the **show mls statistics protocol** command, the statistics in the protocol category, such as Telnet, FTP, or WWW are displayed. Note that this applies for "full flowmask" only. In flowmasks other than full flow, inapplicable fields will have a dash (similar to **show mls entry** outputs).

A value 0 for *src_port* and *dst_port* means "don't care." Note that this applies for "full flowmask" only.

Use the following syntax to specify an IP subnet address:

- *ip_subnet_addr*—This is the short subnet address format. The trailing decimal number "00" in an IP address YY.YY.YY.YY specifies the boundary for an IP subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 255.255.0.0). However, this format can identify only a subnet address with a length of 8, 16, or 24 bits.
- *ip_addr/subnet_mask*—This is the long subnet address format; for example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip_addr* is allowed to be a full host address, such as 172.22.253.1/255.255.252.00, which has the same subnet address as *ip_subnet_addr*.
- *ip_addr/maskbits*—This is the simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip_addr* is allowed to be a full host address, such as 172.22.254.1/22, which has the same subnet address as 172.22.252.00/72.

If you place the MSFC on a supervisor engine installed in slot 1, then the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16.

The **show mls statistics entry** command displays bridged flows on a Supervisor Engine 2 when bridged flow statistics is enabled. The **show mls entry** command displays bridged flows on a Supervisor Engine 1 when bridged flow statistics is enabled. To enable or disable bridged flow statistics, enter the **set mls bridged-flow-statistics** command.

Enter the **show mls statistics entry ip top-talkers** command to identify the NetFlows with the maximum network usage (called “top talkers”). The command output displays the IP addresses of these NetFlows and the number of packets in each NetFlow. If you do not enter a *num_of_top_talkers* argument, up to 32 “top talkers” are displayed.

Note The **show mls statistics entry ip top-talkers** command is available on the PFC2 and the PFC3 for IPv4 traffic.

Examples

This example shows how to display the statistics for all protocol categories:

```
Console> (enable) show mls statistics protocol
Protocol  TotalFlows  TotalPackets    Total Bytes
-------   ----------  --------------  ------------
Telnet    900         630             4298
FTP       688         2190            3105
WWW       389         42679           623686
SMTP      802         4966            92873
X         142         2487            36870
DNS       1580        52              1046
Others    82          1               73
Total     6583        53005           801951
Console> (enable)
```

This example shows how to display the up time and aging time on a Supervisor Engine 2:

```
Console> show mls statistics entry uptime
                                  Last    Used
Destination IP   Source IP       Prot  DstPrt SrcPrt Uptime   Age
---------------- --------------- ----- ------ ------ -------- --------
 172.20.52.19    -               -     -      -      00:07:51 00:00:00
 224.0.0.10      -               -     -      -      00:06:44 00:00:02
 224.0.0.10      -               -     -      -      00:06:49 00:00:01
 255.255.255.255 -               -     -      -      00:02:53 00:00:37
 224.0.0.10      -               -     -      -      00:06:50 00:00:00
 171.69.39.44    -               -     -      -      00:07:51 00:00:00
 224.0.0.2       -               -     -      -      00:06:42 00:00:01
 224.0.0.10      -               -     -      -      00:06:35 00:00:03
 224.0.0.5       -               -     -      -      00:06:33 00:00:03

Destination IPX            Source IPX net Uptime   Age
-------------------------- -------------- -------- --------
Console>
```

This example shows how to display the MLS statistical entries on a Supervisor Engine 2:

```
Console> show mls statistics entry
                                       Last    Used
     Destination IP   Source IP       Prot  DstPrt SrcPrt Stat-Pkts  Stat-Bytes
     ---------------- --------------- ----- ------ ------ ---------- ---------------
      10.0.0.6        10.0.0.1        255   0      0      569735     26207810
      10.0.0.5        10.0.0.1        255   0      0      569735     26207810
      10.0.0.2        10.0.0.1        255   0      0      569735     26207810
     Destination IPX            Source IPX net Stat-Pkts  Stat-Bytes
     -------------------------- -------------- ---------- ----------
Console>
```

Note The following commands are output from switches configured with the Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC. The output from switches configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) are slightly different.

This example shows how to display IP MLS statistics for MSFC 15 in a system configured with the Supervisor Engine 1 with Layer 3 Switching Engine (WS-F6K-PFC):

```
Console> show mls statistics entry ip 15 destination 172.20.22.14
MSFC 127.0.0.12 (Module 15):
                                  Last    Used
Destination IP  Source IP       Prot DstPrt SrcPrt Stat-Pkts Stat-Bytes
--------------- --------------- ---- ------ ------ --------- ---------------
172.20.22.14    172.20.25.10    6    50648  80     3152      347854
Console>
```

This example shows how to display the statistics for a specific destination IP address:

```
Console> show mls statistics entry ip destination 172.20.22.14
                Last Used         Last    Used
Destination IP  Source IP       Prot DstPrt SrcPrt Stat-Pkts  Stat-Bytes
--------------- --------------- ---- ------ ------ ---------- ---------------
172.20.22.14    172.20.25.10    6    50648  80     3152       347854
Console>
```

This example shows how to display the statistics for a specific destination IPX address:

```
Console> show mls statistics entry ipx destination 1.0002.00e0.fefc.6000
Destination IPX           Source IPX net Stat-Pkts  Stat-Bytes
------------------------- -------------- ---------- ----------
MLS-RP 10.20.26.64:
1.0002.00e0.fefc.6000     1.0003         11         521
Console>
```

This example shows how to display the statistics for NetFlows with maximum network usage:

```
Console> show mls statistics entry ip top-talkers

Last    Used
Destination IP   Source IP       Prot  DstPrt SrcPrt Vlan  Stat-Pkts  Stat-Bytes
---------------- ---------------- ----- ------ ------ ----- ---------  -----------
 12.0.0.5        11.0.0.6        255   N/A    N/A    N/A   387110     17807060
 12.0.0.5        11.0.0.7        255   N/A    N/A    N/A   387109     17807014
 12.0.0.5        11.0.0.4        TCP   8      7      N/A   20         920
 127.0.0.20      127.0.0.19      UDP   67     68     N/A   18         828
 12.0.0.5        11.0.0.2        TCP   6      5      N/A   15         690
 12.0.0.5        11.0.0.5        TCP   8      7      N/A   15         690
 12.0.0.5        11.0.0.3        TCP   6      5      N/A   12         552
Console>
```

This example shows how to display the statistics for a specified number of NetFlows with maximum network usage:

```
Console> show mls statistics entry ip top-talkers 2
Last    Used
Destination IP   Source IP       Prot  DstPrt SrcPrt Vlan  Stat-Pkts  Stat-Bytes
---------------- ---------------- ----- ------ ------ ----- ---------  -----------
 12.0.0.5        11.0.0.6        255   N/A    N/A    N/A   387110     17807060
 12.0.0.5        11.0.0.7        255   N/A    N/A    N/A   387109     17807014
Console>
```

Related Commands

clear mls statistics entry
set mls bridged-flow-statistics
set mls statistics protocol
show mls entry

show mls verify

To display the Layer 3 error checking configuration, use the **show mls verify** command.

show mls verify

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the Layer 3 error checking configuration:

```
Console> show mls verify
 IP checksum verification disabled
 IP minimum length verification enabled
 IP inconsistant length verification disabled
 IPX minimum length verification enabled
 IPX inconsistant length verification disabled
Console>
```

Table 2-57 describes the fields in the **show mls verify** command output.

Table 2-57 show mls verify Command Output Fields

Field	Description
IP checksum verification	Status of whether IP checksum verification is enabled or disabled.
IP minimum length verification	Status of whether the verification of IP minimum packet length is enabled or disabled.
IP inconsistent length verification	Status of whether the verification of IP length consistency is enabled or disabled.
IPX minimum length verification	Status of whether the verification of IPX minimum packet length is enabled or disabled.
IPX consistent length verification	Status of whether the verification of IPX length consistency is enabled or disabled.

Related Commands

set mls verify

show module

To display module status and information, use the **show module** command. For supervisor engines, the **show module** command displays the supervisor engine number but appends the uplink daughter card module type and information.

show module [*mod*]

Syntax Description

mod	(Optional) Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a module number, all modules are shown.

The MAC addresses for the supervisor engine are displayed in three lines of output. The first line lists the two MAC addresses for inband ports, the second line lists the two MAC addresses for the two gigabit-uplink ports, and the third line lists the allocated 0x3ff MAC address for the chassis backplane.

If you place the MSFC on a supervisor engine installed in slot 1, then the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16.

The slot field in the **show module** command display is required because submodules, such as the MSM, reside in the same slot as the supervisor engine module, but are treated as a separate module.

The MSM is referenced by the module number in all other CLI commands and is treated like any other module.

The **show module** command does not display information about the 720 Gbps integrated switch fabric because it is not a separate module.

Examples

This example shows how to display status and information for all modules:

```
Console> show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
8   8    48    10/100BaseTX Ethernet     WS-X6248-RJ-45      no  ok
9   9    48    10/100BaseTX Ethernet     WS-X6348-RJ-45      yes ok

Mod Module-Name         Serial-Num
--- ------------------- -----------
1                       SAD03436055
15                      SAD03432597
9                       SAD03414268
```

```
Mod MAC-Address(es)                        Hw     Fw         Sw
--- -------------------------------------- ------ ---------- --------------
1   00-30-80-f7-a5-06 to 00-30-80-f7-a5-07 1.0    5.2(1)     6.1(0.12)
    00-30-80-f7-a5-04 to 00-30-80-f7-a5-05
    00-30-a3-4a-a0-00 to 00-30-a3-4a-a3-ff
15  00-d0-bc-ee-d0-dc to 00-d0-bc-ee-d1-1b 1.2    12.0(3)XE1 12.0(3)XE1
8   00-d0-c0-c8-83-ac to 00-d0-c0-c8-83-db 1.1    4.2(0.24)V 6.1(0.37)FTL
9   00-50-3e-7c-43-00 to 00-50-3e-7c-43-2f 0.201  5.3(1)

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw
--- ----------------------- ------------------- ----------- ------
1   L3 Switching Engine     WS-F6K-PFC          SAD03451187 1.0
9   Inline Power Module     WS-F6K-VPWR                     1.0
Console>
```

This example shows the display for a 48-port 10/100BASE-TX switching services-configured module:

```
Console> show module 5
Mod Slot Ports Module-Type               Model               Status
--- ---- ----- ------------------------- ------------------- --------
5   5    48    10/100BaseTX (RJ-45)      WS-X6248-RJ-45      ok

Mod Module-Name         Serial-Num
--- ------------------- -----------
5                       SAD03181291

Mod MAC-Address(es)                        Hw     Fw         Sw
--- -------------------------------------- ------ ---------- -----------------
5   00-50-f0-ac-30-54 to 00-50-f0-ac-30-83 1.0    4.2(0.24)V 6.1(0.12)
Console>
```

This example shows the display for an 8-port T1/E1 ISDN PRI services-configured module:

```
Console> (enable) show module 3
Mod Slot Ports Module-Type               Model               Status
--- ---- ----- ------------------------- ------------------- --------
3   3    8     T1 PSTN                   WS-X6608-T1         ok

Mod Module-Name         Serial-Num
--- ------------------- -----------
3   T1                  SAD02440056

Mod MAC-Address(es)                        Hw     Fw         Sw
--- -------------------------------------- ------ ---------- -----------------
3   00-50-0f-08-bc-a0 to 00-50-0f-08-bc-cf 0.1    5.1(1)     5.4(1)
Console>
```

This example shows the display for a 24-port FXS analog station interface services-configured module:

```
Console> show module 3
Mod Slot Ports Module-Type               Model               Status
--- ---- ----- ------------------------- ------------------- --------
3   3    24    FXS                       WS-X6624-FXS        ok

Mod Module-Name         Serial-Num
--- ------------------- -----------
3   Elvis-S             SAD02440056

Mod MAC-Address(es)                        Hw     Fw         Sw
--- -------------------------------------- ------ ---------- -----------------
3   00-50-0f-08-bc-a0 to 00-50-0f-08-bc-a0 0.1    5.1(1)     5.4(1)
Console>
```

This example shows the display for a supervisor engine 720:

```
Console> show module 6
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
6   6    0     Sup 3 CPU Board Ariel     --SUP3-ARIEL--      no  ok

Mod Module-Name          Serial-Num
--- -------------------- -----------
6                        SAD04510ATR

Mod MAC-Address(es)                        Hw     Fw         Sw
--- -------------------------------------- ------ ---------- -----------------
6   00-40-0b-ff-00-00                      0.202  6.1(3)     7.5(0.2)CLR
```

Table 2-58 describes the possible fields in the **show module** command output.

Table 2-58 show module Command Output Fields

Field	Description
Mod	Module number.
Slot	Number of the slot where the module or submodule resides.
Ports	Number of ports on the module.
Module-Type	Module (such as 100BASE-X Ethernet).
Model	Model number of the module.
Sub	Status of whether a submodule is installed.
Status	Status of the module. Possible status strings are ok, disable, faulty, other, standby, error, pwr-down, and pwr-deny states[1].
Module-Name	Name of the module.
Serial-Num	Serial number of the module.
MAC-Address(es)	MAC address or MAC address range for the module.
Hw[2]	Hardware version of the module.
Fw[3]	Firmware version of the module.
Sw	Software version on the module.
Sub-Type[4]	Submodule type.
Sub-Model[4]	Model number of the submodule.
Sub-Serial[4]	Serial number of the submodule.
Sub-Hw[4]	Hardware version of the submodule.

[1] The pwr-down and pwr-deny states are supported by the power management feature.

[2] Hw for the supervisor engine displays the supervisor engine’s EARL hardware version.

[3] Fw for the supervisor engine displays the supervisor engine’s boot version.

[4] This field displays EARL information.

show moduleinit

To display contents of the information stored in the system module initiation log, use the **show moduleinit** command.

show moduleinit [*mod*] [**log** *lognum* | *-logcount*]

Syntax Description

mod	(Optional) Number of the module.
log	(Optional) Specifies a specific log.
lognum	(Optional) Number of the log to display.
-logcount	(Optional) Number of previous logs to display.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a module number, contents for all modules are shown.

Examples

This example shows how to show the last two log entries for module 1:

```
Console> show moduleinit 1 log -2
Module 1:   Number of Logs: 3
Log #2:
State 1: Entry/Exit/Elapse Time: 14721/14721/0
  Success_Exit
State 2: Entry/Exit/Elapse Time: 14721/14721/0
  Success
State 3: Entry/Exit/Elapse Time: 14721/32223/17502
  Success_Exit

Log #3:
State 1: Entry/Exit/Elapse Time: 38302/38302/0
  P_PortConfigTokenRingFeatures()
  ConfigModule()
State 2: Entry/Exit/Elapse Time: 38302/38302/0
  Success
State 3: Entry/Exit/Elapse Time: 38302/38310/8
  Success_Exit
Console>
```

This example shows how to display the contents of a specific log for module 1:

```
Console> show moduleinit 1 log 2
Module 1:   Number of Logs: 3
Log #2:
State 1: Entry/Exit/Elapse Time: 14721/14721/0
  Success_Exit
State 2: Entry/Exit/Elapse Time: 14721/14721/0
  Success
State 3: Entry/Exit/Elapse Time: 14721/32223/17502

Console>
```

Table 2-59 describes the possible fields in the **show moduleinit** command output.

Table 2-59 show moduleinit Command Output Fields

Field	Description
Log #	Number of the log.
State #	Number of the module initiation states. Output includes the entry time into and exit time from all the module initiation states, along with the elapsed time, in milliseconds.

show msfcautostate

To display the Multilayer Switch Feature Card (MSFC) auto port state, use the **show msfcautostate** command.

show msfcautostate

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the MSFC auto state status:

```
Console> (enable) show msfcautostate
MSFC Auto port state: enabled
Console> (enable)
```

Related Commands

clear msfcautostate
set msfcautostate

show msmautostate

To display the current status of the line protocol state determination of the MSMs due to Catalyst 6500 series switch port state changes, use the **show msmautostate** command.

show msmautostate *mod*

Syntax Description

mod	Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the current status of MSM line protocol state determination:

```
Console> show msmautostate
MSM Auto port state: enabled
Console>
```

Related Commands

set msmautostate

show multicast group

To display the multicast group configuration, use the **show multicast group** command.

show multicast group [*mac_addr*] [*vlan_id*]

Syntax Description

mac_addr	(Optional) Destination MAC address.
vlan_id	(Optional) Number of the VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the multicast group configuration for VLAN 1:

```
Console> show multicast group 1
VLAN  Dest MAC/Route Des    [CoS]   Destination Ports or VCs / [Protocol Type]
---- ----------------- ----- ---------------------------------
1    01-00-5e-00-01-28*      3/1,12/9
1    01-00-5e-63-7f-6f*      3/1,12/5,12/9
Total Number of Entries = 2
Console>
```

This example shows how to display the multicast group configuration for a specific MAC address on VLAN 5:

```
Console> show multicast group 01-00-5E-00-00-5C 5
VLAN  Dest MAC/Route Des    [CoS]   Destination Ports or VCs / [Protocol Type]
---- ----------------- ----- ---------------------------------
5    01-00-5E-00-00-5C       3/1, 3/9
Total Number of Entries = 1
Console>
```

Table 2-60 describes the fields in the **show multicast group** command output.

Table 2-60 show multicast group Command Output Fields

Field	Description
IGMP enabled/disabled	Status of whether IGMP is enabled or disabled.
GMRP enabled/disabled	Status of whether GMRP is enabled or disabled.
VLAN	VLAN number.
Dest MAC/Route Des	Group destination MAC address.
*	Status of whether the port was configured manually as a multicast router port.

Table 2-60 show multicast group Command Output Fields (continued)

Field	Description
CoS	CoS value.
Destination Ports or VCs	List of all the ports that belong to this multicast group. Traffic destined to this group address will be forwarded on all these ports.
Protocol Type	Type of protocol.
Total Number of Entries	Total number of entries in the multicast group table that match the criteria specified by the command.

Related Commands

clear multicast router
set multicast router
show multicast router

show multicast group count

To show the total count of multicast addresses (groups) in a VLAN, use the **show multicast group count** command.

show multicast group count [*vlan_id*]

Syntax Description

vlan_id	(Optional) Number of the VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

An asterisk in the **show multicast group count** command output indicates the port was configured manually.

Examples

This example shows how to display the total count of multicast groups in VLAN 5:

```
Console> show multicast group count 5

Total Number of Entries = 2
Console>
```

Related Commands

clear multicast router
set multicast router
show multicast router

8.6 EFT Copy

show multicast protocols status

To display the status of Layer 2 multicast protocols on the switch, use the **show multicast protocols status** command.

show multicast protocols status

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the Layer 2 multicast protocol status:

```
Console> show multicast protocols status
IGMP disabled
IGMP fastleave enabled
IGMP V3 processing disabled
IGMP V3 fastblock feature disabled
RGMP enabled
GMRP disabled
Console>
```

Related Commands

set gmrp
set igmp
set igmp fastleave
set igmp v3-processing
set rgmp

show multicast ratelimit-info

To display information about multicast rate limiting, use the **show multicast ratelimit-info** command.

show multicast ratelimit-info

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display information about multicast rate limiting:

```
Console> show multicast ratelimit-info
Multicast ratelimiting enabled
Ratelimit threshold rate:1000 pps
VLAN  RateLimited-Since         Ratelimited-for(seconds)
----  ------------------        ----------------------
  61  Fri Mar 19 2004, 06:32:45  30
Console>
```

Related Commands

set multicast ratelimit

show multicast router

To display the ports that have IGMP or RGMP-capable routers assigned to them, use the **show multicast router** command.

show multicast router {**igmp** | **rgmp**} [*mod/port*] [*vlan_id*]

Syntax Description

igmp	Specifies IGMP-capable routers.
rgmp	Specifies RGMP-capable routers.
mod/port	(Optional) Number of the module and the port on the module.
vlan_id	(Optional) Number of the VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the ports that have IGMP-multicast routers assigned to them:

```
Console> show multicast router igmp
Port    Vlan
------  ------
5/15    1
Total Number of Entries = 1
'*' - Configured
'+' - RGMP-capable
Console>
```

This example shows how to display the ports that have RGMP-multicast routers assigned to them:

```
Console> show multicast router rgmp
Port    Vlan
------  ------
5/1 +   1
5/14 +  2
Total Number of Entries = 2
'*' - Configured
'+' - RGMP-capable
Console>
```

Table 2-61 describes the fields in the **show multicast router** command output.

Table 2-61 show multicast router Command Output Fields

Field	Description
Port	Port through which a multicast router can be reached.
*	Status of whether the port was configured manually or not.
+	Status of whether the router is RGMP capable or not.
VLAN	VLAN associated with the port.
Total Number of Entries	Total number of entries in the table that match the criteria specified by the command.

Related Commands

set igmp
set multicast router
set rgmp
show multicast group
show multicast group count

show multicast v3-group

To display IGMP version 3 information based on group IP address, use the **show multicast v3-group** command.

show multicast v3-group [*vlan_num*] [*group_ip*]

Syntax Description

vlan_num	Number of the VLAN.
group_ip	IP address of the group.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Related Commands

set igmp v3-processing

show netstat

To display the currently active network connections and to list statistics for the various protocols in the TCP/IP, use the **show netstat** command.

show netstat [**tcp** | **udp** | **ip** | **icmp** | **routes** | **stats** | **interface**]

Syntax Description

tcp	(Optional) Shows TCP statistics.
udp	(Optional) Shows UDP statistics.
ip	(Optional) Shows IP statistics.
icmp	(Optional) Shows ICMP statistics.
routes	(Optional) Shows the IP routing table.
stats	(Optional) Shows all statistics for TCP, UDP, IP, and ICMP.
interface	(Optional) Shows interface statistics.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the current active network connections:

```
Console> show netstat
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp        0    128  172.20.25.142.23       171.68.10.75.44720     ESTABLISHED
tcp        0      0  *.7161                 *.*                    LISTEN
tcp        0      0  *.23                   *.*                    LISTEN
udp        0      0  *.*                    *.*
udp        0      0  *.161                  *.*
udp        0      0  *.123                  *.*
Console>
```

This example shows how to display TCP statistics:

```
Console> show netstat tcp
tcp:
        5122 packets sent
                4642 data packets (102292 bytes)
                28 data packets (6148 bytes) retransmitted
                434 ack-only packets (412 delayed)
                0 URG only packets
                0 window probe packets
                1 window update packet
                17 control packets
        7621 packets received
                4639 acks (for 103883 bytes)
                69 duplicate acks
                0 acks for unsent data
                3468 packets (15367 bytes) received in-sequence
                12 completely duplicate packets (20 bytes)
                0 packets with some dup. data (0 bytes duped)
                4 out-of-order packets (0 bytes)
                0 packets (0 bytes) of data after window
                0 window probes
                0 window update packets
                0 packets received after close
                0 discarded for bad checksums
                0 discarded for bad header offset fields
                0 discarded because packet too short
        6 connection requests
        6 connection accepts
        10 connections established (including accepts)
        11 connections closed (including 1 drop)
        2 embryonic connections dropped
        4581 segments updated rtt (of 4600 attempts)
        28 retransmit timeouts
                0 connections dropped by rexmit timeout
        0 persist timeouts
        66 keepalive timeouts
                63 keepalive probes sent
                3 connections dropped by keepalive
Console>
```

Table 2-62 describes the fields in the **show netstat tcp** command output.

Table 2-62 show netstat tcp Command Output Fields

Field	Description
packets sent	Total number of TCP packets sent.
data packets (bytes)	Number of TCP data packets sent and the size of those packets in bytes.
data packets (bytes) retransmitted	Number of TCP data packets retransmitted and the size of those packets in bytes.
ack-only packets (delayed)	Number of TCP acknowledgment-only packets sent and the number of those packets delayed.
URG only packets	Number of URG packets.
window probe packets	Number of window probe packets.
window update packet	Number of window update packets.
packets received	Total number of TCP packets received.
acks (for *x* bytes)	Number of TCP acknowledgments received and the total bytes acknowledged.
duplicate acks	Number of duplicate TCP acknowledgments received.
acks for unsent data	Number of TCP acknowledgments received for data that was not sent.

Table 2-62 show netstat tcp Command Output Fields (continued)

Field	Description
packets (bytes) received in-sequence	Number of TCP packets (and the size in bytes) received in sequence.
completely duplicate packets (bytes)	Number of duplicate TCP packets (and the size in bytes) received.
packets with some dup. data (bytes duped)	Number of TCP packets received with duplicate data (and the number of bytes of duplicated data).
out-of-order packets (bytes)	Number of out-of-order TCP packets (and the size in bytes) received.
packets (bytes) of data after window	Number of TCP packets (and the size in bytes) received outside of the specified data window.
discarded for bad checksums	Number of TCP packets received and discarded that failed the checksum.
discarded because packet too short	Number of TCP packets received and discarded that were truncated.
connection requests	Total number of TCP connection requests sent.
connection accepts	Total number of TCP connection accepts sent.
connections established (including accepts)	Total number of TCP connections established, including those for which a connection accept was sent.
connections closed (including *x* drops)	Total number of TCP connections closed, including dropped connections.
retransmit timeouts	Number of timeouts that occurred when a retransmission was attempted.
connections dropped by rexmit timeout	Number of connections dropped due to retransmission timeouts.
keepalive timeouts	Number of keepalive timeouts that occurred.
keepalive probes sent	Number of TCP keepalive probes sent.
connections dropped by keepalive	Number of connections dropped.

This example shows how to display UDP statistics:

```
Console> show netstat udp
udp:
        0 incomplete headers
        0 bad data length fields
        0 bad checksums
        0 socket overflows
        1116 no such ports
Console>
```

Table 2-63 describes the fields in the **show netstat udp** command output.

Table 2-63 show netstat udp Command Output Fields

Field	Description
incomplete headers	Number of UDP packets received with incomplete packet headers.
bad data length fields	Number of UDP packets received with a data length field that did not match the actual length of the packet payload.
bad checksums	Number of UDP packets received that failed the checksum.
socket overflows	Number of socket overflows.
no such ports	Number of UDP packets received destined for nonexistent ports.

This example shows how to display IP statistics:

```
Console> show netstat ip
ip:
        76894 total packets received
        0 bad header checksums
        0 with size smaller than minimum
        0 with data size < data length
        0 with header length < data size
        0 with data length < header length
        0 fragments received
        0 fragments dropped (dup or out of space)
        0 fragments dropped after timeout
        0 packets forwarded
        0 packets not forwardable
        0 redirects sent
Console>
```

Table 2-64 describes the fields in the **show netstat ip** command output.

Table 2-64 show netstat ip Command Output Fields

Field	Description
total packets received	Total number of IP packets received.
bad header checksums	Number of received IP packets that failed the checksum.
with size smaller than minimum	Number of received IP packets that were smaller than the minimum IP packet size.
with data size < data length	Number of packets in which the data size was less than the data length.
with header length < data size	Number of packets in which the header length was less than the data size.
with data length < header length	Number of packets in which the data length was less than the minimum header length.
fragments received	Number of IP packet fragments received.

Table 2-64 show netstat ip Command Output Fields (continued)

Field	Description
fragments dropped (dup or out of space)	Number of received IP packet fragments that were dropped because of duplicate data or buffer overflow.
fragments dropped after timeout	Number of received IP packet fragments that were dropped.
packets forwarded	Number of forwarded IP packets.
packets not forwardable	Number of IP packets that the switch did not forward.
redirects sent	Number of IP packets that the switch redirected.

This example shows how to display ICMP statistics:

```
Console> show netstat icmp
icmp:
        Redirect enabled
        0 calls to icmp_error
        0 errors not generated 'cuz old message was icmp
        Output histogram:
                echo reply: 1001
        1 message with bad code fields
        0 messages < minimum length
        0 bad checksums
        0 messages with bad length
        Input histogram:
                echo reply: 12
                destination unreachable: 3961
                echo: 1001
        1001 message responses generated
Console>
```

Table 2-65 describes the fields in the **show netstat icmp** command output.

Table 2-65 show netstat icmp Command Output Fields

Field	Description
Redirect enabled	Status of whether ICMP redirection is enabled or disabled.
Output histogram	Frequency distribution statistics for output ICMP packets.
echo reply	Number of output echo reply ICMP packets.
messages with bad code fields	Number of ICMP packets with an invalid code field.
messages < minimum length	Number of ICMP packets with less than the minimum packet length.
bad checksums	Number of ICMP packets that failed the checksum.
messages with bad length	Number of ICMP packets with an invalid length.

Table 2-65 show netstat icmp Command Output Fields (continued)

Field	Description
Input histogram	Frequency distribution statistics for input ICMP packets.
echo reply	Number of input echo-reply ICMP packets.
destination unreachable	Number of input destination-unreachable ICMP packets.
echo	Number of input-echo ICMP packets.
message responses generated	Number of ICMP message responses the system generated.

This example shows how to display the IP routing table:

```
Console> show netstat routes
DESTINATION     GATEWAY         FLAGS   USE             INTERFACE
default         172.16.1.201    UG      6186            sc0
172.16.0.0      172.16.25.142   U       6383            sc0
default         default         UH      0               sl0
Console>
```

Table 2-66 describes the fields in the **show netstat routes** command output.

Table 2-66 show netstat routes Command Output Fields

Field	Description
DESTINATION	Destination IP address or network.
GATEWAY	Next hop to the destination.
FLAGS	Flags indicating the interface state.
USE	Number of times this route was used.
INTERFACE	Interface out of which packets to the destination should be forwarded.

This example shows how to display interface statistics:

```
Console> show netstat interface
Interface          InPackets InErrors OutPackets OutErrors
sl0                        0        0          0         0
sc0                       33        0     117192         0
sc1                        2        0      57075         0
Interface Rcv-Octet            Xmit-Octet
--------- -------------------- --------------------
sc0       2389                 0
sc1       1172                 0
sl0       0                    0
Interface Rcv-Unicast          Xmit-Unicast
--------- -------------------- --------------------
sc0       28                   0
sc1       28                   0
sl0       0                    0
Console>
```

Table 2-67 describes the fields in the **show netstat interface** command output.

Table 2-67 show netstat interface Command Output Fields

Field	Description
Interface	Interface number (sl0 is the SLIP interface; sc0 and sc1 are the two in-band interfaces).
InPackets	Number of input packets on the interface.
InErrors	Number of input errors on the interface.
OutPackets	Number of output packets on the interface.
OutErrors	Number of output errors on the interface.
Rcv-Octet	Number of octet frames received on the port.
Xmit-Octet	Number of octet frames transmitted on the port.
Rcv-Unicast	Number of unicast frames received on the port.
Xmit-Unicast	Number of unicast frames transmitted on the port.

Related Commands

set interface
set ip route

show ntp

To display the current NTP status, use the **show ntp** command.

show ntp

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the current NTP status:

```
Console> show ntp
Current time: Tue Mar 28 2000, 11:19:03 pst
Timezone: 'pst', offset from UTC is -8 hours
Summertime: 'pst', enabled
Last NTP update:
Broadcast client mode: enabled
Broadcast delay: 3000 microseconds
Client mode: disabled

NTP-Server
----------------------------------------
time_server.cisco.com
Console>
```

Table 2-68 describes the fields in the **show ntp** command output.

Table 2-68 show ntp Command Output Fields

Field	Description
Current time	Current system time.
Timezone	Time zone and the offset in hours from UTC.
Summertime	Time zone for daylight saving time and whether the daylight saving time adjustment is enabled or disabled.
Last NTP update	Time of the last NTP update.
Broadcast client mode	Status of whether NTP broadcast-client mode is enabled or disabled.
Broadcast delay	Configured NTP broadcast delay.
Client mode	Status of whether NTP client mode is enabled or disabled.
NTP-Server	List of configured NTP servers.

Related Commands

clear ntp server
set ntp broadcastclient
set ntp broadcastdelay
set ntp client
set ntp server

show packet-capture

To display the current configuration for the Mini Protocol Analyzer feature, use the **show packet-capture** command.

show packet-capture

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the configuration of the Mini Protocol Analyzer feature:

```
Console> show packet-capture
Packet-capture parameter          Value
--------------------------------  ----------------------------------------------
Operational Status                Not-running
Dump File Name                    bootflash:eth
Filter - Source IP                any
Filter - Destination IP           any
Filter - Source MAC address       any
Filter - Destination MAC address  any
Number of packets to capture      1000
Packet Snap Length                0
Source Port                       Not Configured
Console>
```

Related Commands

clear packet-capture
set packet-capture
set packet-capture dump-file
set packet-capture filter
set packet-capture limit
set packet-capture snap-length

show pbf

To display PBF-related information, use the **show pbf** command.

show pbf [{**adjacency** | **statistics** | **map**} [*adj_name*]]

Syntax Description

adjacency	(Optional) Displays PBF adjacency information.
statistics	(Optional) Displays PBF statistics.
map	(Optional) Displays PBF adjacency map.
adj_name	(Optional) Name of the adjacency.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

To display MAC address information, enter the **show pbf** command with no options.

The **show adjacency map** command displays all the ACLs that use a specific adjacency.

Refer to the “Configuring Policy-Based Forwarding” section of Chapter 16, “Configuring Access Control,” in the *Catalyst 6500 Series Switch Software Configuration Guide* for detailed information about PBF.

Examples

This example shows how to display the MAC address for PFC2:

```
Console> show pbf
Pbf status    Mac address
-----------   ------------------
ok            00-01-64-61-39-c2
Console>
```

This example shows how to display adjacency information for PFC2:

```
Console> show pbf adjacency
Index    DstVlan   DstMac             SrcMac             Name
------------------------------------------------------------------
1         2      0a-0a-0a-0a-0a-0a  00-11-22-33-44-55     a_1
2         2      0a-0a-0a-0a-0a-0b  00-11-22-33-44-55     a_2
3         2      0a-0a-0a-0a-0a-0c  00-11-22-33-44-55     a_3
4         2      0a-0a-0a-0a-0a-0d  00-11-22-33-44-55     a_4
5         1      20-20-20-20-20-20  00-11-22-33-44-55     b_1
6         1      20-20-20-20-20-21  00-11-22-33-44-55     b_2
7         1      20-20-20-20-20-22  00-11-22-33-44-55     b_3
8         1      20-20-20-20-20-23  00-11-22-33-44-55     b_4
Console>
```

This example shows how to display adjacency information for adjacency **a_1**:

```
Console> show pbf adj a_1
Index    DstVlan   DstMac             SrcMac             Name
------------------------------------------------------------------
1          2      00-0a-0a-0a-0a-0a  00-11-22-33-44-55     a_1
Console>
```

This example shows how to display statistics for PFC2:

```
Console> show pbf statistics
Index    DstVlan   DstMac             SrcMac          HitCount(hex)  Name
-------------------------------------------------------------------------
1         2      0a-0a-0a-0a-0a-0a  00-11-22-33-44-55  0x00011eb4    a_1
2         2      0a-0a-0a-0a-0a-0b  00-11-22-33-44-55  0x00011ebc    a_2
3         2      0a-0a-0a-0a-0a-0c  00-11-22-33-44-55  0x00011ec3    a_3
4         2      0a-0a-0a-0a-0a-0d  00-11-22-33-44-55  0x00011eca    a_4
5         1      20-20-20-20-20-20  00-11-22-33-44-55  0x00011ed1    b_1
6         1      20-20-20-20-20-21  00-11-22-33-44-55  0x00011ed8    b_2
7         1      20-20-20-20-20-22  00-11-22-33-44-55  0x00011edf    b_3
8         1      20-20-20-20-20-23  00-11-22-33-44-55  0x00011ee6    b_4
Console>
```

This example shows how to display statistics for adjacency **a_1**:

```
Console> show pbf statistics a_1
Index    DstVlan   DstMac             SrcMac          HitCount(hex)  Name

-------------------------------------------------------------------------

1          2      00-0a-0a-0a-0a-0a  00-11-22-33-44-55  0x0038cd58    a_1
Console>
```

This example shows how to display the adjacency map for PFC2:

```
Console> show pbf map
Adjacency            ACL
------------------  --------------------
a_1                  ip1

a_2                  ip1

a_3                  ip1

a_4                  ip1

b_1                  ip2

b_2                  ip2

b_3                  ip2

b_4                  ip2
Console>
```

This example shows how to display the adjacency map for adjacency **a_1**:

```
Console> show pbf map a_1
Adjacency            ACL
------------------  --------------------
a_1                  ip1
Console>
```

Related Commands

clear pbf
set pbf

show pbf arp-inspection

To verify that an ARP-inspection ACE is set on the ACL for a client list or a gateway, use the **show pbf arp-inspection** command.

show pbf arp-inspection *list_name*

Syntax Description

list_name	Client list or gateway list.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

These examples show how to display whether or not ARP-inspection ACEs are on ACLs for a client list or a gateway:

```
Console> show pbf arp-inspection cl1
Arp-inspection ACE set.
Console>
Console> show pbf arp-inspection gw1
Arp-inspection ACE not set.
Console>
```

Related Commands

clear pbf arp-inspection
set pbf arp-inspection

show pbf client

To display the PBF client configuration, use the **show pbf client** command:

show pbf client [*client_name* | *ip_addr*]

Syntax Description

client_name	(Optional) Client name.
ip_addr	(Optional) IP address.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the PBF client configuration:

```
Console> show pbf client
Client    : cl1
Map       : gw1
VLAN      : 101
Adjacency          ip           mac
-------------------------------------------
.c0001cl1          21.1.1.1     00-00-00-00-40-01


Console>
```

Related Commands

clear pbf client
set pbf client

show pbf gw

To display the PBF gateway configuration, use the **show pbf gw** command.

show pbf gw [*gw_name* | *ip_addr*]

Syntax Description

gw_name	(Optional) Gateway name.
ip_addr	(Optional) IP address.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the PBF gateway configuration:

```
Console> show pbf gw
Client    : gw1
Map       : cl1
VLAN      : 102
Adjacency          ip           mask           mac
----------------------------------------------------------------
.g0002gw1          21.0.0.128   255.0.0.0    00-a0-c9-81-e1-13


Console>
```

Related Commands

clear pbf gw
set pbf gw

show pbf-map

To display PBF map information, use the **show pbf-map** command.

show pbf-map {*vlan* | **config**}

Syntax Description

vlan	VLAN number.
config	Displays the PBF_MAP configuration.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display PBF-related ACEs for the specified VLAN and statistics for each adjacency used:

```
Console> show pbf-map 11
Index    DstVlan   DstMac             SrcMac          HitCount(hex)  Name
-------------------------------------------------------------------------
1         22      00-00-00-00-00-02  00-00-00-00-00-00  0x00000000
PBF_MAP_ADJ_1
Console>
```

This example shows how to display all PBF maps and statistics:

```
Console> show pbf-map all

Index    DstVlan   DstMac             SrcMac          HitCount(hex)  Name
-------------------------------------------------------------------------
1         11      00-00-00-00-00-01  00-00-00-00-00-00  0x00000000 PBF_MAP_ADJ_0
2         22      00-00-00-00-00-02  00-00-00-00-00-00  0x00000000 PBF_MAP_ADJ_1
Console>
```

This example shows how to display the PBF_MAP configuration:

```
Console> show pbf-map config
set pbf_map 1.1.1.1 00-00-00-00-00-01 11 2.2.2.2 00-00-00-00-00-02 22
Console>
```

This example shows how to display all the PBF maps:

```
Console> show pbf-map
PBF MAP
Clients             Gatways
---------------------------------------------
cl1                   gw1
Console>
```

Related Commands

clear pbf client
clear pbf gw
clear pbf-map
set pbf client
set pbf gw
set pbf-map

show policy

To display information about policy groups and policy templates, use the **show policy** command.

show policy group {**all** | *group_name*}

show policy name {**all** | *policy_name*}

Syntax Description

group	Displays policy group information.
all	Displays information about all policy groups.
group_name	Group name of a specific policy group.
name	Displays policy templates and their associated policy groups.
all	Displays information about all policies.
policy_name	Policy name for a specific policy.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display policy group information:

```
Console> show policy group all
Group Name            = grp1
Group Id                  = 1
No.of IP Addresses = 3
Src Type                  = ACL CLI
     List of Hosts in group.
     -----------------------
     Interface      = 0/0
     IpAddress    =  100.1.1.1
     Src type       = CONFIG

     Interface      = 0/0
     IpAddress    = 100.1.1.2
     Src type       = CONFIG

--------------------------------------------------
Group Name             = grp2
Group Id                   = 2
No.of IP Addresses  = 0
Src Type                  = ACL CLI
Console>
```

8.6 EFT Copy

This example shows how to display policy templates and their associated policy groups:

```
Console> show policy name all
Policy Name : TEST
----------------------------------------------
Associated IP Address/Mask Information:
0.0.0.18/255.255.255.224
Policy Name : poll
----------------------------------------------
Associated IP Address/Mask Information:
0.0.0.19/255.255.255.224
Policy Name : BLDG_F
----------------------------------------------
Console>
```

This example shows how to display policy information for a specific policy name:

```
Console> show policy name exception_policy
Policy Name: exception_policy
----------------------------------------------
URL-Redirect: http://cisco.com
Associated MAC Address/Mask Information:
00-00-00-00-00-09
Associated Group(s):
group1
Console>
```

Related Commands

clear policy
set policy

show poll

To display system polling information, use the **show poll** command.

show poll

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display system polling information:

```
Console> show poll
System polling is enabled.
Console>
```

Related Commands

set poll

show port

To display port status information, use the **show port** command.

show port [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown.

If you do not specify a *port* value, all the ports on the module are shown.

The output for an 8-port T1/E1 PSTN interface module configured for transcoding or conferencing displays a transcoding port type as "mtp" (media termination point) or a conference port type as "conf bridge."

The output for an 8-port T1/E1 PSTN interface module displays a transcoding port type as "transcoding" or a conference port type as "conferencing."

The PAgP channel protocol and the LACP channel protocol manage channels differently. When all the ports in a channel get disabled, PAgP removes them from its internal channels list; **show** commands do not display the channel. With LACP, when all the ports in a channel get disabled, LACP does not remove the channel; **show** commands continue to display the channel even though all its ports are down. To determine if a channel is actively sending and receiving traffic with LACP, use the **show port** command to see if the link is up or down.

LACP does not support half-duplex links. If a port is in active/passive mode and becomes half duplex, the port is suspended (and a syslog message is generated). The port is shown as "connected" using the **show port** command and as "not connected" using the **show spantree** command. This discrepancy is because the port is physically connected but never joined spanning tree. To get the port to join spanning tree, either set the duplex to full or set the channel mode to off for that port.

For more information about PAgP and LACP, refer to the "Configuring EtherChannel" chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example shows how to display the status and counters for a specific module and port:

```
Console> show port 2/1
* = Configured MAC Address
Port  Name                 Status     Vlan       Duplex Speed Type
----- -------------------- ---------- ---------- ------ ----- ------------
 2/1                       notconnect 1            full  1000 No Connector


Port  Security Violation Shutdown-Time Age-Time Max-Addr Trap     IfIndex
----- -------- --------- ------------- -------- -------- -------- -------
 2/1  disabled  shutdown             0        0        1 disabled       3

Port  Num-Addr Secure-Src-Addr   Age-Left Last-Src-Addr     Shutdown/Time-Left
----- -------- ----------------- -------- ----------------- ------------------
 2/1         0                 -        -                 -        -         -

Port  Flooding on Address Limit
----- -------------------------
 2/1                    Enabled

Port     Broadcast-Limit Multicast Unicast Total-Drop           Action
-------- --------------- --------- ------- -------------------- ------------
 2/1                   -         -       -                    0 drop-packets

Port  Send FlowControl  Receive FlowControl   RxPause    TxPause
      admin    oper     admin     oper
----- -------- -------- --------- ---------   ---------- ----------
 2/1  desired  off      off       off         0          0

Port  Status     Channel              Admin Ch
                 Mode                 Group Id
----- ---------- -------------------- ----- -----
 2/1  notconnect auto silent             41     0

Port  Status      ErrDisable Reason    Port ErrDisableTimeout     Action on Timeout
----  ----------  -------------------  ----------------------     -----------------
 2/1  errdisable  other                Disable                    Remain Disabled (PRBS)

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 2/1           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 2/1           0          0          0          0         0         0         0

Port  Last-Time-Cleared
----- --------------------------
 2/1  Tue Mar 5 2002, 11:43:01
Console>
```

This example shows port information on a 48-port 10/100BASE-TX module with inline power:

```
Console> show port 9/5
* = Configured MAC Address
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 9/5                     notconnect 1            auto  auto 10/100BaseTX

Port  AuxiliaryVlan AuxVlan-Status     InlinePowered     PowerAllocated
                                   Admin Oper   Detected mWatt mA @42V
----- ------------- -------------- ----- ------ -------- ----- --------
 9/5  none          none           auto  off    no       0      0
```

```
Port  Security Violation Shutdown-Time Age-Time Max-Addr Trap     IfIndex
----- -------- --------- ------------- -------- -------- -------- -------
 9/5  disabled  shutdown             0        0        1 disabled     126

Port  Num-Addr Secure-Src-Addr   Age-Left Last-Src-Addr     Shutdown/Time-Left
----- -------- ----------------- -------- ----------------- ------------------
 9/5         0                 -        -                 -        -         -

Port  Flooding on Address Limit
----- -------------------------
 9/5                   Enabled

Port     Broadcast-Limit Broadcast-Drop
-------- --------------- --------------------
 9/5                   -                    0

Port   Send FlowControl    Receive FlowControl   RxPause TxPause Unsupported
       admin    oper       admin    oper                         opcodes
-----  -------- --------   -------- --------     ------- ------- -----------
 9/5   off      off        off      off          0       0       0

Port  Status     Channel              Admin Ch
                 Mode                 Group Id
----- ---------- -------------------- ----- -----
 9/5  notconnect auto silent            546     0

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 9/5           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 9/5           0          0          0          0         0         0         0

Last-Time-Cleared
--------------------------
Wed Mar 15 2000, 21:57:31
Console>
```

This example shows the port information on an 8-port T1/E1 PSTN interface module configured for transcoding and conferencing:

```
Console> show port 7
* = Configured MAC Address
Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- -------------- ---------------
 7/1                     connected  123        full   1.544 T1
 7/2                     connected  2          full   1.544 T1
 7/3                     disable    1          full   1.544 T1
 7/4                     connected  11         full   1.544 T1
 7/5                     connected  123        full   1.544 T1
 7/6                     connected  1          full   1.544 T1
 7/7                     faulty     2          full   1.544 conf bridge
 7/8                     faulty     2          full   1.544 mtp

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 7/1     enable  00-10-7b-00-0a-58 172.20.34.68    255.255.255.0
 7/2     enable  00-10-7b-00-0a-59 172.20.34.70    255.255.255.0
 7/3     enable  00-10-7b-00-0a-5a 172.20.34.64    255.255.255.0
 7/4     enable  00-10-7b-00-0a-5b 172.20.34.66    255.255.255.0
 7/5     enable  00-10-7b-00-0a-5c 172.20.34.59    255.255.255.0
 7/6     enable  00-10-7b-00-0a-5d 172.20.34.67    255.255.255.0
 7/7     enable  00-10-7b-00-0a-5e (Port host processor not online)
 7/8     enable  00-10-7b-00-0a-5f (Port host processor not online)

Port     Call-Manager(s)   DHCP-Server     TFTP-Sever      Gateway
-------- ----------------- --------------- --------------- ---------------
 7/1     172.20.34.207*    172.20.34.207   172.20.34.207   -
         callm.cisco.com
 7/2     172.20.34.207     172.20.34.207   172.20.34.207   172.20.34.20
 7/3     172.20.34.207     172.20.34.207   172.20.34.207   -
 7/4     172.20.34.207     172.20.34.207   172.20.34.207   -
 7/5     172.20.34.207     172.20.34.207   172.20.34.207   -
 7/6     172.20.34.207     172.20.34.207   172.20.34.207   -
 7/7     (Port host processor not online)
 7/8     (Port host processor not online)

Port     DNS-Server(s)   Domain
-------- --------------- -------------------------------------------------
 7/1     172.20.34.207   cisco.com
 7/2     172.20.34.207*  int.cisco.com
         171.69.45.34
         172.78.111.132
 7/3     172.20.34.207   -
 7/4     172.20.34.207   -
 7/5     172.20.34.207   -
 7/6     172.20.34.207   -
 7/7     (Port host processor not online)
 7/8     (Port host processor not online)

Port     CallManagerState DSP-Type
-------- ---------------- --------
 7/1     registered       C549
 7/2     registered       C549
 7/3     registered       C549
 7/4     registered       C549
 7/5     registered       C549
 7/6     notregistered    C549
 7/7     (Port host processor not online)
 7/8     (Port host processor not online)
Port  NoiseRegen NonLinearProcessing
----- ---------- -------------------
 7/1  disabled   disabled
 7/2  disabled   disabled
 7/3  disabled   disabled
 7/4  disabled   disabled
 7/5  enabled    disabled
 7/6  disabled   enabled
 7/7  (Port host processor not online)
 7/8  (Port host processor not online)

(*): Primary
Console>
```

This example show the port information on a 24-port FXS analog station interface services-configured module:

```
Console> (enable) show port 3
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/1                     onhook     1            full   64k FXS
 3/2                     onhook     1            full   64k FXS
 3/3                     onhook     1            full   64k FXS
 3/4                     onhook     1            full   64k FXS
 3/5                     onhook     1            full   64k FXS
 3/6                     onhook     1            full   64k FXS
 3/7                     onhook     1            full   64k FXS
 3/8                     onhook     1            full   64k FXS
 3/9                     onhook     1            full   64k FXS
 3/10                    onhook     1            full   64k FXS
 3/11                    onhook     1            full   64k FXS
 3/12                    onhook     1            full   64k FXS
 3/13                    onhook     1            full   64k FXS
 3/14                    onhook     1            full   64k FXS
 3/15                    onhook     1            full   64k FXS
 3/16                    onhook     1            full   64k FXS
 3/17                    onhook     1            full   64k FXS
 3/18                    onhook     1            full   64k FXS
 3/19                    onhook     1            full   64k FXS
 3/20                    onhook     1            full   64k FXS
 3/21                    onhook     1            full   64k FXS
 3/22                    onhook     1            full   64k FXS
 3/23                    onhook     1            full   64k FXS
 3/24                    onhook     1            full   64k FXS

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 3/1-24  enable  00-10-7b-00-13-e4 172.20.34.50    255.255.255.0

Port     Call-Manager      DHCP-Server     TFTP-Sever      Gateway
-------- ----------------- --------------- --------------- ---------------
 3/1-24  172.20.34.207     172.20.34.207   172.20.34.207   -

Port     DNS-Server      Domain
-------- --------------- --------------------------
 3/1-24  172.20.34.207   -

Port     EchoCancel(ms) CallManagerState DSP-Type
-------- -------------- ---------------- --------
 3/1-24  4660           registered       C549

Port     ToneLocal     Impedance InputGain(dB) OutputAtten(dB)
-------- ------------- --------- ------------- ---------------
 3/1-24  northamerica  0         0             0

Port     RingFreq Timing    Timing         Timing    Timing
         (Hz)     Digit(ms) InterDigit(ms) Pulse(ms) PulseDigit(ms)
-------- -------- --------- -------------- --------- --------------
 3/1-24  20       100       100            0         0
Console> (enable)
```

Table 2-69 describes the possible fields (depending on the port type queried) in the **show port** command output.

Table 2-69 show port Command Output Fields

Field	Description
Port	Module and port number.
Name	Name (if configured) of the port.
Status	Status of the port (connected, notconnect, connecting, standby, faulty, inactive, shutdown, disabled, monitor, active, dot1p, untagged, inactive, or onhook).
Vlan	VLANs to which the port belongs.
Auxiliaryvlan[1]	Auxiliary VLANs to which the port belongs.
Duplex	Duplex setting for the port (auto, full, half).
Speed	Speed setting for the port (auto, 10, 100, 1000).
Type[2]	Port type (for example, 1000BASE-SX or 100BASE-FX, or T1, E1, transcoding, conferencing, mtp, or conf bridge for voice ports).
Security	Status of whether port security is enabled or disabled.
Secure-Src-Addr	Secure MAC address for the security-enabled port.
Last-Src-Addr	Source MAC address of the last packet received by the port.
Broadcast-Limit	Broadcast threshold configured for the port.
Multicast	Number of multicast packets dropped.
Unicast	Number of unicast packets dropped.
Total-Drop	Number of broadcast, multicast, and unicast packets dropped because the port broadcast limit was exceeded.
Shutdown	Status of whether the port was shut down because of security.
Trap	Status of whether the port trap is enabled or disabled.
IfIndex	Number of the ifIndex.
Broadcast-Limit	Broadcast threshold configured for the port.
Broadcast-Drop	Number of broadcast/multicast packets dropped because the broadcast limit for the port was exceeded.
Errdisable Reason	Reason for the port to be in errdisabled state.
Port ErrDisableTimeout	Status of errdisable timer timeout on the port.
Action on Timeout	Action that is taken on errdisable timer timeout.
Align-Err	Number of frames with alignment errors (frames that do not end with an even number of octets and have a bad CRC) received on the port.
FCS-Err	Number of valid size frames with FCS errors but no framing errors.
Xmit-Err	Number of transmit errors that occurred on the port (indicating that the internal transmit buffer is full).
Rcv-Err	Number of receive errors that occurred on the port (indicating that the internal receive buffer is full).

Table 2-69 show port Command Output Fields (continued)

Field	Description
UnderSize	Number of received frames less than 64 octets long (but are otherwise well-formed).
Single-Coll	Number of times one collision occurred before the port transmitted a frame to the media successfully.
Multi-Coll	Number of times multiple collisions occurred before the port transmitted a frame to the media successfully.
Late-Coll	Number of late collisions (collisions outside the collision domain).
Excess-Col	Number of excessive collisions that occurred on the port (indicating that a frame encountered 16 collisions and was discarded).
Carri-Sen	Number of times the port sensed a carrier (to determine whether the cable is currently being used).
Runts	Number of received runt frames (frames that are smaller than the minimum IEEE 802.3 frame size) on the port.
Giants	Number of received giant frames (frames that exceed the maximum IEEE 802.3 frame size) on the port.
CE-State	Connection entity status.
Conn-State	Connection state of the port, as follows: • Disabled—The port has no line module or was disabled by the user. • Connecting—The port attempted to connect or was disabled. • Standby—The connection was withheld or was the inactive port of a dual-homing concentrator. • Active—The port made a connection. • Other—The concentrator was unable to determine the Conn-State.
Type	Type of port, such as A—A port and B—B port.
Neig	Type of port attached to this port. The neighbor can be one of these types: • A—A port • B—B port • M—M port • S—Slave port • U—The concentrator cannot determine the type of the neighbor port.
Ler Con	Status of whether the port is currently in a LER condition.
Est	Estimated LER.
Alm	LER at which a link connection exceeds the LER alarm threshold.
Cut	LER cutoff value (the LER at which a link connection is flagged as faulty).
Lem-Ct	Number of LEM errors received on the port.

Table 2-69 show port Command Output Fields (continued)

Field	Description
Lem-Rej-Ct	Number of times a connection was rejected because of excessive LEM errors.
Last-Time-Cleared	Last time the port counters were cleared.
Auto-Part	Number of times the port entered the auto-partition state due to excessive consecutive collisions.
Data-rate mismatch	Number of valid size frames that experienced overrun or underrun.
Src-addr change	Number of times the last source address changed.
Good-bytes	Total number of octets in frames with no error.
Short-event	Number of short events received.
InlinePowered[1]	InlinePowered for Admin (auto, on, off), Oper (on, off, denied), and Detected (yes, no).
PowerAllocated[1]	PowerAllocated for Watts (values displayed as Watts measurement) and Volts (values displayed as Volts measurement).
Age-Time[1]	Age timeout setting for the port.
Age-Left[1]	Age timeout remaining for the port.
Maximum-Addrs[1]	Maximum number of secured MAC addresses on the port.
CallManagerState[1]	Operational state of the voice port (Not Registered, Registered, Up, Down, and Alarm).
NoiseRegen[3]	Status of whether noise regeneration is enabled for the port.
NonLinear[3]	Status of whether nonlinear processing is enabled for the port.
Comp-Alg[3]	Type of compression algorithm used (for example G.711, G.723, and G.729).
IP-address[3]	IP address associated with the port.
Netmask[3]	Netmask associated with the port.
MAC-Address[3]	MAC address associated with the port.
Call-Manager-IP[3]	Cisco CallManager IP address associated with the port.
DHCP-Server-IP[3]	DHCP server IP address associated with the port.
DNS-Server-IP[3]	DNS server IP address associated with the port.
TFTP-Server-IP[3]	TFTP server IP address associated with the port.

[1] This field is applicable to the 48-port 10/100BASE-TX switching services-configured module.

[2] This field changes according to the system configuration.

[3] This field is applicable to the 8-port T1/E1 DSP services-configured module.

Related Commands

set port disable
set port enable
show port status

show port arp-inspection

To display the drop threshold, the shutdown threshold, and the DAI trust status for specific ports, use the **show port arp-inspection** command.

show port arp-inspection [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a module, the system displays the drop threshold, the shutdown threshold, and the DAI trust status for all ports.

Examples

This example shows how to display the thresholds on module 2, port 1:

```
Console> (enable) show port arp-inspection 2/1
Port                      Drop Threshold Shutdown Threshold        Trust
------------------------  -------------- ------------------       ---------
 2/1                                   0                  0       untrusted
Console> (enable)
```

Related Commands

set port arp-inspection
set security acl arp-inspection

show port auto-mdix

To display the status of the automatic Media-Dependent Interface Crossover (MDIX) feature on a port, use the **show port auto-mdix** command.

show port auto-mdix [*mod*[*/port*]]

Syntax Description

mod[*/port*]	(Optional) Number of the module and optionally, the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal mode.

Usage Guidelines

If you do not enter any arguments, the status of the automatic MDIX feature displays for all ports that support the feature

Related Commands

set port auto-mdix

show port auxiliaryvlan

To display the port auxiliary VLAN status for a specific port, use the **show port auxiliaryvlan** command.

show port auxiliaryvlan {*vlan* | **untagged** | **dot1p** | **none**}

Syntax Description

vlan	Number of the VLAN; valid values are from 1 to 4094.
untagged	Displays the Cisco IP Phone 7960 that sends untagged packets without 802.1p priority.
dot1p	Displays the Cisco IP Phone 7960 that sends packets with 802.1p priority.
none	Displays the switch that does not send any auxiliary VLAN information in the CDP packets from that port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to display the port information for a specific auxiliary VLAN:

```
Console> (enable) show port auxiliaryvlan
AuxiliaryVlan Status   Mod/Ports
------------- -------- -----------------------------------------------------
222           active   8/4-7
333           active   8/13-18
dot1p         dot1p    8/23,8/31-34
untagged      untagged 9/12
none          none     8/1-3,8/8-12,8/19-22,8/24-30,8/35-48,9/1-11,9/13-48
Console> (enable)
```

This example shows how to display the port information for a specific auxiliary VLAN:

```
Console> (enable) show port auxiliaryvlan 222
AuxiliaryVlan Status   Mod/Ports
------------- -------- -----------------------------------------------------
222           active   8/4-7
Console> (enable)
```

This example shows how to display the status of the switch that does not send any auxiliary VLAN information in the CDP packets:

```
Console> (enable) show port auxiliaryvlan none
AuxiliaryVlan Status   Mod/Ports
------------- -------- -----------------------------------------------------
none          none     8/1-3,8/8-12,8/19-22,8/24-30,8/35-48,9/1-11,9/13-48
Console> (enable)
```

This example shows how to display the status of the Cisco IP Phone 7960 that sends untagged packets without 802.1p priority:

```
Console> (enable) show port auxiliaryvlan untagged
AuxiliaryVlan Status   Mod/Ports
------------- -------- -----------------------------------------------------
untagged      untagged 9/12
Console> (enable)
```

This example shows how to display the status of the Cisco IP Phone 7960 that sends packets with 802.1p priority:

```
Console> (enable) show port auxiliaryvlan dot1p
AuxiliaryVlan Status   Mod/Ports
------------- -------- -----------------------------------------------------
dot1p         dot1p    8/23,8/31-34
Console> (enable)
```

Table 2-70 describes the possible fields (depending on the port type queried) in the **show port auxiliaryvlan** command output.

Table 2-70 show port auxiliaryvlan Command Output Fields

Field	Description
AuxiliaryVlan	Number of the auxiliary VLAN.
AuxVlanStatus	Status of the auxiliary VLAN.
Mod/Ports	Number of the module and ports assigned to the auxiliary VLAN.

Related Commands

set port auxiliaryvlan

show port broadcast

To display broadcast information, use the **show port broadcast** command.

show port broadcast [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown.

If you do not specify a *port* value, all the ports on the module are shown.

On the 1000BASE-X switching module, when you specify a port for broadcast suppression, the traffic is suppressed only in the network-to-Catalyst 6500 series switch bus direction.

Examples

This example shows how to display broadcast information for module 4, port 6:

```
Console> show port broadcast 4/6
Port     Broadcast-Limit Multicast Unicast Total-Drop           Violation
-------- --------------- --------- ------- -------------------- ------------
 4/6             90.00 %         -       -                    0 drop-packets
Console>
```

Table 2-71 describes the possible fields (depending on the port type queried) in the **show port broadcast** command output.

Table 2-71 show port broadcast Command Output Fields

Field	Description
Port	Module and port number.
Broadcast-Limit	Broadcast threshold configured for the port.
Multicast	Number of multicast packets dropped.
Unicast	Number of unicast packets dropped.

Table 2-71 show port broadcast Command Output Fields (continued)

Field	Description
Total-Drop	Number of broadcast, multicast, and unicast packets dropped because the port broadcast limit was exceeded.
Violation	Action the port takes when the broadcast threshold is exceeded; the port either errdisables or drops packets.

Related Commands

set port broadcast

show port capabilities

To display the capabilities on the ports, use the **show port capabilities** command.

show port capabilities [*mod*[/*port*]]

show port capabilities vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown.

If you do not specify a *port* value, all the ports on the module are shown.

Examples

This example shows how to list the port capabilities on a specific module and port:

```
Console> show port capabilities 1/1
Model                        WS-X6548-RJ-45
Port                         1/1
Type                         10/100BaseTX
Auto MDIX                    yes
AuxiliaryVlan                1..4094,untagged,dot1p,none
Broadcast suppression        percentage(0-100)
Channel                      yes
COPS port group              not supported
CoS rewrite                  yes
Dot1q-all-tagged             yes
Dot1x                        yes
Duplex                       half,full
Fast start                   yes
Flow control                 receive-(off,on),send-(off)
Inline power                 no
Jumbo frames                 yes
Link debounce timer          yes
Link debounce timer delay    no
Membership                   static,dynamic
Port ASIC group              1/1-48
Port VLAN Mapping           Group:1/1-48     Maximum Allowed Mappings:32
QOS scheduling              rx-(1p1q0t),tx-(1p3q1t)
Security                    yes
SPAN                        source,destination
Speed                       auto,10,100
Sync restart delay          no
ToS rewrite                 no
Trunk encap type            802.1Q,ISL
Trunk mode                  on,off,desirable,auto,nonegotiate
UDLD                        yes
Console>
```

This example shows the port capabilities on a 48-port 10/100BASE-TX switching services configured-module:

```
Console> show port capabilities 3/2
Model                    WS-X6248-RJ-45
Port                     3/2
Type                     10/100BaseTX
Speed                    auto,10,100
Duplex                   half,full
Trunk encap type         802.1Q,ISL
Trunk mode               on,off,desirable,auto,nonegotiate
Channel                  yes
Broadcast suppression    percentage(0-100)
Flow control             receive-(off,on),send-(off)
Security                 yes
Membership               static
Fast start               yes
QOS scheduling           rx-((null)),tx-((null))
QOS classification       layer 2,layer 3
UDLD                     Capable
SPAN                     source,destination
Inline power             auto,on,off
Auxiliaryvlan            1..1000,dot1p,untagged,none
Console>
```

This example shows the port capabilities on an 8-port T1/E1 ISDN PRI services configured-module:

```
Console> show port capabilities 3/2
Model                    WS-X6608-T1   (or WS-X6608-E1)
Port                     3/2
Type                     T1, transcoding, conferencing
Speed                    1.544 Mps     (or 2.048Mps)
Duplex                   full
Channel                  no
Broadcast suppression    no
Flow control             no
Security                 no
Membership               no
Fast start               no
QOS scheduling           no
QOS classification       no
UDLD                     no
Inline power             no
Auxiliaryvlan            no
Console>
```

This example shows the port capabilities on a 24-port FXS analog station interface services-configured module:

```
Console> show port capabilities 3/2
Model                    WS-X6624-FXS
Port                     3/2
Type                     FXS
Speed                    64kps
Duplex                   full
Trunk encap type         none
Trunk mode               off
Channel                  no
Broadcast suppression    no
Flow control             no
Security                 no
Membership               no
Fast start               no
QOS scheduling           no
QOS classification       no
UDLD                     no
Inline power             no
Auxiliaryvlan            no
Console>
```

This example shows the port capabilities on an Intrusion Detection System Module:

```
Console> show port capabilities 5/2
Model                    WS-X6381-IDS
Port                     5/2
Type                     Intrusion Detection
Speed                    1000
Duplex                   full
Trunk encap type         no
Trunk mode               no
Channel                  no
Broadcast suppression    no
Flow control             no
Security                 no
Dot1x                    no
Membership               static
Fast start               no
QOS scheduling           rx-(none),tx-(none)
CoS rewrite              no
ToS rewrite              no
UDLD                     no
Inline power             no
AuxiliaryVlan            no
SPAN                     source
COPS port group          not supported
Link debounce timer      yes
Console>
```

Table 2-72 describes the possible fields (depending on the type of port queried) and the values in the **show port capabilities** command output.

Table 2-72 show port capabilities Command Output Fields

Field	Description
Model	Module model number.
Port	Module number and port number.
Type[1]	Port type (1000BASE-SX or 100BASE-FX).
Auto MDIX	Status of whether the port supports the automatic Media-Dependent Interface Crossover (MDIX) function (yes, no).
Auxiliaryvlan[2]	Status of whether the port supports voice VLANs (yes, no).
Broadcast suppression	Percentage of total available bandwidth that can be used by broadcast traffic (0–100).
Channel	Status of which ports can form a channel group. The ports are shown in *mod/port* format. For example, 3/1-2 indicates module 3, ports 1 and 2. Also, any ports in range [*mod/1-mod/high_port*] or no ports may be indicated.
COPS port group	Status of whether the port supports COPS port group (not supported, ports that are supported).
CoS rewrite	Status of whether the port supports CoS rewrite (yes, no).
Dot1q-all-tagged	Status of whether the port supports the 802.1Q tagging feature (yes, no).
Duplex	Duplex mode (half, full, auto).
Fast start	Status of whether the spanning tree PortFast-start feature on the port is enabled (yes, no).
Flow control	Flow-control options you can set (receive-[off, on, desired], send-[off, on, desired], or no).
Inline power[2]	Status of whether the port supports inline power (yes, no).
Jumbo Frames	Status of whether the port supports Jumbo Frames (yes, no).
Link debounce timer	Status of whether the port supports debounce timer (yes, no).
Link debounce timer delay	Status of whether the port supports the link debounce timer delay (yes, no).
Membership	Method of membership assignment of a port or range of ports to a VLAN (static, dynamic).
Port ASIC group	Ports controlled by a port ASIC.
Port VLAN Mapping	Ports that support VLAN mapping and the maximum number of mappings allowed.
QOS classification	Status of whether the port supports QoS classification (yes, no).
QOS scheduling	Status of whether the port supports QoS scheduling (yes, no).
Security	Status of whether port security is enabled (yes, no).
SPAN	SPAN type supported.
Speed[1]	Speed setting for the port (auto, 10, 100, 1000).

8.6 EFT Copy

Table 2-72 show port capabilities Command Output Fields (continued)

Field	Description
Sync restart delay	Status of whether the port supports the synchronization restart delay function (yes, no).
ToS rewrite	Status of whether the port supports ToS rewrite (IP-Precedence).
Trunk encap type[2]	Trunk encapsulation type (ISL, 802.1Q, 802.10, or no).
Trunk mode[2]	Trunk administrative status of the port (on, off, auto, desirable, nonegotiate, or no).[3]
UDLD	Status of whether the port is UDLD-capable or not.

[1] This field will change depending on the module configuration.

[2] This field is applicable to the 48-port 10/100BASE-TX switching services-configured module and the 24-port FXS analog station interface services-configured module.

[3] "No" means that the port is trunk incapable.

Related Commands

set port broadcast
set port channel
set port security
set port speed
set spantree portfast
set trunk
show port
show port voice active

show port cdp

To display the port CDP enable state and the message interval, use the **show port cdp** command.

show port cdp [*mod*[/*port*]]

show port cdp vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown.

If you do not specify a *port* value, all the ports on the module are shown.

Examples

This example shows how to display CDP information for all ports:

```
Console> show port cdp
CDP                : enabled
Message Interval   : 60
Hold Time          : 180
Version            : V2

Port      CDP Status
--------  ----------
 1/1      enabled
 1/2      enabled
Console>
```

Table 2-73 describes the fields in the **show port cdp** command output.

Table 2-73 show port cdp Command Output Fields

Field	Description
CDP	Status of whether CDP is enabled or not.
Message-Interval	Interval between CDP message exchange with a neighbor.

Table 2-73 show port cdp Command Output Fields (continued)

Field	Description
Hold Time	Hold time setting.
Version	CDP version.
Port	Module and port number.
CDP Status	CDP status of the port (enabled, disabled).

Related Commands

set cdp
show cdp

show port channel

To display EtherChannel information, use the **show port channel** command.

show port channel [**all** | *mod*[*/port*]] [**statistics**]

show port channel [**all** | *mod*[*/port*]] {**info** [*type*]}

Syntax Description

all	(Optional) Displays information about PAgP and LACP channels.
mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
statistics	(Optional) Displays statistics about the port (PAgP packets sent and received).
info	(Optional) Displays port information such as speed, duplex status, priority, secure or dynamic status, and trunk status.
type	(Optional) Displays feature-related parameters; valid values are **spantree**, **trunk**, **protocol**, **gmrp**, **gvrp**, **qos**, **rsvp**, **cops**, **dot1qtunnel**, **auxiliaryvlan**, **jumbo**, **l2prottunnel**, **security-acl**, **dhcp-snooping**, **arp-inspection**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The protocol conditions are as follows:

- On indicates the port will receive all the flood traffic for that protocol.
- Off indicates the port will not receive any flood traffic for that protocol.
- Auto indicates the port will not receive any flood traffic for that protocol.

The GVRP registration status is defined as follows:

- Normal allows dynamic registering and deregistering each VLAN (except VLAN 1) on the port.
- Fixed supports manual VLAN creation and registration and prevents VLAN deregistration.
- Forbidden statically deregisters all the VLANs (except VLAN 1) from the port.

When you enter the **option** keyword with any of the options (**spantree** | **trunk** | **protocol** | **gmrp** | **gvrp** | **qos** | **rsvp** | **cops** | **dot1qtunnel** | **auxiliaryvlan** | **jumbo**), associated VLANs and the specified feature-related parameters are displayed.

If you do not specify a *mod* or a *port*, EtherChannel information is shown for all PAgP channeling ports on all modules.

If you enter the **all** keyword, information about PAgP and LACP channels is displayed.

Examples

This example shows how to display Ethernet channeling information for module 1:

```
Console> show port channel 1
Port  Status     Channel   Admin Ch
                 Mode      Group Id
----- ---------- --------- ----- -----
 1/1  nonconnect on        195   769
 1/2  connected  on        195   769

Port  Device-ID                       Port-ID                   Platform
----- ------------------------------- ------------------------- ----------------
 1/1
 1/2
Console>
```

This example shows how to display port statistics:

```
Console> show port channel 4 statistics
Port  Admin   PAgP Pkts   PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts
      Group   Transmitted Received  InFlush   RetnFlush OutFlush  InError
----- ------- ----------- --------- --------- --------- --------- ---------
 4/1       69          20         0         0         0         0         0
 4/2       69         105        60         0         0         0         0
 4/3      151           0         0         0        10         0         0
 4/4      151           0         5         0         0         0         0
 4/5       70           0         0         0         0         0         0
 4/6       70          42         0         0         2         0         0
 4/7      152           0        92         0         0         0         0
 4/8      152           0         0         0         0         0         0
Console>
```

This example shows how to display port information:

```
Console> show port channel 1 info
Switch Frame Distribution Method:mac both

Port  Status     Channel   Admin Channel Speed Duplex Vlan PortSecurity/
                 mode      group id                        Dynamic port
----- ---------- --------- ----- ------- ----- ------ ---- -------------
 1/1  notconnect auto          1       0 1000  full      1 -
 1/2  connected  auto          1       0 1000  full      1 -

Port  ifIndex Oper-group Neighbor   Oper-Distribution
                         Oper-group Method
----- ------- ---------- ---------- -----------------
 1/1  -                1            mac both
 1/2  -                2            mac both

Port  Device-ID                       Port-ID                   Platform
----- ------------------------------- ------------------------- ----------------
 1/1
 1/2

Port  Trunk-status Trunk-type    Trunk-vlans
----- ------------ ------------- -----------------------------------------------
 1/1  not-trunking negotiate     1-1005
 1/2  not-trunking negotiate     1-1005

Port  Portvlancost-vlans
----- --------------------------------------------------------------------------
 1/1
 1/2
```

```
Port  Port     Portfast Port    Port
      priority          vlanpri vlanpri-vlans
----- -------- -------- ------- ------------------------------------------------
 1/1        32 disabled       0
 1/2        32 disabled       0

Port  IP       IPX      Group
----- -------- -------- --------
 1/1  on       auto-on  auto-on
 1/2  on       auto-on  auto-on

Port  GMRP     GMRP         GMRP
      status   registration forwardAll
----- -------- ------------ ----------
 1/1  enabled  normal       disabled
 1/2  enabled  normal       disabled

Port  GVRP     GVRP          GVRP
      status   registeration applicant
----- -------- ------------- ---------
 1/1  disabled normal        normal
 1/2  disabled normal        normal

Port  Qos-Tx Qos-Rx Qos-Trust    Qos-DefCos
----- ------ ------ ------------ ----------
 1/1  2q2t   1q4t   untrusted             0
 1/2  2q2t   1q4t   untrusted             0
Console>
```

These examples show how to display feature-specific parameter information:

```
Console> (enable) show port channel 3 info spantree
Port  Port     Portfast Port    Port
      priority          vlanpri vlanpri-vlans
----- -------- -------- ------- ------------------------------------------------
3/1        32 disabled      12 2,4,90
3/2        32 disabled      12 2,4,90
3/3        32 disabled      12 2,4,90
3/4        32 disabled      12 2,4,90
Console>

Console> (enable) show port channel 3 info trunk
Port  Trunk-status Trunk-type    Trunk-vlans
----- ------------ ------------- -----------------------------------------------
3/1  not-trunking negotiate     1-1005
3/2  not-trunking negotiate     1-1005
3/3  not-trunking negotiate     1-1005
3/4  not-trunking negotiate     1-1005
Console>

Console> (enable) show port channel 3 info protocol
Port  IP       IPX      Group
----- -------- -------- --------
3/1  on       auto-on  auto-on
3/2  on       auto-on  auto-on
3/3  on       auto-on  auto-on
3/4  on       auto-on  auto-on
Console>
Console> (enable) show port channel 3 info gmrp
Port  GMRP     GMRP         GMPR
      status   registration forwardAll
----- -------- ------------ ----------
3/1  enabled  normal       disabled
3/2  enabled  normal       disabled
```

```
3/3  enabled  normal       disabled
3/4  enabled  normal       disabled
Console>

Console> (enable) show port channel 1 info gvrp
Port  GVRP     GVRP          GVRP
      status   registeration applicant
----- -------- ------------- ---------
1/1   disabled normal        normal
1/2   disabled normal        normal
Console>

Console> (enable) show port channel 1 info qos
Port  Qos-Tx   Qos-Rx   Qos-Trust    Qos-DefCos Qos-Interface
      PortType PortType Type                    Type
----- -------- -------- ------------ ---------- --------------
1/1   2q2t     1q4t     untrusted             0 port-based
1/2   2q2t     1q4t     untrusted             0 port-based
----- -------- -------- ------------ ---------- --------------

Port  ACL name                         Type
----- -------------------------------- ----
1/1                                    IP
                                       IPX
                                       MAC
1/2                                    IP
                                       IPX
                                       MAC
Port  Policy Source
----- -------------
1/1           COPS
1/2           COPS
Console>
```

Table 2-74 describes the possible fields (depending on the type of port queried) and the values in the **show port channel** command outputs.

Table 2-74 show port channel Command Outputs Fields

Field	Description
Port	Module and port number.
Status	Channeling status of the port (connected, notconnect).
Channel mode	Status of whether EtherChannel is on, off, auto, or desirable on the port.
Admin Group	Number of the admin group.
PAgP Pkts Transmitted	Number of PAgP packets transmitted.
PAgP Pkts Received	Number of PAgP packets received.
PAgP Pkts InFlush	Number of PAgP flush packets received.
PAgP Pkts RetnFlush	Number of PAgP flush packets returned.
PAgP Pkts OutFlush	Number of PAgP flush packets transmitted.
PAgP Pkts InError	Number of PAgP error packets received.
Channel ID	Number of the channel group.
Neighbor device	Neighboring device with which the port is channeling.
Neighbor port	Port on the neighboring device with which the port is channeling.

Table 2-74 show port channel Command Outputs Fields (continued)

Field	Description
Speed	Speed setting for the port (auto, 10, 100, 1000).
Duplex	Duplex setting for the port (auto, full, half).
Vlan	VLAN to which the port belongs.
Port priority	Priority associated with the port.
PortSecurity/Dynamic port	Status of whether the port is secure or dynamic.
ifIndex	Interface number to which the port belongs.
Oper-group	Capability of the group.
Neighbor device-id	Device ID of the neighboring device with which the port is channeling.
Neighbor port-id	Port ID of the neighboring device with which the port is channeling.
Neighbor Oper-group	Capability of the neighboring device.
Oper-Distribution	Frame distribution method operating status on a per-port basis (ip source, ip destination, ip both, mac source, mac destination, mac both, hotstandby-active, or hotstandby-idle).
Trunk-status	Status of whether the port is trunking or not.
Trunk-type	Type of trunk port.
Trunk-vlans	VLANs to which the port belongs.
Portvlancost-vlans	Port VLAN cost.
Portfast	Status of whether the PortFast-start mode is enabled or disabled.
Port vlanpri	Port VLAN priority.
Port vlanpri-vlans	Priority VLAN number.
IP	Status of the IP protocol (on, off, auto).
IPX	Status of the IPX protocol (on, off, auto).
Group	Status of the VINES, AppleTalk, and DECnet protocols (on, off, auto).
GMRP status	Status of whether GMRP is enabled or disabled.
GMRP registration	Status of the administrative control of an outbound port (normal, fixed, forbidden).
GMRP forward/all	Status of whether the Forward All feature is enabled or disabled.
GVRP status	Status of whether GVRP is enabled or disabled.

Table 2-74 show port channel Command Outputs Fields (continued)

Field	Description
GVRP registration	Status of the administrative control of an outbound port (normal, fixed, forbidden).
Qos-Tx	Transmit drop threshold.
Qos-Rx	Receive drop threshold.
Qos-Trust	Status of whether the port is trusted or untrusted.
Qos-DefCos	CoS value.
Qos Port-based	Status of whether the port is port-based QoS or not.
ACL name	Name of the ACL.
Policy Source	Type of policy source.
COPS Admin Roles	COPS admin role designation.
Dot1q tunnel mode	Status of the dot1q tunnel mode.
Jumbo	Status of the jumbo feature.
Auxiliaryvlan	Number of the auxiliary VLAN.
Protocol	Protocol associated with the port.

Related Commands

set port channel
show channel
show channel group

show port cops

To display COPS information on all or individual ports, use the **show port cops** command.

show port cops [*mod*[*/port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value or a *port* value, information is shown for all ports on all modules.

For a few minutes after a switchover from the active to the standby supervisor engine, note that if you enter the **show port cops** command, the output may be incorrect. If this is the case, the following warning displays:

```
COPS High Availability Switch Over in progress, hardware may be
programmed differently than as suggested by the output of these
commands.
```

Examples

This example shows how to display COPS information for all ports:

```
Console> show port cops
Port    Admin Roles                       Oper Roles
------  --------------------------------  -------------------------
 1/1    backbone_port                     backbone_port
        branch_office_port                -
        access_port                       -
 1/2    -                                 -
 3/1    -                                 -
 3/2    backbone_port                     backbone_port
 3/3    backbone_port                     backbone_port
 3/4    access_port                       access_port
 3/5    access_port                       branch_office_port
        backbone_port                     -
        branch_office_port                -
        net_port                          -
 3/6    access_port                       access_port
 3/7    -                                 -
 3/8    -                                 -
Console>
```

This example shows how to display COPS information for a specific port:

```
Console> show port cops 1/1
Port    Admin Roles                        Oper Roles
------  ------------------------------     -------------------------
 1/1    backbone_port                      backbone_port
        branch_office_port                 -
        access_port                        -
 1/2    -                                  -
Console>
```

Table 2-75 describes the fields displayed in the **show port cops** command output.

Table 2-75 show port cops Command Output Fields

Field	Description
Port	Module and port number.
Admin Roles	Administration role.
Oper Roles	Operating role.

Related Commands

clear port cops
set port cops

show port counters

To show all the counters for a port, use the **show port counters** command.

show port counters [*mod*[*/port*]]

show port counters vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module for which to show port counter information.
port	(Optional) Number of the port on the module for which to show port counter information.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown.

If you do not specify a *port* value, all the ports on the module are shown.

Examples

This example shows counters for all ports:

```
Console> show port counters
Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 1/1           0          0          0          0         0
 1/2           0          0          0          0         0
 4/1           0          0          0          0         0
 4/2           0          0          0          0         0
 4/3           0          0          0          0         0
 4/4           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 1/1          12          0          0          0         0         0         -
 1/2           0          0          0          0         0         0         0
 4/1           0          0          0          0         0         0         0
 4/2           0          0          0          0         0         0         0
 4/3           0          0          0          0         0         0         0
 4/4           0          0          0          0         0         0         0

Last-Time-Cleared
```

```
--------------------------
Wed Jan 11 2000, 14:58:19
```

Table 2-76 describes the possible fields (depending on the port type queried) in the **show port counters** command output.

Table 2-76 show port counters Command Output Fields

Field	Description
Port	Module and port number.
Align-Err	Number of frames with alignment errors (frames that do not end with an even number of octets and have a bad CRC) received on the port.
FCS-Err	Number of frame check sequence errors that occurred on the port.
Xmit-Err	Number of transmit errors that occurred on the port (indicating that the internal transmit buffer is full).
Rcv-Err	Number of receive errors that occurred on the port (indicating that the internal receive buffer is full).
UnderSize	Number of received frames less than 64 octets long (but are otherwise well-formed).
Single-Coll	Number of times one collision occurred before the port successfully transmitted a frame to the media.
Multi-Coll	Number of times multiple collisions occurred before the port successfully transmitted a frame to the media.
Late-Coll	Number of late collisions (collisions outside the collision domain).
Excess-Col	Number of excessive collisions that occurred on the port (indicating that a frame encountered 16 collisions and was discarded).
Carri-Sen	Number of times the port sensed a carrier (to determine whether the cable is currently being used).
Runts	Number of received runt frames (frames that are smaller than the minimum IEEE 802.3 frame size) on the port.
Giants	Number of received giant frames (frames that exceed the maximum IEEE 802.3 frame size) on the port.
Last-Time-Cleared	Last time the port counters were cleared.

Related Commands

clear counters
show port

show port critical

To display the status of the Inaccessible Authentication Bypass (IAB) feature for 802.1X, LPIP, MAC authentication bypass, or Web Authentication on a specified port, use the **show port critical** command.

show port critical [*mod*[*/port*]]

Syntax Description

mod[*/port*]	(Optional) Number of the module and optionally, the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not enter a *mod/port* argument, the IAB feature status on all ports on all modules is displayed. If you enter only a *mod* argument, the IAB feature status for all ports on the specified module is displayed.

Examples

```
Console> show port critical 8/1
Port  Critical State Features in Critical State
----- -------------- ---------------------------
  8/1 enabled        dot1x, eou
Console>
```

Related Commands

set port critical

show port debounce

To display whether the port debounce timers are enabled or disabled, use the **show port debounce** command.

show port debounce [*mod* | *mod/port*]

Syntax Description

mod	(Optional) Number of the module.
mod/port	(Optional) Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a port, all ports are displayed.

Examples

This example shows how to display the debounce link timer for a specific port on a specific module:

```
Console> show port debounce 2/1
Port Debounce link timer
----- ---------------
 2/1   disable
Console>
```

Related Commands

set port debounce

show port description

To display a desciption for a port, use the **show port description** command.

show port desciption [*mod*[*/port*]]

show port description vlan [*vlan* | *vlan_name*]

Syntax Description

mod[*/port*]	(Optional) Number of the module and optionally, the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **set port description** command adds another 43 characters to the existing limit of 21 characters that can be set when you enter the **set port name** command. This command displays the description.

If you do not specify a module number or a port number, all port descriptions are displayed. If you only specify a module number, descriptions for all ports on that module are displayed.

Examples

This example shows how to display a description for a specified port:

```
Console> show port description 7/1
Port  Description
----- ---------------------------------------------------------------
 7/1  sarahtom 172.30.8.35 00-0a-5e-44-8b-78 2/2
Console>
```

Related Commands

set port description
set port name

show port dhcp-snooping

To display the port specific DHCP snooping configuration, use the **show port dhcp-snooping** command.

show port dhcp-snooping [*mod*[*/ports*]]

Syntax Description

mod[*/ports*]	(Optional) Number of the module and optionally, the port or ports on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not enter a module number or a module and port numbers, the DHCP snooping configuration is displayed for all ports on the switch.

Examples

This example shows how to display the DHCP snooping configuration on all ports:

```
Console> show port dhcp-snooping
Port     Trust        Source-Guard    Source-Guarded IP Addresses        Binding
 Limit
-----    -----------  ------------    ---------------------------        -------
-----------
 5/1     untrusted    disabled                                           32
 5/2     untrusted    disabled                                           32
 5/3     untrusted    disabled                                           32
 5/4     untrusted    disabled                                           32
 5/5     untrusted    disabled                                           32
 5/6     untrusted    disabled                                           32
 5/7     untrusted    disabled                                           32
 5/8     untrusted    disabled                                           32
 5/9     untrusted    disabled                                           32
 5/10    untrusted    disabled                                           32
 5/11    untrusted    disabled                                           32
 5/12    untrusted    disabled                                           32
 5/13    untrusted    disabled                                           32
 5/14    untrusted    disabled                                           32
 5/15    untrusted    disabled                                           32
 5/16    untrusted    disabled                                           32
***Truncated output***
Console>
```

This example shows how to display the DHCP snooping configuration for module 4, ports 1-4 on a switch with a PFC3 or later:

```
Console> (enable) show port dhcp-snooping 4/1-4
Port     Trust     Source-Guard    Source-Guarded IP Addresses    Binding
----     ------    ------------    ---------------------------    -------
 4/1   untrusted      disabled                                    32
 4/2   untrusted      disabled      enabled                       48
 4/3   untrusted      disabled                                    32
 4/4   untrusted      disabled                                    32
Console> (enable)
```

This example shows how to display the DHCP snooping configuration on module 1 ports:

```
Console> show port dhcp-snooping 1
Port     Trust     Source-Guard    Source-Guarded IP Addresses
----     ------    ------------    ---------------------------
 1/1     trusted      enabled
 1/2   untrusted      disabled
 1/3   untrusted      disabled
 1/4   untrusted      disabled
 1/5   untrusted      disabled
 1/6   untrusted      disabled
 1/7   untrusted      disabled
 1/8   untrusted      disabled
Console>
```

Related Commands

clear dhcp-snooping bindings
set port dhcp-snooping
show dhcp-snooping config

8.6 EFT Copy

show port dot1q-all-tagged

To show the status of the dot1q-all-tagged feature on all or specific ports, use the **show port dot1q-all-tagged** command.

show port dot1q-all-tagged [*mod*[*/port*]]

show port dot1q-all-tagged vlan [*vlan* | *vlan_name*]

Syntax Description

mod[*/port*]	(Optional) Number of the module and optionally, the number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a module or port number, the status of the dot1q-all-tagged feature is displayed for all ports on all modules.

Examples

This example shows how to display the status of the feature on a specific port:

```
Console> (enable) show port dot1q-all-tagged 1/1
Dot1q-all-tagged feature globally enabled.
Port Dot1q-all-tagged mode
---- -------------------------------
1/1 disable
Console> (enable)
```

This example shows how to display the status of the feature on all ports on a specific module:

```
Console> (enable) show port dot1q-all-tagged 1
Dot1q-All-Tagged feature globally disabled.
Port Dot1q-all-tagged mode
----- -----------------------------
1/1 disable
1/2 disable
Console> (enable)
```

Related Commands

set dot1q-all-tagged
set port dot1q-all-tagged
show dot1q-all-tagged

show port dot1q-ethertype

To show the status of the 802.1q Ethertype field on all or specific ports, use the **show port dot1q-ethertype** command.

show port dot1q-ethertype [*mod*[*/port*]]

show port dot1q-ethertype vlan [*vlan* | *vlan_name*]

Syntax Description

mod[*/port*]	(Optional) Number of the module and the number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a module or port number, the Ethertype field is displayed for all ports on all modules.

Examples

This example shows how to display the status of the feature on a specific port:

```
Console> (enable) show port dot1q-ethertype 3/2
Port                Dot1q ethertype value
------              ---------------------
3/2                 1234
Console> (enable)
```

Related Commands

set trunk

show port dot1qtunnel

To display the dot1q tunnel mode status, use the **show port dot1qtunnel** command.

show port dot1qtunnel [*mod*[*/port*]]

show port dot1qtunnel vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the dot1q tunnel mode status for a specific module:

```
Console> show port dot1qtunnel 4
Port   Dot1q tunnel mode
-----  -----------------
 4/1   access
 4/2   access
 4/3   access
 4/4   access
 4/5   trunk
 4/6   trunk
 4/7   trunk
 4/8   disabled
Console>
```

Related Commands

set port dot1qtunnel

show port dot1x

To display all the configurable and current state values associated with the authenticator port access entity (PAE) and backend authenticator and statistics for the different types of Extensible Authentication Protocol (EAP) packets transmitted and received by the authenticator on a specific port, use the **show port dot1x** command. You can also use this command to display which VLANs have been specified for users that have failed 802.1X authentication.

show port dot1x [*mod*[*/port*]]

show port dot1x statistics [*mod*[*/port*]]

show port dot1x *mod/port* **guest-vlan** {*vlan* | **none**}

show port dot1x auth-fail-vlan [*vlan* | **none**]

Syntax Description

mod	Number of the module.
port	Number of the port on the module.
statistics	Displays statistics for different EAP packets transmitted and received by the authenticator on a specific port.
guest-vlan	Displays the active VLAN that functions as an 802.1X guest VLAN.
vlan	Number of the VLAN; valid values are from 1 to 4094.
none	Displays ports that do not have guest VLANs.
auth-fail-vlan	Displays information about ports that have VLANs for users that have failed 802.1X authentication.
none	(Optional) Displays ports that do not have an authentication failure VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Authentication failure VLANs give end users limited network access after they have failed three attempts at 802.1X authentication. To display the information about ports that have these types of VLANs, enter the **show port dot1x auth-fail-vlan** command.

Examples

This example shows how to display all the configurable and current state values associated with the authenticator PAE and backend authenticator on a specific port:

```
Console> show port dot1x 5/10
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 5/10 -                   -          force-authorized    -

Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                           admin   oper
----- ------------- -----------------   ----------------   ---------------
 5/10 SingleAuth    disabled            disabled           Both     -

Port  Posture-Token Critical-Status Termination action Session-timeout
----- ------------- --------------- ------------------ ---------------
 5/10 -             -               -                  -

Port  Session-Timeout-Override Url-Redirect
----- ------------------------ ----------------------------------
 5/10 disabled                 -

Port  Critical
----- --------
 5/10 enabled
Console>
```

This example displays the statistics of different types of EAP packets that are transmitted and received by the authenticator on a specific port:

```
Console> show port dot1x statistics 4/1,4/2
Port    Tx_Req/Id    Tx_Req    Tx_Total    Rx_Start    Rx_Logff     Rx_Resp/Id    Rx_Resp
4/1     1            2         4           2           0            1             0
4/2     3            4         6           0           1            1             0

Port    Rx_Invalid    Rx_Len_Err    Rx_Total    Last_Rx_Frm_Ver    Last_Rx_Frm_Src_Mac
4/1     0             0             3           1                  00-f0-3b-2b-d1-a9
4/2     0             0             3           1                  00-d0-62-95-7b-ff
Console>
```

This example displays information about ports that have VLANs for users that have failed 802.1X authentication:

```
Console> show port dot1x auth-fail-vlan
Auth-Fail-Vlan Status   Mod/Ports
-------------- -------- ------------------
81             active   3/33
none           none     1/1-2,2/1-2,3/1-32,3/34-48
Console>
```

Related Commands

clear dot1x config
set port dot1x
show dot1x

show port eou

To display the Extensible Authentication Protocol over User Datagram Protocol (EoU) configuration on a specified port, use the **show port eou** command.

show port eou [*mod[/port*]]

show port eou [*mod*[*/port*]] **aaa-fail-policy**

Syntax Description

mod/port	(Optional) Number of the module and optionally, the port on the module.
aaa-fail-policy	Displays the AAA fail policy for EoU that is mapped to a port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a module and a port, the EoU configuration is displayed for all EoU-enabled ports.

Examples

This example shows how to display the EoU configuration on a specified port:

```
Console> show port eou 5/10
Port     EOU-State IP Address      MAC Address       Critical
-------- --------- --------------- ----------------- ---------
 5/10    disabled  -               -                 Enabled

Port     FSM State     Auth Type   SQ-Timeout Session Timeout
-------- ------------- ----------- ---------- ---------------
 5/10     -             -           -          -

Port     Posture      URL Redirect
-------- ------------ --------------------
 5/10     -            -

Port     Termination action Session id
-------- ------------------ --------------------------------
 5/10     -                  -

Port     PolicyGroups
-------- ------------------------------------------------------
 5/10     -
Console>
```

This example shows how to display the AAA fail policy for EoU that is mapped to module 5, port 10:

```
Console> show port eou 5/10 aaa-fail-policy
Port  AAA-Fail-Policy
----- ------------------
 5/10  BLDG_E
Console> (enable)
```

Related Commands

clear eou
set eou
set port eou
set security acl ip
show eou

show port errdisable-timeout

To display the configuration and status of the errdisable timeout for a particular port, use the **show port errdisable-timeout** command.

show port errdisable-timeout [*mod*[*/port*]]

Syntax Description

mod[*/port*]	(Optional) Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If the port is disabled and the reason is disabled globally, the No Change value is displayed in the Action on Timeout field regardless of the value in the Port ErrDisableTimeout field. If the port is not in errdisabled state, the No Change value always is displayed in the Action on Timeout field.

Examples

This example shows how to display the errdisable timeout configuration and status for a particular port:

```
Console> show port errdisable-timeout 3/3
Port  Status      ErrDisableReason  Port ErrDisableTimeout  Action on Timeout
----  ----------  ----------------  ----------------------  -----------------
 3/3  errdisable  udld              Disable                 Remain Disabled
Console>
```

This example shows the output for a port in errdisabled state with the timeout flag enabled and with the reason disabled:

```
Console> show port errdisable-timeout 3/3

Port  Status      ErrDisableReason  Port ErrDisableTimeout  Action on Timeout
----  ----------  ----------------  ----------------------  -----------------
 3/3  errdisable  udld              Enable                  No Change
Console>
```

This example shows the output for a port in errdisabled state with the timeout flag enabled and with the reason enabled:

```
Console> show port errdisable-timeout 3/3

Port  Status      ErrDisableReason  Port ErrDisableTimeout  Action on Timeout
----  ----------  ----------------  ----------------------  -----------------
 3/3  errdisable  udld              Enable                  Enabled
Console>
```

This example shows the output for a port in errdisabled state with the timeout flag disabled and the reason disabled:

```
Console> show port errdisable-timeout 3/3

Port  Status      ErrDisableReason  Port ErrDisableTimeout  Action on Timeout
----  ----------  ----------------  ----------------------  -----------------
 3/3  errdisable  udld              Disable                 No Change
Console>
```

This example shows the output for a port in errdisabled state with the timeout flag disabled and the reason enabled:

```
Console> show port errdisable-timeout 3/3

Port  Status      ErrDisableReason  Port ErrDisableTimeout  Action on Timeout
----  ----------  ----------------  ----------------------  -----------------
 3/3  errdisable  udld              Disable                 Remain Disabled
Console>
```

This example shows the output for a port that is not errdisabled state with the timeout flag enabled and with the reason disabled:

```
Console> show port errdisable-timeout 3/3

Port  Status      ErrDisableReason  Port ErrDisableTimeout  Action on Timeout
----  ----------  ----------------  ----------------------  -----------------
 3/3  connected                  -  Enable                  No Change
Console>
```

Related Commands

set errdisable-timeout
set port errdisable-timeout
show errdisable-timeout

show port errordetection

To display information about port error detection, use the **show port errordetection** command.

show port errordetection [*mod*[*/port*]]

show port errordetection vlan [*vlan* | *vlan_name*]

Syntax Description

mod[*/port*]	(Optional) Number of the module and optionally, number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the status of RXCRC and TXCRC error monitoring on port 3/1:

```
Console> show port errordetection 3/1
Port   Rxcrc    Txcrc
-----  -------- --------
 3/1   enabled  disabled
Console>
```

This example shows how to display the status of inerrors, RXCRC, and TXCRC error monitoring for all the ports on module 2:

```
Console> show port errordetection 2
Port   Rxcrc    Txcrc    Inerrors
-----  -------- -------- --------
 2/1   disabled disabled disabled
 2/2   disabled disabled disabled
Console>
```

Related Commands

set errordetection
set port errordetection
show errordetection

show port ethernet-oam

To display the IEEE 802.3ah Operations, Administrations, and Maintenance (OAM) configuration, status, and counters on a port, use the **show port ethernet-oam** command. You can also use the command to display OAM information about a peer entity and the most recent loopback test results on a port.

show port ethernet-oam [*mod*[*/port*]] **neighbor**

show port ethernet-oam [*mod/port*] **remote-loopback**

Syntax Description

mod/port	(Optional) Number of the module and the port on the module.
neighbor	Displays information about a peer OAM entity.
remote-loopback	Displays the most recent remote loopback test result.

Command Default

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a module or a port, the **show port ethernet-oam** command displays the OAM configuration, status, and counters for all OAM-enabled ports.

If you do not specify a port, the **show port ethernet-oam neighbors** command displays all neighbors that are connected to all OAM-enabled ports.

Examples

This example shows how to display OAM-related configuration, status, and counters on all OAM-enabled ports:

```
Console> show port ethernet-oam
$ = local OAM in loopback
* = remote OAM in loopback

Port  State    Mode    LinkMonitor ConfigRev MaxPdu
----- -------- ------- ----------- --------- ------
1/1   enable*  active  enable      11        1518
3/5   enable$  passive enable      38        1518
4/6   disable  active  disable     0         1518

Port  Remote   Link     UniDir Variable
      Loopback Event           retrieval
----- -------- ------- ------- ---------
1/1   disable  enable  disable disable
3/5   enable   enable  enable  disable
4/6   enable   enable  disable disable
```

```
Port  ErrSymbol         Period  ErrSymbol Period    ErrSymbol Period
      Window                      LowThreshold        HighThreshold
     (millions)         Count     Action    Count     Action
----- ----------------- --------- --------- --------- ---------
1/1   625               1         None      10        Warning
3/5   65535             1         Warning   1000      Errordis
4/6   1                 1         Errordis  1         Errordis

Port  Errored Frame      Errored Frame        Errored Frame
      Window              LowThreshold         HighThreshold
      (100 msec)        Count     Action    Count    Action
----- ----------------- --------- --------- --------- ---------
1/1   300               1         None      10        Warning
3/5   65535             1         Warning   1000      Errordis
4/6 1000 1 Errordis 1 Errordis

Port  ErrFrame Period   ErrFrame Period      ErrFrame Period
      Window             LowThreshold        HighThreshold
                         Count    Action    Count     Action
----- ----------------- --------- --------- --------- ---------
1/1   10000             1         None      10        Warning
3/5   4294967000        1         Warning   1000      Errordis
4/6   1                 1         Errordis  1         Errordis

Port LinkFaultAction    CriticalEventAction
----- ----------------- -------------------
1/1  Errordisable       Warning
3/5  None               None
4/6  Errordisable       None

Port  InfoPduRx         InfoPduTx
----- ----------------- ------------------
1/1   33333             22222
3/5   22222             33333
4/6   0                 0
Console>
```

This example shows how to display the information of peer OAM entities:

```
Console> show port ethernet-oam neighbor
Port  MAC Addr          OUI    VendorInfo Mode    ConfigRev MaxPDU
----- ----------------- ------ ---------- ------- --------- ------
1/1   00-50-54-6c-b5-20 00000C 0000018C   passive 3         1518
3/5   00-0b-fc-fb-4a-10 00000C 0000018D   active  7         1518
Port  Remote   Link    UniDir  Variable
      Loopback Event           retrieval
----- -------- ------- ------- ---------
1/1   disable  enable  disable disable
3/5   enable   enable  enable  disable
Console>
```

This example shows how to display the most recent remote loopback test results on a port:

```
Console> show port ethernet-oam 3/3 remote-loopback
OAM remote loopback summary on port 3/3 (loopback slave):
Port MAC Rx    MAC Drop  OAM Rx     OAM Loopback OAM PDU Rx
---- --------- --------- ---------- ------------ ----------
3/3  999999    500       999444     999444       55
Console>
```

Related Commands	
	clear port ethernet-oam set port ethernet-oam set port ethernet-oam action set port ethernet-oam link-monitor set port ethernet-oam mode set port ethernet-oam remote-loopback

show port flexlink

To display the Flexlink port configuration, use the **show port flexlink** command.

show port flexlink [*mod*[*/port*]]

Syntax Description

mod[*/port*]	(Optional) Number of the module and optionally, the number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a module or a port, only ports that are configured with Flexlink pairings are displayed. If you specify only a module number, all ports are displayed, including those ports that are not configured with Flexlink pairings.

Examples

This example shows how to display all the Flexlink ports that are configured on the switch:

```
Console> show port flexlink
Port   State       Peer port  State
-----  ----------  ---------  ----------
 3/47  linkdown    3/48       active
 3/48  active      3/47       linkdown
Console>
```

This example shows how to display Flexlink information for a specified port:

```
Console> show port flexlink 3/1
Port   State       Peer port  State
-----  ----------  ---------  ----------
 3/1   linkdown    3/2        linkdown
Console>
```

Usage Guidelines

clear port flexlink
set port flexlink

show port flowcontrol

To display per-port status information and statistics related to flow control, use the **show port flowcontrol** command.

show port flowcontrol [*mod*[/*port*]]

show port flowcontrol vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown.

If you do not specify a *port* value, all the ports on the module are shown.

Examples

This example shows how to display the flow-control port status and statistics for module 6:

```
Console> show port flowcontrol 6
Port   Send FlowControl   Receive FlowControl   RxPause    TxPause
       admin    oper      admin    oper
-----  -------- --------  -------- --------     ---------- ----------
 6/1   desired  off       off      off          0          0
 6/2   desired  off       off      off          0          0
 6/3   desired  off       off      off          0          0
 6/4   desired  off       off      off          0          0
 6/5   desired  off       off      off          0          0
 6/6   desired  off       off      off          0          0
 6/7   desired  off       off      off          0          0
 6/8   desired  off       off      off          0          0
Console>
```

Table 2-77 describes the fields in the **show port flowcontrol** command output.

Table 2-77 show port flowcontrol Command Output Fields

Field	Description
Port	Module and port number.
Send Flowcontrol Admin	Flow-control administration. Possible settings: on indicates the local port sends flow control to the far end; off indicates the local port does not send flow control to the far end; desired indicates the local end sends flow control to the far end if the far end supports it.
Send Flowcontrol Oper	Flow-control operation. Possible settings: on indicates flow control is operational; off indicates flow control is not operational; disagree indicates the two ports could not agree on a link protocol.
Receive Flowcntl Admin	Flow-control administration. Possible settings: on indicates the local port requires the far end to send flow control; off indicates the local port does not allow the far end to send flow control; desired indicates the local end allows the far end to send flow control.
Receive Flowcntl Oper	Flow-control operation. Possible settings: on indicates flow control is operational; off indicates flow control is not operational; disagree indicates the two ports could not agree on a link protocol.
RxPause	Number of Pause frames received.
TxPause	Number of Pause frames transmitted.

Related Commands

set port flowcontrol

show port inlinepower

To display the port power administration and operational status, use the **show port inlinepower** command.

show port inlinepower [*mod*[/*port*]] [**detail**]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
detail	(Optional) Displays detailed inline power information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

An inline power-capable device can still be detected even if the inline power mode is set to off.

The Operational (Oper) status field descriptions are as follows:

- on—Power is being supplied by the port.
- off—Power is not being supplied by the port.
- denied—The system does not have enough available power for the port; power is not being supplied by the port.
- faulty—The port is unable to provide power to the connected device.

Examples

This example shows how to display the inline power for multiple ports on a specific module:

```
Console> show port inlinepower 6/1
Configured Default Inline Power allocation per port: 15.400 Watts (0.36
Amps @42V)
Total inline power drawn by module 4:  33.934 Watts ( 0.807 Amps @42V)

Port  InlinePowered  PowerAllocated   Device     IEEE class
                    From PS   To PD
      Admin  Oper   mWatts    mWatts
----- ------ ------ -------   ------- ---------- ----------
 6/1  auto   on     7079      6300    cisco      none

Port  MaximumPower  ActualConsumption
      mWatts        mWatts
----- ------------  -----------------
 6/1  15400         6300

Console>
```

This example shows how to display the detailed power status for modules and individual ports:

```
Console> show port inlinepower 4/1 detail
Configured Default Inline Power allocation per port: 15.400 Watts (0.36
Amps @42V)
Total inline power drawn by module 4:  33.934 Watts ( 0.807 Amps @42V)

Port      InlinePowered      PowerAllocated  Device     IEEE class DiscoverMode
                             From PS To PD
      Admin  Oper   Detected mWatts  mWatts
----- ------ ------ -------- ------- ------- ---------- ---------- ------------
 4/1  auto   on     yes      7079    6300    cisco      none        cisco

Port  MaximumPower  ActualConsumption  absentCounter  OverCurrent
      mWatts        mWatts
----- ------------  -----------------  -------------  -----------
 4/1  15400         6300               0              0
Console>
```

Table 2-78 describes the possible fields (depending on the type of port queried) and the values in the **show port inline power** command output.

Table 2-78 show port inlinepower Command Output Fields

Field	Description
Configured Default Inline Power allocation per port	Number of watts configured as the default for each port on the module. This value is set with the **set inlinepower defaultallocation** command.
Total inline power drawn by module	Number of watts drawn by the module.
Port	Module number and port number.
Admin	Administrative status for the port.
Oper	Operation status of the port. The status field descriptions are the following: • on—Power is being supplied by the port. • off—Power is not being supplied by the port. • denied—System does not have enough available power for the port, and power is not supplied by the port. • faulty—The port is unable to provide power to the connected device.
Detected	Status of whether or not an IP phone with inline power requirements has been detected on the port (yes or no).
Power Allocated from PS mWatts	Number of milliwatts available from the power supply for the port.
Power Allocated to PD mWatts	Number of milliwatts allocated to the powered device on the port. This number may be less than the power allocated from the power supply if the module and daughter card has an efficiency factor.
Device	Type of IP phone connected to the port (Cisco, Cisco/IEEE, IEEE, or n/a).
IEEE class	IEEE class for the IP phone (Class 0, Class 1, Class 2, Class 3, Class 4, or none for a Cisco device).
Discover Mode	Discovery method used to detect the IP phone (Cisco, IEEE, n/a).

Table 2-78 show port inlinepower Command Output Fields (continued)

Field	Description *(continued)*
Port	Module number and port number.
Max Power mWatts	Maximum power (milliwatts) associated with the port.
Actual Consumption mWatts	Actual power (milliwatts) the port uses.

Related Commands

set inlinepower
set port inlinepower
show environment

show port jumbo

To display the jumbo frame settings for all ports with the feature enabled, use the **show port jumbo** command.

show port jumbo

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the jumbo frame settings for ports with the feature enabled:

```
Console> show port jumbo
Jumbo frames MTU size is 9216 bytes.
Jumbo frames enabled on port(s) 6/1-2,7/1-8.
Console>
```

This example shows the display if the jumbo frame feature could not be enabled on some ports at system startup:

```
Console> show port jumbo
Jumbo frames MTU size is 9216 bytes.
Jumbo frames enabled on port(s) 6/1-2.
Jumbo frames are in an inconsistent state on port(s) 7/1-8
Console>
```

Related Commands

set port jumbo

show port l2protocol-tunnel

To display Layer 2 protocol tunneling information on a port or range of ports, use the **show port l2protocol-tunnel** command.

show port l2protocol-tunnel [*mod*[*/port*]]

show port l2protocol-tunnel vlan [*vlan* | *vlan_name*]

Syntax Description

mod[*/port*]	(Optional) Number of the module and the number of the port or range of ports on the module. See the "Usage Guidelines" section for more information.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a port or range or ports, Layer 2 protocol tunneling information is displayed for all tunneling ports.

Examples

This example shows how to display Layer 2 protocol tunneling information for a range of ports:

```
Console> show port l2protocol-tunnel 7/1-2
Port                 Tunnel Protocol(s)     Drop Threshold Shutdown Threshold
-------------------- ---------------------- -------------- ------------------
 7/1                 None                                0                  0
 7/2                 None                                0                  0

Port                 CDP       CDP       STP       STP       VTP       VTP
                     Drop      Shutdown  Drop      Shutdown  Drop      Shutdown
                     Threshold Threshold Threshold Threshold Threshold Threshol
-------------------- --------- --------- --------- --------- --------- --------
 7/1                      1000      1200         0         0         0
 7/2                         0         0         0         0         0

Port                 EOAM      EOAM
                     Drop      Shutdown
                     Threshold Threshold
-------------------- --------- ---------
 7/1                         0         0
 7/2                         0         0
```

Related Commands

clear l2protocol-tunnel cos
clear l2protocol-tunnel statistics
set l2protocol-tunnel cos
set port l2protocol-tunnel
show l2protocol-tunnel statistics

show port lacp-channel

To display information about LACP channels by port or module number, use the **show port lacp-channel** command.

show port lacp-channel [*mod*[/*port*]] [**statistics**]

show port lacp-channel [*mod*[/*port*]] **info** [*type*]

Syntax Description

mod[/*port*]	(Optional) Number of the module and the port number on the module.
statistics	(Optional) Displays the LACP channel statistics.
info	Displays detailed LACP channel information.
type	(Optional) Displays feature-related parameters; valid values are **auxiliaryvlan**, **cops**, **dot1qtunnel**, **gmrp**, **gvrp**, **jumbo**, **protocol**, **qos**, **rsvp**, **spantree**, **trunk**.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not enter a module or a port number, information about all modules is displayed.

If you enter the module number only, information about all ports on the module is displayed.

For differences between PAgP and LACP, refer to the “Guidelines for Port Configuration” section of the “Configuring EtherChannel” chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example shows how to display LACP channel information for all system modules:

```
Console> show port lacp-channel
Port  Channel    Admin Ch    Partner Oper                         Partner
      Mode        Key  Id    Sys ID                               Port
----- --------- ----- ----- ----------------------------------- -----
 2/1  active     143   768   1276,45-12-24-AC-78-90              5/1
 2/2  active     143   768   1276,45-12-24-AC-78-90              5/2
----- --------- ----- ----- ----------------------------------- -----
 4/3  passive    151   769   13459,89-BC-24-56-78-90             1/1
 4/4  passive    151   769   13459,89-BC-24-56-78-90             1/2
----- --------- ----- ----- ----------------------------------- -----
 4/7  passive    152   770   8000,AC-12-24-56-78-90              4/3
 4/8  passive    152   770   8000,AC-12-24-56-78-90              4/4
----- --------- ----- ----- ----------------------------------- -----
Console>
```

This example shows how to display LACP channel information for all ports on module 4:

```
Console> show port lacp-channel 4
Port  Channel   Admin Ch    Partner Oper                        Partner
      Mode       Key  Id    Sys ID                              Port
----- --------- ----- ----- ----------------------------------- -----
 4/1  active    69    0     0,00-00-00-00-00-00                 3/1
 4/2  active    69    0     0,00-00-00-00-00-00                 4/5
 4/3  passive   151   769   13459,89-BC-24-56-78-90             1/1
 4/4  passive   151   769   13459,89-BC-24-56-78-90             1/2
 4/5  active    70    0     0,00-00-00-00-00-00                 7/3
 4/6  active    70    0     0,00-00-00-00-00-00                 7/4
 4/7  passive   152   770   8000,AC-12-24-56-78-90              4/3
 4/8  passive   152   770   8000,AC-12-24-56-78-90              4/4
Console>
```

This example shows how to display LACP channel information for port 7 on module 4:

```
Console> show port lacp-channel 4/7
Port  Channel   Admin Ch    Partner Oper                        Partner
      Mode       Key  Id    Sys ID                              Port
----- --------- ----- ----- ----------------------------------- -----
 4/7  passive   152   770   8000,AC-12-24-56-78-90              4/3
 4/8  passive   152   770   8000,AC-12-24-56-78-90              4/4
Console>
```

This example shows how to display detailed LACP channel information for port 7 on module 4:

```
Console> show port lacp-channel 4/7 info
I = Isolated Port.  C = Channeling Port.  N = Not Connected.
H = Hot Stand-by Port.  S = Suspended Port.

Port  LACP Port Port  Speed Duplex Vlan Trunk status Port  STP Port PortSecurity/
      Priority  Status                               Cost  Priority Dynamic port
----- --------- ------ ----- ------ ---- ------------ ----- -------- -------------
 4/7  130       C      1000  full   1    not-trunking     4       32
 4/8  131       C      1000  full   1    not-trunking     4       32

Port  Admin Channel_id ifIndex Partner Oper            Partner    Partner  Partner
       Key                     Sys ID                  Port prior port     Oper Key
----- ----- ---------- ------- ----------------------- ---------- -------- ----------
 4/7  152   770        31      8000,AC-12-24-56-78-90  248         4/3      15678
 4/8  152   770        31      8000,AC-12-24-56-78-90  249         4/4      15768
Console>
```

This example shows how to display LACP channel statistics for all ports on module 4:

```
Console> show port lacp-channel 4 statistics
Port  Admin    LACP Pkts  LACP Pkts Marker Pkts Marker Pkts LACP Pkts
       Key    Transmitted Received  Transmitted   Received    Errors
----- ------- ----------- --------- ----------- ----------- ---------
 4/1       69         20         0         0         0         0
 4/2       69        105        60         0         0         0
 4/3      151          0         0         0        10         0
 4/4      151          0         5         0         0         0
 4/5       70          0         0         0         0         0
 4/6       70         42         0         0         2         0
 4/7      152          0        92         0         0         0
 4/8      152          0         0         0         0         0
Console>
```

This example shows how to display LACP channel statistics for port 7 on module 4:

```
Console> show port lacp-channel 4/7 statistics
Port   Admin    LACP Pkts   LACP Pkts Marker Pkts Marker Pkts LACP Pkts
        Key    Transmitted Received  Transmitted   Received     Errors
----- ------- ----------- --------- ----------- ----------- ---------
 4/7      152            0        92          0          0          0
 4/8      152            0         0          0          0          0
Console>
```

Related Commands

clear lacp-channel statistics
set channelprotocol
set lacp-channel system-priority
set port lacp-channel
set spantree channelcost
set spantree channelvlancost
show lacp-channel

show port mac

To display port MAC counter information, use the **show port mac** command.

show port mac [*mod*[**/***port*]]

show port mac vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display port MAC counter information for a specific module:

```
Console> show port mac 1

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 1/1                        0                    0                    0
 1/2                        0                    0                    0
 1/3                        0                    0                    0
 1/4                        0                    0                    0

Port     Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
 1/1                        0                    0                    0
 1/2                        0                    0                    0
 1/3                        0                    0                    0
 1/4                        0                    0                    0

Port     Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------
 1/1                        0                    0
 1/2                        0                    0
 1/3                        0                    0
 1/4                        0                    0

MAC      Dely-Exced MTU-Exced  In-Discard Lrn-Discrd In-Lost    Out-Lost
-------- ---------- ---------- ---------- ---------- ---------- ----------
 1/1              0          0          0          0          0          0
 1/2              0          0          0          0          0          0
 1/3              0          0          0          0          0          0
 1/4              0          0          0          0          0          0

Last-Time-Cleared
--------------------------
Fri Sep 1 2000, 20:03:06
Console>
```

Table 2-79 describes the possible fields in the **show port mac** command output.

Table 2-79 show port mac Command Output Fields

Field	Description
Rcv-Unicast	Number of unicast frames received on the port.
Rcv-Multicast	Number of multicast frames received on the port.
Rcv-Broadcast	Number of broadcast frames received on the port.
Xmit-Unicast	Number of unicast frames transmitted by the port.
Xmit-Multicast	Number of multicast frames transmitted by the port.
Xmit-Broadcast	Number of broadcast frames transmitted by the port.
Rcv-Octet	Number of octet frames received on the port.
Xmit-Octet	Number of octet frames transmitted on the port.
Dely-Exced	Number of transmit frames aborted due to excessive deferral.
MTU-Exced	Number of frames for which the MTU size was exceeded.
In-Discard	Number of incoming frames that were discarded because the frame did not need to be switched.
Out-Discard	Number of outbound packets chosen to be discarded even though no errors had been detected to prevent their being transmitted.
In-Lost	Number of incoming frames.
Out-Lost	Number of outbound packets.

Related Commands

clear counters

show port mac-address

To display the MAC address associated with a physical port or ports, use the **show port mac-address** command.

show port mac-address [*mod*[/*port*]]

Syntax Description

mod[/*port*]	(Optional) Number of the module and optionally, the number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a module number, the MAC addresses for all ports on all modules are shown. If you specify a module number but no port number, the MAC addresses for all ports on the specified module are shown.

Examples

This example shows how to display the MAC address for port 1 on module 2:

```
Console> show port mac-address 2/1
Port  Mac address
----- ----------------------
 2/1  00-50-3e-7e-71-3c
Console>
```

This example shows how to display the MAC addresses for all ports on module 2:

```
Console> show port mac-address 2
Port  Mac address
----- ----------------------
 2/1  00-50-3e-7e-71-3c
 2/2  00-50-3e-7e-71-3d
Console>
```

This example shows how to display the MAC addresses for all ports on all modules:

```
Console> show port mac-address
Port  Mac address
----- ----------------------
 2/1  00-50-3e-7e-71-3c
 2/2  00-50-3e-7e-71-3d
```

```
Port  Mac address
----- ----------------------
 5/1  00-d0-d3-33-80-9c
 5/2  00-d0-d3-33-80-9d
.
.
.
 5/48 00-d0-d3-33-80-cb

Port  Mac address
----- ----------------------
 7/1  00-50-54-6c-94-9c
 7/2  00-50-54-6c-94-9d
 7/3  00-50-54-6c-94-9e
 7/4  00-50-54-6c-94-9f
 7/5  00-50-54-6c-94-a0
 7/6  00-50-54-6c-94-a1
 7/7  00-50-54-6c-94-a2
 7/8  00-50-54-6c-94-a3
Console>
```

show port mac-auth-bypass

To display information about the MAC authentication bypass feature on a port, use the **show port mac-auth-bypass** command.

show port mac-auth-bypass [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display MAC address authentication bypass information for module 10, port 5:

```
Console> show port mac-auth-bypass 5/10
Port  Mac-Auth-Bypass State MAC Address       Auth-State         Vlan
----- --------------------- ----------------- -----------------  -----
 5/10 Disabled              -                 -                  1

Port  Termination action Session Timeout Shutdown/Time-Left
----- ------------------ --------------- ------------------
 5/10 -                  3600            NO       -

Port  PolicyGroups
----- -----------------------------------------------------
 5/10  -

Port  Critical
----- -----------------------------------------------------
 5/10 -
Console>
```

Related Commands

set mac-auth-bypass
set port critical
set port mac-auth-bypass
show mac-auth-bypass
show port mac-auth-bypass

show port negotiation

To display the link negotiation protocol setting for the specified port, use the **show port negotiation** command.

show port negotiation [*mod*[/*port*]]

show port negotiation vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is not supported on the 16-Port Gigabit Ethernet Switching Module (WS-X6316-GE-TX) and on the 16-Port 10/100/1000BASE-T Switching Module (WS-X6516-GE-TX).

Examples

This example shows how to display the link negotiation protocol settings for all ports on module 4:

```
Console> show port negotiation 4
Port   Link Negotiation  Link Negotiation
         admin                     oper
--  -----------   ------- ----------------
 4/1   enabled                  enabled
 4/2   enabled                  enabled
 4/3   enabled                  enabled
 4/4   enabled                  enabled
 4/5   enabled                  enabled
 4/6   enabled                  enabled
 4/7   enabled                  enabled
Console>
```

Related Commands

set port negotiation
show port flowcontrol

show port prbs

To display the ports that are running the Pseudo Random Binary Sequence (PRBS) test and to display the counter values for ports on which the test has run, use the **show port prbs** command.

show port prbs [*mod*[*/port*]]

show port prbs vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown. If you do not specify a *port* value, all the ports on the module are shown.

The PRBS error counter measures the reliability of the cable. The error counter range is 0 to 255. A value of 0 signifies a perfect link connection. A value of 255 signifies that the port is faulty or not connected or that there is no communication through the link. If the counter does not remain at zero for a predetermined length of time, the link is faulty. For example, for a baud error rate (BER) of 10^-12, the counter should remain at zero for 100 seconds.

Each time you access the PRBS counter by entering the **show port prbs** command, the PRBS error counter value is reset to 0, and the counter begins to accumulate errors again.

Note The PRBS counter is a “read and clear” register: the first reading in a sequence is usually unreliable and serves primarily to purge the counter; successive readings are accurate.

Examples

This example shows how to display PRBS counter values and the ports that are running the PRBS test:

```
Console> show port prbs

Max error counters = 255
Port    PRBS state    PRBS error counters
----    ----------------------------------
6/1     start         30
```

```
7/1      stop         Console>
```

Related Commands

test cable-diagnostics

show port protocol

To view protocol filters configured on the EtherChannel ports, use the **show port protocol** command.

show port protocol [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *port* value, filters configured on all the ports on the module are shown.

Examples

This example shows how to view protocol filters on configured ports:

```
Console> show port protocol
Port     Vlan       IP       IP Hosts IPX      IPX Hosts Group    Group Hosts
-------- ---------- -------- -------- -------- --------- -------- -----------
1/1      1          on       0        on       0         on       0
1/2      1          on       0        on       0         on       0
2/1      1          on       3        auto-on  0         auto-on  0
2/2      1          on       0        on       0         on       0
2/3      1          on       0        on       0         on       0
2/4      1          on       0        on       0         on       0
2/5      1          on       0        on       0         on       0
2/6      1          on       0        on       0         on       0
2/7      1          on       0        on       0         on       0
2/8      1          on       0        on       0         on       0
2/9      1          on       0        on       0         on       0
2/10     1          on       0        on       0         on       0
2/11     1          on       0        on       0         on       0
2/12     1          on       0        on       0         on       0
Console>
```

Related Commands

set port protocol

show port qos

To display QoS-related information, use the **show port qos** command.

show port qos [*mod*[*/port*]]

show port qos vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Note When a switchover occurs, you cannot view the ACLs and policers deployed using COPS-DS until the COPS-DS client on the new active supervisor engine establishes connection to the PDP and downloads the QoS policy. The runtime fields in the output display will be blank until QoS policy is downloaded to the new active supervisor engine.

Examples

This example shows how to display QoS-related information for a specific module and port:

```
Console> show port qos 2/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.

Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------- -------------
2/1      vlan-based     vlan-based          COPS         local

Port  TxPort Type  RxPort Type  Trust Type   Trust Type   Def CoS Def CoS
                                config       runtime      config  runtime
----- ------------ ------------ ------------ ------------ ------- -------
2/1          2q2t         1q4t    untrusted    untrusted       0

Config:
Port  ACL name                         Type
```

```
----- ------------------------------- ----
No ACL is mapped to port 2/1.

Runtime:
Port  ACL name                         Type
----- ------------------------------- ----
No ACL is mapped to port 2/1.
Console>
```

This example shows how to display QoS-related information for a single port on a specific module, which, in this example, is connected to a port on a phone device:

```
Console> (enable) show port qos 3/4
QoS is disabled for the switch.
Configured settings are not used.
QoS policy source for the switch set to local.

Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------- -------------
 3/4               -              -         local         local

Port  TxPort Type  RxPort Type  Trust Type   Trust Type    Def CoS Def CoS
                                config       runtime       config  runtime
----- ------------ ------------ ------------ ------------- ------- -------
 3/4          2q2t         1q4t    untrusted    trust-cos        0       0
Port  Ext-Trust Ext-Cos
----- --------- -------
 3/4  untrusted       0

(*)Trust type set to untrusted.

Config:
Port  ACL name                         Type
----- ------------------------------- ----
No ACL is mapped to port 3/4.

Runtime:
Port  ACL name                         Type
----- ------------------------------- ----
No ACL is mapped to port 3/4.
Console> (enable)
```

This example shows how to display QoS-related information for a single port on a specific module, which, in this example, trusts only Cisco IP phones:

```
Console> (enable) show port qos 4/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.

Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------- -------------
 4/1      port-based     port-based          COPS         local

Port  TxPort Type  RxPort Type  Trust Type   Trust Type    Def CoS Def CoS
                                config       runtime       config  runtime
----- ------------ ------------ ------------ ------------- ------- -------
 4/1        1p3q1t       1p1q0t    trust-cos    trust-cos*        0       0

Port  Ext-Trust Ext-Cos Trust-Device
----- --------- ------- ------------
 4/1  untrusted       0 ciscoIPPhone
```

```
(*)Runtime trust type set to untrusted.

Config:
Port  ACL name                         Type
----- -------------------------------- ----
No ACL is mapped to port 4/1.

Runtime:
Port  ACL name                         Type
----- -------------------------------- ----
No ACL is mapped to port 4/1.
Console> (enable)
```

Related Commands

clear port qos autoqos
clear qos autoqos
set port qos
set port qos cos
set port qos trust
set port qos trust-device

show port rsvp

To display RSVP information on a per-port basis, use the **show port rsvp** command.

show port rsvp [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display RSVP information for a specific port:

```
Console> (enable) show port rsvp 2
Port  DSBM     Managed Configured Elected DSBM DSBM IP Address
      Election Segment Priority   Priority
----- -------- ------- ---------- ------------ ---------------
 2/1   enabled     yes        232          232    171.21.34.25
 2/2  disabled      no        128            -               -
Console> (enable)
```

Related Commands

set port rsvp dsbm-election

show port security

To view port security configuration information and statistics, use the **show port security** command.

show port security [*mod*[*/port*]]

show port security statistics {*mod*[*/port*]}

show port security statistics system

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
statistics	Displays security statistics.
system	Displays system-wide configuration information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display port security configuration information on a specific port that is a secured port:

```
Console> show port security 4/1
* = Configured MAC Address

Port  Security Violation Shutdown-Time Age-Time Maximum-Addrs Trap     IfIndex
----- -------- --------- ------------- -------- ------------- -------- -------
 4/1  enabled  shutdown  120           1440     25            disabled 3

Port Secure-Src-Addrs   Age-Left Last-Src-Addr     Shutdown Shutdown-Time-Left
---- ----------------- -------- ----------------- -------- ------------------
 4/1 00-11-22-33-44-55 4        00-11-22-33-44-55 No       -
     00-10-14-da-77-f1 100
Port  Flooding on Address Limit
----- -------------------------
 4/1                    Enabled
Console>
```

This example shows the display on a port that has experienced a security violation:

```
Console> show port security 4/1
* = Configured MAC Address

Port  Security Violation Shutdown-Time Age-Time Maximum-Addrs Trap     IfIndex
----- -------- --------- ------------- -------- ------------- -------- -------
 4/1  enabled  shutdown  120           600      25            disabled 3
```

```
Port Secure-Src-Addrs  Age-Left Last-Src-Addr     Shutdown Shutdown-Time-Left
---- ----------------- -------- ----------------- -------- ------------------
 4/1 00-11-22-33-44-55 60       00-11-22-33-44-77 Yes      -
     00-10-14-da-77-f1 200
     00-11-22-33-44-66 200

Port  Flooding on Address Limit
----- -------------------------
 4/1                   Enabled
Console>
```

This example shows that port 4/1 has been shut down and that the timeout left is 60 minutes before the port will be reenabled:

```
Console> show port security 4/1
* = Configured MAC Address

Port  Security Violation Shutdown-Time Age-Time Maximum-Addrs Trap     IfIndex
----- -------- --------- ------------- -------- ------------- -------- -------
 4/1  enabled  restrict  120           600      25            disabled 3

Port Secure-Src-Addrs  Age-Left Last-Src-Addr     Shutdown Shutdown-Time-Left
---- ----------------- -------- ----------------- -------- ------------------
 4/1 00-11-22-33-44-55 60       00-11-22-33-44-77 Yes      -
     00-10-14-da-77-ff

Port  Flooding on Address Limit
----- -------------------------
 4/1                   Enabled
Console>
```

This example shows how to display system-wide configuration information:

```
Console> show port security statistics system

Auto-Configure Option Disabled

Module 1:
 Total ports:2
 Total secure ports:0
 Total MAC addresses:2
 Total global address space used (out of 1024):0
 Status:installed
Module 3:
 Total ports:48
 Total secure ports:1
 Total MAC addresses:49
 Total global address space used (out of 1024):1
 Status:installed
Total secure ports in the system:1
Total secure MAC addresses in the system:51
Total global MAC address resource used in the system (out of 1024):1
Console>
```

This example shows how to display security statistical information for a specific module:

```
Console> show port security statistics 2
Port  Total-Addrs Maximum-Addrs
----- ----------- -------------
Module 2:
  Total ports: 1
  Total secure ports: 0
  Total MAC addresses: 0
  Total global address space used (out of 1024): 0
  Status: removed
Console>
```

Related Commands

clear port security
set port security
show config

show port security-acl

To display the port access control list (PACL) mode and the status of a PACL merge operation, use the **show port security-acl** command.

show port security-acl *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **show port security-acl** command displays PACL information for a specific port. The command output displays both configuration and runtime information. Configuration information shows what is stored in the NVRAM; runtime information shows what is programmed in the hardware.

The output also displays the status of the merge operation. The status can be as follows:

- active—There is a PACL configured on the port and it is successfully merged with the VLAN.
- inactive—There is no PACL configured on the port.
- disabled—There is a PACL configured on the port, but the merge was unsuccessful (for any number of reasons).

The **show port security-acl** command also displays the VLAN with which the port is configured to merge.

Examples

This example shows how to display PACL information for port 3/1:

```
Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1           merge          merge      (VLAN=2) disabled



Config:
Port  ACL name                         Type
----- -------------------------------- ----
 3/1  ipacl1                           IP

Runtime:
Port  ACL name                         Type
----- -------------------------------- ----
No ACL is mapped to port 3/1.
```

```
dhcp-snooping:
Port     Trust      Source-Guard    Source-Guarded IP Addresses
----- ----------- ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable)
```

Related Commands

set port security-acl

show port spantree

To view port spanning tree information, use the **show port spantree** command.

show port spantree [*mod*[*/port*]]

show port spantree vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown. If you do not specify a *port* value, all the ports on the module are shown.

Examples

This example shows how to display spanning tree information on a specific module:

```
Console> (enable) show port spantree 5
Port(s)                  Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
5/1                      1    not-connected   2684354   32 disabled 0
5/2                      1    not-connected   2684354   32 disabled 0
5/3                      1    not-connected   2684354   32 disabled 0
5/4                      1    not-connected   2684354   32 disabled 0
5/5                      1    not-connected   2684354   32 disabled 0
5/6                      1    not-connected   2684354   32 disabled 0
5/7                      1    not-connected   2684354   32 disabled 0
5/8                      1    not-connected   2684354   32 disabled 0
5/9                      1    forwarding       268435   32 disabled 0
.
.
.
```

Related Commands

show spantree

show port status

To display port status information, use the **show port status** command.

show port status [*mod*[*/port*]]

show port status vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown. If you do not specify a *port* value, all the ports on the module are shown.

Examples

This example shows how to display port status information for all ports:

```
Console> show port status
Port  Name               Status     Vlan       Duplex Speed  Type
----- ------------------ ---------- ---------- ------ ------ ------------
 1/1                     connected  52          half   100    100BaseTX
 1/2                     notconnect             half   100    100BaseTX
Console>
```

Table 2-80 describes the fields in the **show port status** command output.

Table 2-80 show port status Command Output Fields

Field	Description
Port	Module and port number.
Name	Name (if configured) of the port.
Status	Status of the port (connected, notconnect, connecting, standby, faulty, inactive, shutdown, disabled, or monitor).

Table 2-80 show port status Command Output Fields

Field	Description
Vlan	VLANs to which the port belongs.
Duplex	Duplex setting for the port (auto, full, half).
Speed	Speed setting for the port (auto, 10, 100, 1000).
Type[1]	Port type (100BASE-TX).

[1] These fields will change according to the system configuration.

show port sync-restart-delay

To display a port's synchronization restart delay, use the **show port sync-restart-delay** command.

show port sync-restart-delay *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **set port sync-restart-delay** and **show port sync-restart-delay** commands are available in both binary mode and text configuration mode, but the synchronization delay you specify is only saved in text configuration mode.

Related Commands

clear config
set port sync-restart-delay

show port tdr

To display the results of the Time Domain Reflectometer (TDR) test on a port, use the **show port tdr** command.

show port tdr [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown. If you do not specify a *port* value, all the ports on the module are shown.

The TDR test is supported on these modules: WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548-GE-45AF, WS-X6748-GE-TX, WS-X6148A-GE-TX, WS-X6148-GE-45AF, WS-X6148A-GE-45AF, WS-X6148A-RJ-45, and WS-X6148A-45AF.

Examples

This example shows how to display the TDR test results for port 1 on module 2:

```
Console> show port tdr 2/1
TDR test last run on Mon, March 10 2003 1:35:00

Port  Speed  Local pair  Pair length              Remote pair  Pair status
----  ------ ----------  -----------------------  -----------  ------------
2/1   1000   Pair A      12  +/- 3 meters          Pair A        Terminated
             Pair B      12  +/- 3 meters          Pair B        Terminated
             Pair C      12  +/- 3 meters          Pair C        Terminated
             Pair D      12  +/- 3 meters          Pair D        Terminated
Console>
```

This example shows how to display the TDR test results for all ports on module 5:

```
Console> show port tdr 5
Port  Speed  Local pair  Pair length              Remote pair  Pair status
----  ------ ----------  -----------------------  -----------  ------------
5/1   1000   Pair A      12  +/- 3 meters          Pair A        Terminated
             Pair B      12  +/- 3 meters          Pair B        Terminated
             Pair C      12  +/- 3 meters          Pair C        Terminated
             Pair D      12  +/- 3 meters          Pair D        Terminated
----  ------ ----------  -----------------------  -----------  ------------
```

```
Port  Speed  Local pair  Pair length              Remote pair  Pair status
----  ------ ----------  -----------------------  -----------  ------------
5/2   1000   Pair A      n/a                       Pair A        Terminated
             Pair B      100 +/- 1 meters          Pair B        Shorted
             Pair C      100 +/- 1 meters          Pair C        Shorted
             Pair D      70 +/- 1 meters           Pair D        Open
----  ------ ----------  -----------------------  -----------  ------------
Port  Speed  Local pair  Pair length              Remote pair  Pair status
----  ------ ----------  -----------------------  -----------  ------------
5/3   1000   Pair A      running tdr test          n/a          n/a
             Pair B      running tdr test          n/a          n/a
             Pair C      running tdr test          n/a          n/a
             Pair D      running tdr test          n/a          n/a
Console>
```

Table 2-81 describes the fields in the **show port tdr** command output.

Table 2-81 show port tdr Command Output Fields

Field	Description
Port	Module and port number.
Speed	Port speed.
Local pair	Identifies the local pair of cables.
Pair length	Identifies the distance the transmitted signal went before it was reflected off the cable imperfection.
Remote pair	Identifies the remote pair of cables.
Pair status	Status of the pair: • Terminated—the link is up. • Shorted—a short is detected on the cable. • Open—an opening is detected on the cable. • Not Completed—the test on the port failed. • Not Supported—the test on the port is not supported.

Related Commands

test cable-diagnostics

show port transceiver

To display operating information about Digital Optical Monitoring (DOM), use the **show port transceiver** command.

show port transceiver [**detail** | **threshold-violation** | *mod* | *mod/port*]

Syntax Description

detail	(Optional) Shows detailed information about the port transceiver.
threshold-violations	(Optional) Displays port transceiver threshold violations.
mod	(Optional) Module number, range 1..6, 15-16
mod/port	(Optional) Number of the module and port.

Command Default

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The DOM feature measures the transceiver characteristics such as temperature, voltage, laser bias current, receive optical power and laser transmit power and allows software to monitor them against alarm and threshold values.

If you do not enter any arguments or keywords, ______________________________

Examples

This example shows how to display port transceiver-related information:

```
Console> show port transceiver
Transceiver monitoring is disabled for all ports.
Monitor interval is set to 10 minutes.

If device is externally calibrated, only calibrated values are printed.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).

                                                    Optical       Optical
         Temperature       Voltage    Current       Tx Power      Rx Power
Port     (Celsius)         (Volts)    (mA)          (dBm)         (dBm)
-----   --------------   ---------  --------     ------------  -----------
 3/1     34.6              0.00        29.3          -1.7           -2.1
 3/2     32.9              0.00        30.5          -1.8           -2.3
Console>
```

This example shows how to display detailed information about the port transceiver:

```
Console> (enable) show port transceiver detail
Transceiver monitoring is disabled for all ports.
Monitor interval is set to 10 minutes.
```

```
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.

                             High Alarm      High Warn      Low Warn      Low Alarm
         Temperature         Threshold       Threshold      Threshold     Threshold
Port   (Celsius)             (Celsius)       (Celsius)      (Celsius)     (Celsius)
-----  ------------------  --------------  -------------  -------------  ---------
 3/1    34.5                  70.0              70.0           0.0              0.0
 3/2    32.9                  70.0              70.0           0.0              0.0

                            High Alarm      High Warn      Low Warn        Low Alarm
       Voltage              Threshold       Threshold      Threshold       Threshold
Port   (Volts)              (Volts)         (Volts)        (Volts)         (Volts)
-----  ---------------    ---------------  -------------  -------------  ---------------
 3/1   0.00                  5.24              5.24            5.24             5.24
 3/2   0.00                  5.24              5.24            5.24             5.24
                            High Alarm     High Warn        Low Warn         Low Alarm
         Current            Threshold      Threshold        Threshold        Threshold
Port   (milliamperes)       (mA)           (mA)             (mA)             (mA)
-----  -----------------  --------------  --------------  -------------  --------------
 3/1    29.3                 2.5               2.5               2.5              2.5
 3/2    30.4                 2.5               2.5               2.5              2.5

         Optical              High Alarm     High Warn      Low Warn         Low Alarm
         Transmit Power       Threshold      Threshold      Threshold        Threshold
Port     (dBm)                (dBm)          (dBm)          (dBm)           (dBm)
-----  -------------------  -------------  --------------  -------------  --------------
 3/1    -1.7                   1.0                0.0             -7.2              -8.2
 3/2    -1.8                   1.0                0.0             -7.2              -8.2

         Optical              High Alarm     High Warn       Low Warn        Low Alarm
         Receive Power        Threshold      Threshold       Threshold       Threshold
Port     (dBm)                (dBm)          (dBm)           (dBm)           (dBm)
-----  -----------------   --------------  --------------  -------------  --------------
 3/1    -2.1                  1.0               0.0                -14.1          -16.4
 3/2    -2.3                  1.0               0.0                -14.1          -16.4
```

This example shows how to display information about the port-transceiver threshold violations:

```
Console> show port transceiver 3 threshold-violations
Transceiver monitoring is enabled for all ports.
Monitor interval is set to 5 minutes.

Rx: Receive, Tx: Transmit.
DDDD: days, HH: hours, MM: minutes, SS: seconds

                                      Time since Last Known
         Time in slot                 Threshold Violation            Type(s) of Last Known
Port     (DDDD:HH:MM:SS)              (DDDD:HH:MM:SS)                Threshold Violation(s)
-----  --------------------------  -----------------------------  ---------------------------
 3/1   0000:06:39:07               0000:00:03:57                  Tx bias high alarm
                                                                  5.8 mA >   0.5 mA
 3/2   0000:06:39:07               0000:00:03:56                  Tx bias high alarm
                                                                  6.0 mA >   0.5 mA
Console>
```

This example shows how to display port transceiver-related information about a specific module and port:

```
Console> show port transceiver 3/1
Transceiver monitoring is disabled for all ports.
Monitor interval is set to 10 minutes.

If device is externally calibrated, only calibrated values are printed.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).

                                                  Optical       Optical
         Temperature      Voltage    Current      Tx Power      Rx Power
Port     (Celsius)        (Volts)    (mA)         (dBm)         (dBm)
-----   --------------   ---------   --------    ------------  -----------
 3/1     34.6             0.00        29.3         -1.7           -2.1
Console>
```

Related Commands

set transceiver-monitoring

show port trap

To display port trap status, use the **show port trap** command.

show port trap [*mod*[/*port*]]

show port trap vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown. If you do not specify a *port* value, all the ports on the module are shown.

Examples

This example shows how to display the port trap status for a specific module:

```
Console> show port trap 1

Port   Trap
-----  --------
 1/1   disabled
 1/2   enabled
 1/3   disabled
 1/4   disabled
Console>
```

Related Commands

set port trap

show port trunk

To display port trunk information, use the **show port trunk** command.

show port trunk [*mod*[*/port*]]

show port trunk vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a *mod* value, the ports on all modules are shown. If you do not specify a *port* value, all the ports on the module are shown.

Examples

This example shows how to display trunking information for a specific port:

```
Console> (enable) show port trunk 4/5
* - indicates vtp domain mismatch

Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 4/5      nonegotiate  dot1q          trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 4/5      1-1005

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 4/5      1-3,1003,1005

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 4/5      1005
Console> (enable)
```

Table 2-82 describes the fields in the **show port trunk** command output.

Table 2-82 show port trunk Command Output Fields

Field	Description
Port	Module and port numbers.
Mode	Trunk administrative status of the port (on, off, auto, or desirable).
Encapsulation	Trunking type configured by administration.
Status	Status of whether the port is trunking or nontrunking.
Native VLAN	Number of the native VLAN for the trunk link (for 802.1Q trunks, the VLAN for which untagged traffic can be transmitted and received over the trunk; for ISL trunks, packets are tagged on all VLANs, including the native VLAN).
Vlans allowed on trunk	Range of VLANs allowed to go on the trunk (default is 1 to 1000).
Vlans allowed and active in management domain	Range of active VLANs within the allowed range.
Vlans in spanning tree forwarding state and not pruned	Range of VLANs that actually go on the trunk with Spanning Tree Protocol forwarding state.

Related Commands

set trunk

show port unicast-flood

To display the run-time configuration of the port using unicast flood blocking, use the **show port unicast-flood** command.

show port unicast-flood [*mod/*[*port*]]

Syntax Description

mod/[*port*]	Number of the module and optionally, number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the status of unicast flood blocking on module 2:

```
Console> show port unicast-flood 2
Port   Unicast Flooding
-----  ----------------
 2/1   Enabled
 2/2   Enabled
Console>
```

This example shows how to display the status of unicast flood blocking on module 3, port 40:

```
Console> show port unicast-flood 3/40
Port   Unicast Flooding
-----  ----------------
 3/40  Enabled
Console>
```

Related Commands

set port unicast-flood

show port vlan-mapping

To display the current VLAN mapping configuration on a specified port, use the **show port vlan-mapping** command.

show port vlan-mapping [*mod*[*/port*]]

Syntax Description

mod[*/port*]	(Optional) Number of the module and the port on the module. valid values for the *mod* argument are from 1 to 9, 15, and 16.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a port or a module, all VLAN mapping configurations for all ports are displayed.

Examples

This example shows how to display the VLAN mapping for a specified port:

```
Console> show port vlan-mapping 4/1
Mod/Port Source VLAN Translated VLAN State      Max Allowed (Current) Entries
-------- ----------- --------------- ---------- -----------------------------
 4/1     2           1               Enabled    8   (2)
 4/1     98          99              Enabled    8   (2)
Console>
```

Table 2-83 describes the fields in the **show port vlan mapping** command output.

Table 2-83 show port vlan-mapping Command Output Fields

Field	Description
Mod/Port	Number of the module and the port on the module.
Source VLAN	Number of the source VLAN.
Translated VLAN	Number of the VLAN that is mapped to the source VLAN.
State	Status of whether VLAN mapping is enabled or disabled.
Max Allowed (Current) Entries	Maximum number of per-port VLAN mappings that are supported; current number of entries in parentheses.

Related Commands

clear port vlan-mapping
set port vlan-mapping

show port voice

To display voice port information, use the **show port voice** command.

show port voice [**noalias**]

Syntax Description

noalias	(Optional) Forces the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to display voice port information:

```
Console> show port voice
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 7/1                     connected  100          full     1 T1
 7/2                     notconnect 100          full     1 T1
 7/3                     connected  100          full     1 T1
 7/4                     connected  100          full     1 T1
 7/5                     notconnect 100          full     1 T1

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 7/1     disable 00-e0-b0-ff-31-c0 sjcf-12a-sw1-p7 255.255.254.0
 7/2     disable 00-e0-b0-ff-31-c1 sjcf-12a-sw1-p7 255.255.254.0
 7/3     disable 00-e0-b0-ff-31-c2 sjcf-12a-sw1-p7 255.255.254.0
 7/4     disable 00-e0-b0-ff-31-c3 sjcf-12a-sw1-p7 255.255.254.0
 7/5     disable 00-e0-b0-ff-31-c4 sjcf-12a-sw1-p7 255.255.254.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Server     Gateway
-------- ----------------- --------------- --------------- ---------------
 7/1     gigantic-2.cisc*  -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/2     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/3     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/4     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/5     10.34.1.11*       -               10.34.1.11      10.34.10.1
         10.34.16.10
         10.34.42.11
(*):Primary
```

```
Port     DNS-Server(s)     Domain
-------- ----------------- -------------------------------------------------
 7/1     dns-sj3.cisco.c*  cisco.com
         dns-sj4.cisco.c
 7/2     dns-sj3.cisco.c*  cisco.com
         dns-sj4.cisco.c
 7/3     dns-sj3.cisco.c*  cisco.com
         dns-sj4.cisco.c
 7/4     dns-sj3.cisco.c*  cisco.com
         dns-sj4.cisco.c
 7/5     dns-sj3.cisco.c*  cisco.com
         dns-sj4.cisco.c
(*):Primary

Port     CallManagerState DSP-Type
-------- ---------------- --------
 7/1     registered       C549
 7/2     registered       C549
 7/3     registered       C549
 7/4     registered       C549
 7/5     registered       C549

Port  NoiseRegen NonLinearProcessing
----- ---------- -------------------
 7/1  enabled    enabled
 7/2  enabled    enabled
 7/3  enabled    enabled
 7/4  enabled    enabled
 7/5  enabled    enabled
Console>
```

This example shows how to display voice port information without displaying the IP address in DNS name format:

```
Console> show port voice noalias
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 7/1                     connected  100          full     1 T1
 7/2                     notconnect 100          full     1 T1
 7/3                     connected  100          full     1 T1
 7/4                     connected  100          full     1 T1
 7/5                     notconnect 100          full     1 T1

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 7/1     disable 00-e0-b0-ff-31-c0 10.34.10.11     255.255.254.0
 7/2     disable 00-e0-b0-ff-31-c1 10.34.10.12     255.255.254.0
 7/3     disable 00-e0-b0-ff-31-c2 10.34.10.13     255.255.254.0
 7/4     disable 00-e0-b0-ff-31-c3 10.34.10.14     255.255.254.0
 7/5     disable 00-e0-b0-ff-31-c4 10.34.10.15     255.255.254.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Server     Gateway
-------- ----------------- --------------- --------------- ---------------
 7/1     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/2     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/3     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/4     10.34.16.10*      -               10.34.1.11      10.34.10.1
         10.34.1.11
 7/5     10.34.1.11*       -               10.34.1.11      10.34.10.1
         10.34.16.10
         10.34.42.11
(*):Primary

Port     DNS-Server(s)     Domain
-------- ----------------- -------------------------------------------------
 7/1     171.68.10.70*     cisco.com
         171.68.10.140
 7/2     171.68.10.70*     cisco.com
         171.68.10.140
 7/3     171.68.10.70*     cisco.com
         171.68.10.140
 7/4     171.68.10.70*     cisco.com
         171.68.10.140
 7/5     171.68.10.70*     cisco.com
         171.68.10.140
(*):Primary

Port     CallManagerState DSP-Type
-------- ---------------- --------
 7/1     registered       C549
 7/2     registered       C549
 7/3     registered       C549
 7/4     registered       C549
 7/5     registered       C549

Port  NoiseRegen NonLinearProcessing
----- ---------- -------------------
 7/1  enabled    enabled
 7/2  enabled    enabled
 7/3  enabled    enabled
 7/4  enabled    enabled
```

Related Commands

set port voice interface dhcp
show port voice fdl
show port voice interface

show port voice active

To display active call information on a port, use the **show port voice active** command.

show port voice active [*mod/port*] [**all** | **call** | **conference** | **transcode**] [*ipaddr*]

Syntax Description

mod/port	(Optional) Number of the module and port on the module.
all	(Optional) Displays all calls (regular calls, conference calls, and transcoding calls) in the system.
call	(Optional) Displays call information for the 24-port FXS analog interface and the 8-port T1/E1 PSTN interface modules.
conference	(Optional) Displays call information for the 8-port T1/E1 PSTN interface module configured for conferencing.
transcode	(Optional) Displays call information for the 8-port T1/E1 PSTN interface module configured for transcoding.
ipaddr	(Optional) Remote IP address.

Defaults

The default is all active calls are displayed.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The information displayed when using the **show port voice active** command is not available through the supervisor engine SNMP agent.

The **call** keyword is supported by the 24-port FXS analog interface and the 8-port T1/E1 PSTN interface modules.

The **conference** and **transcode** keywords are supported by the 8-port T1/E1 PSTN interface module.

You can use the optional *mod* or *mod/port* variables to display calls that belong to the specified module or port in detailed format.

There are up to 8 calls per port for the 8-port T1/E1 ISDN PRI services-configured module but only one call per port for the 24-port FXS analog station interface services-configured module.

The *ipaddr* option displays one specific call for the specified IP address. You can also use an IP alias.

This command is not supported by the NAM.

Examples

This example shows how to display all calls (regular calls, conference calls, and transcoding calls) in the system:

```
Console> show port voice active
Port  Type         Total Conference-ID/ Party-ID IP-Address
                         Transcoding-ID
----- ------------ ----- -------------- -------- ---------------
 6/3  transcoding  1     2              12       192.1.1.12
                                        10       10.6.106.101
 8/2  call         1     -              -        123.46.1.100
 8/5  call         1     -              -        123.46.1.101
 8/7  conferencing 1     1              8        192.1.1.5
                                        7        123.45.1.52
                                        9        192.1.1.14
Total: 3
Console> (enable)
```

This example shows how to display regular calls:

```
Console> (enable) show port voice active call
Port  Total IP-Address
----- ----- ---------------
 8/2  1     123.46.1.100
 8/5  1     123.46.1.101
Total: 2 calls
Console> (enable)
```

This example shows the output display for the 8-port T1/E1 PSTN interface module configured for transcoding:

```
Console> (enable) show port voice active transcode
Port  Total Transcoding-ID Party-ID IP-Address
----- ----- -------------- -------- ---------------
 6/3  1     2              12       192.1.1.12
                           10       10.6.106.101
Total: 1 transcoding session
Console> (enable)
```

This example shows the output display for the 8-port T1/E1 PSTN interface module configured for conferencing:

```
Console> (enable) show port voice active conference
Port  Total Conference-ID  Party-ID IP-Address
----- ----- -------------- -------- ---------------
 8/7  1     1              8        192.1.1.5
                           7        123.45.1.52
                           9        192.1.1.14
Total: 1 conferencing session
Console> (enable)
```

This example shows how to display calls for a specified port:

```
Console> show port voice active 3/2
Port 3/2:
Channel #1:
  Remote IP address                         : 165.34.234.111
  Remote UDP port                           : 124
  Call state                                : Ringing
  Codec Type                                : G.711
  Coder Type Rate                           : 35243
  Tx duration                               : 438543 sec
  Voice Tx duration                         : 34534 sec
  ACOM Level Current                        : 123213
  ERL Level                                 : 123 dB
  Fax Transmit Duration                     : 332433
  Hi Water Playout Delay                    : 23004 ms
  Logical If index                          : 4
  Low water playout delay                   : 234 ms
  Receive delay                             : 23423 ms
  Receive bytes                             : 2342342332423
  Receive packets                           : 23423423402384
  Transmit bytes                            : 23472377
  Transmit packets                          : 94540
Channel #2:
  Remote IP address                         : 165.34.234.112
  Remote UDP port                           : 125
  Call state                                : Ringing
  Codec Type                                : G.711
  Coder Type Rate                           : 35243
  Tx duration                               : 438543 sec
  Voice Tx duration                         : 34534 sec
  ACOM Level Current                        : 123213
  ERL Level                                 : 123 dB
  Fax Transmit Duration                     : 332433
  Hi Water Playout Delay                    : 23004 ms
  Logical If index                          : 4
  Low water playout delay                   : 234 ms
  Receive delay                             : 23423 ms
  Receive bytes                             : 2342342332423
  Receive packets                           : 23423423402384
  Transmit bytes                            : 23472377
  Transmit packets                          : 94540
Port  3/7 :
  Conference ID: 1
    Party ID: 8
      Remote IP address                     : 192.1.1.5
      UDP Port                              : 28848
      Codec Type                            : G729 B CS ACELP VAD
      Packet Size (ms)                      : 20
    Party ID: 7
      Remote IP address                     : 123.45.1.52
      UDP Port                              : 28888
      Codec Type                            : G711 ULAW PCM
      Packet Size (ms)                      : 20
    Party ID: 9
      Remote IP address                     : 192.1.1.14
      UDP Port                              : 28898
      Codec Type                            : G711 ULAW PCM
      Packet Size (ms)                      : 20
Total: 2
Console>
```

This example shows the output display for a specified IP address on a 24-port FXS analog interface module or the 8-port T1/E1 PSTN interface module:

```
Console> show port voice active 3/2 171.69.67.91
  Remote IP address                         : 171.69.67.91
  Remote UDP port                           : 125
  Call state                                : Ringing
  Codec Type                                : G.711
  Coder Type Rate                           : 35243
  Tx duration                               : 438543 sec
  Voice Tx duration                         : 34534 sec
  ACOM Level Current                        : 123213
  ERL Level                                 : 123 dB
  Fax Transmit Duration                     : 332433
  Hi Water Playout Delay                    : 23004 ms
  Logical If index                          : 4
  Low water playout delay                   : 234 ms
  Receive delay                             : 23423 ms
  Receive bytes                             : 2342342332423
  Receive packets                           : 23423423402384
  Transmit bytes                            : 23472377
  Transmit packets                          : 94540
Console>
```

Related Commands

set port voice interface dhcp

show port voice fdl

To display the facilities data link (FDL) statistics for the specified ports, use the **show port voice fdl** command.

show port voice fdl [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to display FDL information on an 8-port T1/E1 ISDN PRI services-configured module:

```
Console> (enable) show port voice fdl 7/1-3
Port  ErrorEvents       ErroredSecond     SeverlyErroredSecond
      Last 15’ Last 24h Last 15’ Last 24h Last 15’ Last 24h
----- -------- -------- -------- -------- -------- -----------
 7/1  17       18       19       20       21       22
 7/2  17       18       19       20       21       22
 7/3  17       18       19       20       21       22

Port  FailedSignalState FailedSignalSecond
      Last 15’ Last 24h Last 15’ Last 24h
----- -------- -------- -------- ---------
 7/1  37       38       39       40
 7/2  37       38       39       40
 7/3  37       38       39       40

Port         LES               BES               LCV
      Last 15’ Last 24h Last 15’ Last 24h Last 15’ Last 24h
----- -------- -------- -------- -------- -------- --------
 7/1  41       48       49       50       53       54
 7/2  41       48       49       50       53       54
 7/3  41       48       49       50       53       54
Console> (enable)
```

Table 2-84 describes the possible fields (depending on the port type queried) in the **show port voice fdl** command output.

Table 2-84 show port voice fdl Command Output Fields

Field	Description
ErrorEvents	Count of errored events.
ErroredSecond	Count of errored seconds.
SeverelyErroredSecond	Count of severely errored seconds.
FailedSignalState	Count of failed signal state errors.
FailedSignalSecond	Count of failed signal state.
LES	Line errored seconds detected.
BES	Bursty errored seconds detected.
LCV	Line code violation seconds detected.

Related Commands

show port voice

show port voice interface

To display the port voice interface configuration, use the **show port voice interface** command.

show port voice interface [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to display voice interface information for a specific module:

```
Console> show port voice interface 5
Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 5/1-24  disable 00-10-7b-00-13-ea 10.6.15.158     255.255.255.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Server     Gateway
-------- ----------------- --------------- --------------- ---------------
 5/1-24  10.6.15.155       -               10.6.15.155     -

Port     DNS-Server(s)     Domain
-------- ----------------- -------------------------------------------------
 5/1-24  12.2.2.1*         cisco.cisco.com
         7.7.7.7
(*): Primary
Console>
```

Related Commands

set port voice interface dhcp
show port voice
show port voice active

8.6 EFT Copy

show port vtp

To display the status of VLAN Trunk Protocol (VTP) on a per-port basis, use the **show port vtp** command.

show port vtp [*mod*[/*port*]]

show port vtp vlan [*vlan* | *vlan_name*]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
vlan	Limits output to ports in the specified VLAN.
vlan	(Optional) VLAN number; valid values are from 1 to 4094.
vlan_name	(Optional) VLAN name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

VTP version 3 allows you to enable or disable VTP on a per-port basis. When a port is disabled for VTP, it will not send or accept any VTP packets, regardless of the VTP version.

Examples

This example shows how to display the status of VTP on module 2, port 1:

```
Console> show port vtp 2/1
Port      VTP Status
--------  ----------
 2/1      enabled
Console>
```

This example shows how to display the status of VTP on all ports on all modules:

```
Console> show port vtp
Port      VTP Sta
--------  -------
 2/1      enabled
 2/2      enabled
 3/1      enabled
 3/2      enabled
 3/3      enabled
 3/4      enabled
 3/5      enabled
 3/6      enabled
 3/7      enabled
 3/8      enabled
 3/9      enabled
 3/10     enabled
 3/11     enabled
 3/12     enabled
 3/13     enabled
 3/14     enabled
 3/15     enabled
 3/16     enabled
 3/17     enabled
 3/18     enabled
 3/19     enabled
 3/20     enabled
 3/21     enabled
 3/22     enabled
 3/23     enabled
 3/24     enabled
 3/25     enabled
 3/26     enabled
 3/27     enabled
 3/28     enabled
 3/29     enabled
 3/30     enabled
 3/31     enabled
 3/32     enabled
 3/33     enabled
 3/34     enabled
 3/35     enabled
 3/36     enabled
 3/37     enabled
 3/38     enabled
 3/39     enabled
 3/40     enabled
 3/41     enabled
 3/42     enabled
 3/43     enabled
 3/44     enabled
 3/45     enabled
 3/46     enabled
 3/47     enabled
 3/48     enabled
16/1      enabled
Console>
```

Related Commands

set port vtp
set vtp
show vtp

show port web-auth

To display information about a web-based proxy authentication port, use the **show port web-auth** command.

show port web-auth [*mod*[*/port*]]

show port web-auth [*mod*[*/port*]] **aaa-fail-policy**

Syntax Description

mod[*/port*]	(Optional) Module number and optionally, the port number.
aaa-fail-policy	Displays the AAA fail policy for web-based proxy authentication that is mapped to a port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **show port web-auth** command displays the following information:

- IP address of the host.
- Current state.
- Session-timeout. The time displayed is the configured timeout if it is not supplied by RADIUS.
- Leftover session timeout value.

Examples

This example shows how to display information about web-based proxy authentication on module 5, port 10:

```
CConsole> show port web-auth 5/10

Port  IP-Address      Vlan Web-Auth-State    Critical-Status
----- --------------- ---- ----------------- ---------------
 5/10  -               1    disabled          -

Port  IP-Address      Session-Timeout Session-Timeleft Radius-Rcvd-Timeout
----- --------------- --------------- ---------------- -------------------
 5/10  -               -               -                No

Port  IP-Address      Policy-Groups
----- --------------- -------------
 5/10  -               -
Console>
```

This example shows how to display the AAA fail policy for EoU that is mapped to module 5, port 11:

```
Console> show port web-auth 5/11 aaa-fail-policy
Port  AAA-Fail-Policy
----- ------------------
 5/11  BLDG_F
Console>
```

Related Commands

clear web-auth
set port critical
set port web-auth
set port web-auth initialize
set web-auth
set web-auth login-attempts
set web-auth login-fail-page
set web-auth login-page
set web-auth quiet-timeout
set web-auth session-timeout
show port web-auth
show web-auth summary

show proc

To display CPU, memory allocation, and process utilization information, use the **show proc** command.

show proc [**cpu** | **mem**]

Syntax Description

cpu	(Optional) Specifies CPU information.
mem	(Optional) Specifies memory allocation information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can enter this command only in privileged mode.

If you do not specify **cpu** or **mem**, process information is displayed. The **mem** keyword allows you to display memory allocation information, such as how much each process has allocated and freed.

Examples

This example shows how to display CPU information:

```
Console> (enable) show proc cpu
(W)CPU utilization for five seconds: 1.0%; one minute: 1. 0%; five minutes: 1. %

PID Runtime(ms) Invoked uSecs   5Sec   1Min    5min   TTY Process
0   0           0       0       99.10%  99.0 %  99.0 %  0    idle
1   1           36      1000     0.0 %   0.0 %   0.0 %  0    Flash MIB Updat
2   1342        2846    460000   0.0 %   0.0 %   0.0 %  0    SynDiags
3   730172      4440594 400000   0.0 %   0.0 %   0.0 %  0    SynConfig
4   33752       424120  1000     0.0 %   0.0 %   0.0 %  0    Statuspoll
5   7413        44916   1000     0.0 %   0.0 %   0.0 %  0    SWPoll64bCnt
6   9568        15889836 1000     0.0 %   0.0 %   0.0 %  0    SL_TASK
7   746         636118  105000   0.0 %   0.0 %   0.0 %  0    RedundantTask
Console> (enable)
```

This example shows how to display process utilization information:

```
Console> (enable) show proc
PID Q  T  PC         Runtime(ms) Invoked uSecs  Stacks    TTY Process
0   1  rd 0x80407b10 0           0       0      1640/6144 0   idle
1   65376 st 0x80407d8c 1           36      1000   1188/6144 0   Flash MIB
Upda
2   2  st 0x80407d8c 1342        2846    460000 3160/6144 0   SynDiags
3   1  rd 0x80407d8c 729979      4439406 400000 1672/6144 0   SynConfig
4   2  si 0x80407d8c 33739       424007  1000   1572/6144 0   Statuspoll
5   4  si 0x80407d8c 7413        44916   1000   1888/6144 0   SWPoll64bCnt
6   2  si 0x80407d8c 9565        15885713 1000   1096/6144 0   SL_TASK
7   2  si 0x80407d8c 746         635948  105000 1192/6144 0   RedundantTask
```

```
Memory Pool Utilization
Memory Pool Type 1Min  5Min  10Min
---------------- ----- ----- -----
DRAM               49%   49%   49%
FLASH              82%   82%   82%
NVRAM              49%   49%   49%
MBUF                2%    2%    2%
CLUSTER            12%   12%   12%
MALLOC             15%   15%   15%
Console> (enable)
```

This example shows how to display process information:

```
Console> (enable) show proc mem

Memory Used:  7141936
       Free: 53346800
      Total: 60488736

PID        TTY        Allocated  Freed      Holding    Process
---------- ---------- ---------- ---------- ---------- ---------------
1          -2         2928912    4544       2924368    Kernel and Idle
2          -2         160        0          160        Flash MIB Updat
3          -2         160        0          160        L2L3IntHdlr
4          -2         0          0          0          L2L3PatchRev
5          -2         288        0          288        SynDiags
6          -2         128        0          128        GenMsgHndlr
7          -2         1158560    526480     632080     SynConfig
8          -2         32         0          32         TempMon
9          -2         16         0          16         EM_garbageColle
10         -2         192        0          192        PowerMgmt
11         -2         1136       0          1136       FabricConfig
12         -2         97536      0          97536      SL_TASK
13         -2         18368      5056       13312      RedundantTask
14         -2         2384       0          2384       Status Poll
15         -2         96         0          96         SWPoll64bCnt
16         0          384        0          384        HavailTask
17         -2         10304      0          10304      SyncTask
18         -2         48         0          48         SecurityRx
19         -2         144        0          144        DeviceLinkChk
20         -2         10576      10560      16         Earl
21         -2         2768       2464       304        DTP_Rx
22         -2         280624     151680     128944     EthChnlRx
23         -2         0          0          0          llcSSTPFlood
24         -2         1584       1152       432        EthChnlConfig
25         -2         1232       0          1232       ACL
26         -2         27760      3552       24208      VaclLog
27         0          0          0          0          L3Aging
28         0          209168     0          209168     NetFlow
29         0          2688400    112        2688288    Fib
30         -2         0          0          0          Fib_bg_task
31         -2         176        0          176        ProtocolFilter
32         -2         16         0          16         telnetd
33         -2         16         0          16         tftpd
34         -2         1744       1632       112        ProtocolTimer
35         -2         96         0          96         ciscoRmonTimer
36         -2         96         0          96         ciscoUsrHistory
37         -2         112        0          112        rmonMediaIndep
38         -2         0          0          0          SnmpTraps
39         -2         0          0          0          memPoolMain
40         -2         16         0          16         Acct Send Bkg
41         -2         80         0          80         l2t_server
42         -2         144        0          144        Authenticator_S
43         -2         16         0          16         dot1x_rx
```

```
44         -2         16         0          16         Backend_Rx
45         -2         16         0          16         Backend_SM
46         -2         3216       2992       224        Debug Port Coun
47         -2         16         0          16         SysLogTask
48         -2         112        0          112        pinggateA
49         -2         8704       8000       704        cdpd
50         -2         124576     124416     160        cdpdtimer
51         -2         1296       1088       208        SptTimer
52         -2         2336       1120       1216       SptBpduRx
53         -2         144        0          144        SptBpduTx
54         -2         0          0          0          GL2Prot_Tunnel
55         -2         176        0          176        VtpTimer
56         -2         16         1072       4294966240 HPConfig
57         -2         96         0          96         RMON AlarmTimer
58         -2         0          0          0          sptTraps
59         -2         6128       5952       176        McastRx
60         -2         16         0          16         IGMPQuerierProc
61         -2         272        0          272        M-MLS_stats
62         -2         5808       1504       4304       M-MLS_manager
63         -2         47520      15216      32304      QoSTask
64         0          11936      0          11936      Read Stats Task
65         0          32         0          32         QDE Task
66         -2         144        0          144        EnvMon
67         -2         1120       0          1120       VlanStatsTask
70         -2         16         0          16         HPActive
71         -2         48         0          48         HPTrapMgr
143        0          57200      4208       52992      Console
144        -2         256208     29920      226288     snmpdm
145        -2         208        0          208        VtpRx
146        2252448660 68448      6864       61584      telnet146
191        -2         29360      19504      9856       AclManager

Memory Pool Utilization
Memory Pool Type 1Min  5Min  10Min
---------------- ----- ----- -----
DRAM               45%   45%   45%
FLASH              83%   83%   83%
NVRAM              49%   49%   49%
MBUF                2%    2%    2%
CLUSTER            11%   11%   11%
MALLOC             11%   11%   11%

Console> (enable)
```

Table 2-85 describes the possible fields in the **show proc** command outputs.

Table 2-85 show proc Command Output Fields

Field	Description
CPU Utilization	Sum of all the loads from all the processes running on the CPU in the last 5 seconds, 1 minute, and 5 minutes.
PID	Process ID.
Runtime	Time the process has run since initiation (in milliseconds).
Invoked	Number of times the process was invoked since initiation.
uSecs	Maximum time a process ran in a single invocation.
5sec	Amount of time this process ran on the CPU in the last 5-second interval.
1Min	Average memory pool usage over the last 1-minute interval.

Table 2-85 show proc Command Output Fields (continued)

Field	Description
5Min	Average memory pool usage over the last 5-minute interval.
10Min	Average memory pool usage over the last 10-minute interval.
TTY	TTY associated with the process.
Process	Name of the process.
Allocated	Amount of all the memory allocated by the process since it was initiated, including the memory previously freed up.
Freed	Amount of memory the process has freed up until now.
Holding	Amount of memory the process is currently holding.
Q	Process priority in terms of numbers. A low number means high priority.
T	State of the process (Running, we = waiting for event, st = sleeping, si = sleeping on an interval, rd = ready to run, id = idle, xx = dead/zombie).
PC	Calling PC for "show_process" function.
Stacks	Size of the stack used by the process/the total stack size allocated to the process (in bytes).

show protocolfilter

To list whether protocol filtering is enabled or disabled, use the **show protocolfilter** command.

show protocolfilter

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display whether protocol filtering is enabled or disabled:

```
Console> show protocolfilter
Protocol filtering is enabled on this switch.
Console>
```

Related Commands

set port protocol
set protocolfilter

show pvlan

To show the configuration for a given private VLAN, use the **show pvlan** command.

show pvlan [*vlan* | **primary** | **isolated** | **community** | **twoway-community**]

Syntax Description

vlan	(Optional) Number of the private VLAN.
primary	(Optional) Displays the primary private VLANs.
isolated	(Optional) Displays the isolated private VLANs.
community	(Optional) Displays the community private VLANs.
twoway-community	(Optional) Displays the bidirectional community private VLANs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

A **twoway-community** private VLAN is a bidirectional community private VLAN that carries traffic among community ports and to and from community ports to and from the MSFC.

Examples

This example shows how to display the status for VLAN 10:

```
Console> show pvlan 10
Primary Secondary Secondary-Type Ports
------- --------- -------------- ------------
10      20        isolated       6/1
Console>
```

This example shows how to display the status for all VLANs set as primary:

```
Console> show pvlan primary
Primary Secondary Secondary-Type Ports
------- --------- -------------- ------------
10      20        isolated       6/1
11      21        isolated       6/2
30      -         -
Console>
```

This example shows how to display the status for all VLANs set as isolated:

```
Console> show pvlan isolated
Primary Secondary Secondary-Type Ports
------- --------- -------------- ------------
10      20        isolated       6/1
11      21        isolated       6/2
-       31        isolated
Console>
```

This example shows how to display the status for all VLANs set as community:

```
Console> show pvlan community
Primary Secondary Secondary-Type Ports
------- --------- -------------- ------------
7       902       community      2/4-6
Console>
```

Related Commands

clear config pvlan
clear pvlan mapping
clear vlan
set pvlan
set pvlan mapping
set vlan
show pvlan mapping
show vlan

show pvlan capability

To determine whether or not a port can be made a private port, use the **show pvlan capability** command.

show pvlan capability *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to determine if a port can be made into a private VLAN:

```
Console> (enable) show pvlan capability 5/20
Ports 5/13 - 5/24 are in the same ASIC range as port 5/20.

Port 5/20 can be made a private vlan port.
Console> (enable)
```

These examples show the output if a port cannot be made into a private VLAN:

```
Console> (enable) show pvlan capability 3/1
Port 3/1 cannot be made a private vlan port due to:
------------------------------------------------------
Promiscuous ports cannot be made private vlan ports.
Console> (enable)

Console> (enable) show pvlan capability 5/1
Ports 5/1 - 5/12 are in the same ASIC range as port 5/1.

Port 5/1 cannot be made a private vlan port due to:
------------------------------------------------------
Trunking ports are not Private Vlan capable.
Conflict with Promiscuous port(s) : 5/2
Console> (enable)

Console> (enable) show pvlan capability 5/2
Ports 5/1 - 5/12 are in the same ASIC range as port 5/2.

Port 5/2 cannot be made a private vlan port due to:
------------------------------------------------------
Promiscuous ports cannot be made private vlan ports.
Conflict with Trunking port(s) : 5/1
Console> (enable)
Console> (enable) show pvlan capability 5/3
Ports 5/1 - 5/12 are in the same ASIC range as port 5/3.

Port 5/3 cannot be made a private vlan port due to:
------------------------------------------------------
Conflict with Promiscuous port(s) : 5/2
Conflict with Trunking port(s) : 5/1
Console> (enable)

Console> (enable) show pvlan capability 15/1
Port 15/1 cannot be made a private vlan port due to:
------------------------------------------------------
Only ethernet ports can be added to private vlans.
Console> (enable)
```

Related Commands

clear config pvlan
clear pvlan mapping
clear vlan
set pvlan
set pvlan mapping
set vlan
show pvlan mapping
show vlan

show pvlan mapping

To show the private VLAN mappings configured on promiscuous ports, use the **show pvlan mapping** command.

show pvlan mapping [*private_vlan* | *mod/port*]

Syntax Description

private_ vlan	(Optional) Number of the private VLAN.
mod/port	(Optional) Number of the module and port.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the private VLAN mapping by port:

```
Console> show pvlan mapping
Port Primary Secondary
---- ------- ---------
 6/3  10      20
Console>
```

This example shows how to display the private VLAN mapping for a specific VLAN:

```
Console> show pvlan mapping 10
Primary Secondary Ports
------- --------- -----
10      20        6/3
Console>
```

This example shows how to display the private VLAN mapping for a specific port:

```
Console> show pvlan mapping 6/3
Port Primary Secondary
---- ------- ---------
 6/3  10      20
Console>
```

This example shows the results when no VLANs are mapped:

```
Console> show pvlan mapping
Port Primary Secondary
---- ------- ---------
No Private Vlan Mappings configured.
Console>
```

Related Commands

clear config pvlan
clear pvlan mapping
clear vlan
set pvlan
set pvlan mapping
set vlan
show vlan

show qos acl editbuffer

To display ACL names in the edit buffer, use the **show qos acl editbuffer** command.

show qos acl editbuffer

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Enter the **show qos acl editbuffer** command to display the committed access lists that you configured. The information is helpful when you are adding or deleting ACEs.

Examples

This example shows how to display QoS ACL edit buffer contents:

```
Console> (enable) show qos acl editbuffer
ACL                                  Type Status
--------------------------------     ---- ----------
ip1                                  IP   Committed
ipx1                                 IPX  Committed
mac1                                 MAC  Committed
```

Related Commands

commit
rollback

show qos acl info

To display QoS ACL information, use the **show qos acl info** command.

show qos acl info default-action {**ip** | **ipx** | **mac** | **all**}

show qos acl info runtime {*acl_name* | **all**}

show qos acl info config {*acl_name* | **all**} [**editbuffer** [*editbuffer_index*]]

Syntax Description

default-action	Displays default action (using the **set qos acl default-action** command) for packets that do not match any entry in an access list.
ip	Displays QoS IP ACL information.
ipx	Displays all QoS IPX ACL information.
mac	Displays all QoS MAC ACL information.
all	Displays all QoS ACL information.
runtime	Displays runtime ACE information.
acl_name	Name of the ACL to be displayed.
config	Displays configured ACE information.
editbuffer	(Optional) Displays edit buffer information.
editbuffer_index	(Optional) Position of the ACE in the ACL.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display all ACL default configurations:

```
Console> (enable) show qos acl info default-action all
set qos acl default-action
--------------------------
ip dscp 7 my1 my2
ipx dscp 0
mac dscp 0
Console> (enable)
```

This example shows how to display edit buffer information for a specific ACL:

```
Console> (enable) show qos acl info my_ip_acl editbuffer
set qos acl ip my_ip_acl
----------------------------------------------------
1. set qos acl ip my_ip_acl trustdscp microflow my-micro tcp 1.2.3.4 255.0.0.0
eq port 21 172.20.20.1 255.255.255.0
```

```
2. set qos acl ip my_ip_acl trustdscp microflow my-micro aggregate agg tcp
173.22.3.4 255.0.0.0 eq port 19 173.22.20.1 255.255.255.0 tos 5
ACL status: Not Committed
Console> (enable)
```

This example shows how to display information for a specific ACL:

```
Console> (enable) show qos acl info my_ip_acl
set qos acl ip my_ip_acl
----------------------------------------------------
1. trust-dscp microflow my-micro tcp 1.2.3.4 255.0.0.0 eq
port 21 172.20.20.1 255.255.255.0 tos 5
2. trust-dscp microflow my-micro aggregate agg tcp
173.22.3.4 255.0.0.0 eq port 19 173.22.20.1 255.255.255.0 tos 5
Console> (enable)
```

This example shows how to display runtime information for all ACLs:

```
Console> (enable) show qos acl info runtime all
set qos acl IP _Cops_1
----------------------------------------------
1. dscp 0 any

set qos acl IP _Cops_2
----------------------------------------------
1. dscp 8 ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
2. dscp 16 tcp any any
3. dscp 24 udp any any
Console> (enable)
```

Related Commands

clear qos policer
set qos acl default-action
set qos policer

show qos acl map

To display the ACL mapping information, use the **show qos acl map** command.

show qos acl map {**config** | **runtime**} {*acl_name* | *mod/port* | *vlan* | **all** | **all-vlans** | **all-ports**}

Syntax Description

config	Displays NVRAM QoS information.
runtime	Displays QoS runtime information.
acl_name	Name of the list.
mod/port	Number of the module and the port.
vlan	VLAN list.
all	Displays information regarding all ACLs.
all-vlans	Displays all ACL-to-VLAN mapping.
all-ports	Displays all ACL-to-port mapping.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can enter the **config** keyword to display information that was configured through the CLI and saved in NVRAM, regardless of the current runtime information.

Note When a switchover occurs, you cannot view the ACLs and policers deployed using COPS-DS until the COPS-DS client on the new active supervisor engine establishes connection to the PDP and downloads the QoS policy. The runtime fields in the output display will be blank until QoS policy is downloaded to the new active supervisor engine.

Examples

This example shows how to display information for all ACLs:

```
Console> show qos acl map all
ACL name   Vlan #            Ports
--------   ----------------- -----------------------------
web-acc    1,4-7
isp1       2                 1/1
Console>
```

This example shows how to display information for a specific VLAN:

```
Console> show qos acl map 1
Vlan  ACL name
----  ----------------
1     web-acc
Console>
```

This example shows how to display information for a specific ACL:

```
Console> show qos acl map isp1

ACL name   Vlan #            Ports
--------   ----------------  ---------------
isp1       2                 1/1
Console>
```

Related Commands

clear qos acl
set qos acl map

show qos acl resource-usage

To display ACL management information, use the **show qos acl resource-usage** command.

show qos acl resource-usage

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display ACL management information:

```
Console> (enable) show qos acl resource-usage
ACL resource usage:
Label:0%
Logical Operation Unit:0%
TCAM mask:0%
TCAM value:0%
Console> (enable)
```

Related Commands

commit
rollback

show qos bridged-microflow-policing

To display the VLAN-bridged packet-policing status, use the **show qos bridged-microflow-policing** command.

show qos bridged-microflow-policing {**config** | **runtime**} [*vlan*]

Syntax Description

config	Displays NVRAM configuration.
runtime	Displays the run time configuration.
vlan	(Optional) Number of the VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you do not specify a VLAN number, the status of all VLANs are displayed.

Examples

This example shows how to display the NVRAM configuration of a specific VLAN:

```
Console> show qos bridged-microflow-policing config 1
QoS microflow policing is disabled for bridged packets on vlan 1.
Console>
```

This example shows how to display the NVRAM configuration of all VLANs:

```
Console> show qos bridged-microflow-policing config
QoS microflow policing is disabled for bridged packets on vlan(s) 1-1000,1025-40
94.
Console>
```

RelatedCommands

clear qos policer
set qos bridged-microflow-policing
set qos policer

show qos info

To display QoS-related information for a specified port, use the **show qos info** command.

show qos info {**runtime** | **config**} {*mod/port*}

show qos info config *port_type* {**tx** | **rx**}

Syntax Description

runtime	Shows the current QoS runtime information.
config	Displays NVRAM QoS configuration.
mod/port	Number of the module and port.
port_type	Port type; valid values are **2q2t**, **1p3q1t**, **1p2q2t**, **1p2q1t** for transmit and **1q4t**, **1p1q4t**, and **1p1q0t**, **1p1q8t**, and **1q2t** for receive. See the "Usage Guidelines" section for additional information.
tx	Displays transmit port information.
rx	Displays receive port information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can enter the **show qos info runtime** *mod/port* command to view the currently used values in the hardware or the **show qos info runtime** *mod/port* command to view the values that have been configured administratively (present in NVRAM). The outputs differ when QoS has been disabled. When you disable QoS, the values set on all the ports are different from the values present in NVRAM. When you enable QoS, the values in NVRAM are used to program the hardware.

The display of **show qos info runtime** *mod/port* shows both the absolute values and the percentages you specified for the drop thresholds, queue sizes, and WRR. However, the absolute values may not exactly match the percentages specified due to the granularity of permitted settings in hardware.

The number preceding the **t** letter in the *port_type* value (for example, **2q2t**, **1p2q2t**, **1q4t**, **1p1q4t**, or **1q2t**) determines the number of threshold values the hardware supports. For example, with **2q2t**, **1q2t** and **1p2q2t**, the number of thresholds specified is two; with **1q4t** and **1p1q4t**, the number of thresholds specified is four. Due to the granularity of programming the hardware, the values set in hardware will be close approximations of the values provided.

The number preceding the **q** letter in the *port_type* value determines the number of the queues that the hardware supports. For example, with **2q2t** and **1p2q2t**, the number of queues specified is two; with **1q4t 1p1q4t**, and **1q2t**, the number of queues specified is one. The system defaults for the transmit queues attempt to keep the maximum latency through a port at a maximum of 10 ms.

The number preceding the **p** letter in the *port_type* value (for example, **1p2q2t** and **1p1q4t**) determines the threshold in the priority queue.

The **1p2q1t** and **1p1q8t** port types are not supported.

Note When a switchover occurs, you cannot view the ACLs and policers deployed using COPS-DS until the COPS-DS client on the new active supervisor engine establishes connection to the PDP and downloads the QoS policy. The runtime fields in the output display will be blank until QoS policy is downloaded to the new active supervisor engine.

Examples

This example shows how to display QoS-related NVRAM-transmit threshold information:

```
Console> (enable) show qos info config 2q2t tx
QoS setting in NVRAM for 2q2t transmit:
QoS is disabled
 CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Tx drop thresholds:
Queue #  Thresholds - percentage (abs values )
-------  -------------------------------------
1        40% 100%
2        40% 100%
Queue Sizes:
Queue #  Sizes - percentage (abs values )
-------  -------------------------------------
1        80%
2        20%
WRR Configuration:
Ports have transmit ratios between queue 1 and 2 of
100:256
Console> (enable)
```

This example shows how to display QoS-related NVRAM receive-threshold information:

```
Console> (enable) show qos info config 1p1q4t rx
QoS setting in NVRAM for 1p1q4t receive:
QoS is disabled
Queue and Threshold Mapping for 1p1q4t (rx):
Queue Threshold CoS
----- --------- ---------------
1     1         0
1     2         2 3
1     3         4 5
1     4         1 6 7
2     1
Rx drop thresholds:
Queue #  Thresholds - percentage (abs values )
-------  -------------------------------------
1        50% 60% 80% 100%
Console> (enable)
```

This example shows how to display all QoS-related NVRAM threshold information:

```
Console> (enable) show qos info config 2q2t tx
QoS setting in NVRAM for 2q2t transmit:
QoS is enabled
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Tx drop thresholds:
Queue #  Thresholds - percentage (abs values )
-------  -------------------------------------
1        40% 100%
2        40% 100%
Queue Sizes:
Queue #  Sizes - percentage (abs values )
-------  -------------------------------------
1        80%
2        20%
WRR Configuration:
Ports with 2q2t have ratio of 100:255 between transmit queue 1 and 2
Console> (enable)
```

This example shows how to display the current QoS runtime information:

```
Console> (enable) show qos info runtime 1/1
Run time setting of QoS:
QoS is enabled on 2/1
Port 2/1 has 2 transmit queue with 2 drop thresholds (2q2t).
Port 2/1 has 1 receive queue with 4 drop thresholds (1q4t).
The qos trust type is set to trust-cos.
 CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Rx drop thresholds:
Queue #  Thresholds - percentage (abs values )
-------  -------------------------------------
1        50% (38912 bytes) 60% (46688 bytes) 80% (62240 bytes) 100% (73696
bytes)
Tx drop thresholds:
Queue #  Thresholds - percentage (abs values )
-------  -------------------------------------
1        40% (144224 bytes) 100% (360416 bytes)
2        40% (32864 bytes) 100% (77792 bytes)
Queue Sizes:
Queue #  Sizes - percentage (abs values)
-------  -------------------------------------
1        80% (360416 bytes)
2        20% (81888 bytes)
WRR Configuration:
Ports with speed 1000Mbps have ratio of 100:255 between transmit queue 1
and 2 (25600:65280 bytes)
Console> (enable)
```

This example shows another display of the current QoS runtime information:

```
Console> show qos info runtime 8/1
Run time setting of QoS:
QoS is enabled
Policy Source of port 8/1:Local
Tx port type of port 8/1 :1p2q2t
Rx port type of port 8/1 :1q2t
Interface type:port-based
ACL attached:
The qos trust type is set to trust-cos.
Default CoS = 0
Queue and Threshold Mapping for 1p2q2t (tx):
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 6
2     2         7
3     -         5
Queue and Threshold Mapping for 1q2t (rx):
Queue Threshold CoS
----- --------- ---------------
1     1         0 1 2 3 4
1     2         5 6 7
Rx drop thresholds:
Queue #  Thresholds - percentage (* abs values)
-------  ------------------------------------
1        80% (13106 bytes) 100% (16384 bytes)
Tx drop thresholds:
Tx drop-thresholds feature is not supported for this port type.
Rx WRED thresholds:
WRED feature is not supported for this port type.
Tx WRED thresholds:
Queue #  Thresholds - percentage (* abs values)
-------  -----------------------------------------
1        40%:70% (170393:298240 bytes) 70%:100% (298188:425856 bytes)
2        40%:70% (32768:57344 bytes) 70%:100% (57344:77824 bytes)
Tx queue size ratio:
Queue #  Sizes - percentage (* abs values)
-------  ------------------------------------
1        70% (425984 bytes)
2        15% (81920 bytes)
3        15% (81920 bytes)
Rx queue size ratio:
Rx queue size-ratio feature is not supported for this port type.
WRR Configuration of ports with speed 10Mbps:
Queue #  Ratios (* abs values)
-------  ------------------------------------
1        100 (25600 bytes)
2        255 (65280 bytes)
(*) Runtime information may differ from user configured setting due to hardware
granularity.
Console> (enable)
```

This example shows how to display the current QoS configuration information:

```
Console> (enable) show qos info config 8/1
QoS setting in NVRAM:
QoS is disabled
Port 8/1 has 3 transmit queue with 2 drop thresholds (1p2q2t).
Port 8/1 has 2 receive queue with 4 drop thresholds (1p1q4t).
ACL attached:
The qos trust type is set to untrusted.
 CoS = 0
Queue and Threshold Mapping for 1p2q2t (tx):
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         7
3     1         6
Queue and Threshold Mapping for 1p1q4t (rx):
Queue Threshold CoS
----- --------- ---------------
1     1         0
1     2         2 3
1     3         4 5
1     4         1 6 7
2     1
Rx drop thresholds:
Rx drop thresholds are disabled for untrusted ports.
Queue #  Thresholds - percentage (abs values )
-------  -------------------------------------
1        50% 60% 80% 100%
Tx drop thresholds:
Tx drop-thresholds feature is not supported for this port type.
Tx WRED thresholds:
Queue #  Thresholds in percentage ( in abs values )
-------  ------------------------------------------
1        80% 100%
2        80% 100%
Queue Sizes:
Queue #  Sizes - percentage (abs values )
-------  -------------------------------------
1        70%
2        15%
3        15%
WRR Configuration of ports with speed 1000Mbps:
Queue #  Ratios (abs values )
-------  -------------------------------------
1        100
2        255
Console> (enable)
```

This example shows another display of the current QoS configuration information:

```
Console> (enable) show qos info config 1p2q2t tx
QoS setting in NVRAM for 1p2q2t transmit:
QoS is enabled
Queue and Threshold Mapping:
Tx WRED thresholds:
Queue #  Thresholds - percentage
-------  --------------------------------------
1        0%:60% 0%:90%
2        0%:50% 0%:90%
Tx queue size ratio:
Queue #  Sizes - percentage
-------  -------------------------------------
1        70%
2        15%
3        15%
WRR Configuration of ports with 1p2q2t:
Queue #  Ratios
-------  -------------------------------------
1        5
2        255
Console> (enable)
```

Related Commands

clear port qos autoqos
clear qos autoqos
set port qos autoqos
set qos
set qos autoqos
show port qos

show qos mac-cos

To display the currently configured QoS-related information for the MAC address and VLAN pair, use the **show qos mac-cos** command.

show qos mac-cos *dest_mac* [*vlan*] [**config**]

show qos mac-cos all [**config**]

Syntax Description

dest_mac	MAC address of the destination host.
vlan	(Optional) Number of the VLAN; valid values are from 1 to 1005.
config	(Optional) Displays NVRAM QoS configuration.
all	Specifies all MAC address and VLAN pairs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can enter the **show qos mac-cos** command to display the currently configured QoS-related information.

You can enter the **config** keyword to display information that was configured through the CLI and saved in NVRAM, regardless of the current runtime information.

Examples

This example shows how to display currently configured QoS-related information for all MAC address and VLAN pairs:

```
Console> (enable) show qos mac-cos all
VLAN  Dest MAC           CoS
----  ------------------ ---
1       01-02-03-04-05-06  2
9       04-05-06-07-08-09  3
Console> (enable)
```

This example shows how to display currently configured QoS-related information for a specific MAC address:

```
Console> (enable) show qos mac-cos 01-02-03-04-05-06
VLAN  Dest MAC           CoS
----  ------------------ ---
1       01-02-03-04-05-06  2
Console> (enable)
```

Related Commands

clear qos mac-cos
set qos mac-cos

show qos maps

To display the mapping of different maps, use the **show qos maps** command.

show qos maps {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map** [**normal-rate** | **excess-rate**] | **dscp-mutation-map** [*mutation_table_id*] | **dscp-mutation-table-map** [*mutation_table_id*] | **cos-cos-map** [*mod/port*]]

Syntax Description

config	Displays NVRAM QoS configuration.
runtime	Displays current QoS configuration.
cos-dscp-map	(Optional) Specifies the CoS-to-DSCP map.
ipprec-dscp-map	(Optional) Specifies the IP precedence-to-DSCP map.
dscp-cos-map	(Optional) Specifies the DSCP-to-CoS map.
policed-dscp-map	(Optional) Specifies the marked-down map.
normal-rate	(Optional) Specifies normal rate.
excess-rate	(Optional) Specifies excess rate.
dscp-mutation-map	(Optional) Specifies a DSCP mutation map.
mutation_table_id	(Optional) Number of the mutation table; valid values are from 1 to 15. See the "Usage Guidelines" section for more information.
dscp-mutation-table-map	(Optional) Specifies a DSCP mutation table map.
cos-cos-map	(Optional) Specifies the CoS-to-CoS map.
mod/port	(Optional) Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can enter the **config** keyword to display information that was configured through the CLI and saved in NVRAM, regardless of the current runtime information.

If you do not specify an option, all maps are displayed.

Note When a switchover occurs, you cannot view the ACLs and policers deployed using COPS-DS until the COPS-DS client on the new active supervisor engine establishes connection to the PDP and downloads the QoS policy. The runtime fields in the output display will be blank until QoS policy is downloaded to the new active supervisor engine.

If you do not enter a *mutation_table_id* argument, the system displays all DSCP mutation maps.

Examples

This example shows how to display the cos-dscp-map map:

```
Console> show qos maps cos-dscp-map
CoS - DSCP map:
CoS   DSCP
---   ---------------
0     10
...
7     52
Console>
```

This example shows how to display the ipprec-dscp-map map:

```
Console> show qos maps ipprec-dscp-map
IP-Precedence - DSCP map:
IP-Prec   DSCP
-------   -------------------
0         1
...
7         52
Console>
```

This example shows how to display the dscp-cos-map map:

```
Console> show qos maps dscp-cos-map
DSCP - CoS map:
DSCP             CoS
---------------  ----
34-40,60         0
...
50               7
Console>
```

This example shows how to display the policed-dscp-map map:

```
Console> show qos maps policed-dscp-map
DSCP policed-dscp map:
In-profile DSCP  Policed DSCP
---------------  -------------
0-20             0
Console>
```

This example shows how to display all maps:

```
Console> show qos maps
CoS - DSCP map:
CoS   DSCP
---   ---------------
0     10
...
7     52

IP-Precedence - DSCP map:
IP-Prec   DSCP
-------   -------------------
0         1
...
7         52

IP-Precedence - CoS map:
IP-Prec   CoS
-------   -----
0         0
...
7         7
```

```
DSCP - CoS map:
DSCP             CoS
---------------  ----
34-40,60         0
...
50               7

DSCP policed-dscp map:
In-profile DSCP  Policed DSCP
---------------  -------------
0-20             0
Console>
```

This example shows how to display normal-rate maps:

```
Console> show qos maps config policed-dscp-map normal-rate
DSCP - Policed DSCP map normal-rate:
DSCP                              Policed DSCP
--------------------------------  ------------
                        0, 24-63  0
                               1  1
                               2  2
                               3  3
                               4  4
                               5  5
                               6  6
                               7  7
                               8  8
                               9  9
                              10  10
                              11  11
                              12  12
                              13  13
                              14  14
                              15  15
                              16  16
                              17  17
                              18  18
                              19  19
                              20  20
                              21  21
                              22  22
                              23  23
Console>
```

This example shows how to display the configuration for DSCP mutation map 1:

```
Console> show qos maps config dscp-mutation-map 1
Mutation Table ID:
Map ID  VLANS
------  ----------------------------------------
     1  1,78-1005,1025-4094
DSCP mutation map 1:
DSCP                              Policed DSCP
--------------------------------  ------------
                               0  0
                               1  1
                               2  2
                               3  3
                               4  4
                               5  5
                               6  6
                               7  7
                               8  8
                               9  9
                              10  10
                              11  11
                              12  12
                              13  13
                              14  14
                              15  15
                              16  16
                              17  17
                              18  18
                              19  19
                              20  20
                              21  21
                              22  22
                              23  23
                              24  24
                              25  25
                              26  26
                              27  27
                              28  28
                              29  29
                              30  30
                              31  31
                              32  32
                              33  33
                              34  34
                              35  35
                              36  36
                              37  37
                              38  38
                              39  39
                              40  40
                              41  41
                              42  42
                              43  43
                              44  44
                              45  45
                              46  46
                              47  47
                              48  48
                              49  49
                              50  50
                              51  51
                              52  52
                              53  53
                              54  54
                              55  55
                              56  56
                              57  57
                              58  58
                              59  59
                              60  60
                              61  61
                              62  62
                              63  63
Console>
```

This example shows how to display the NVRAM CoS-to-CoS map:

```
Console> show qos maps config cos-cos-map
CoS - CoS map:
CoS   CoS
---   ----
  0   0
  1   5
  2   4
  3   5
  4   4
  5   5
  6   6
  7   7
Console>
```

This example shows how to display the current CoS-to-CoS map on a specific port:

```
Console> show qos maps runtime cos-cos-map 3/2
CoS - CoS map:
CoS   CoS
---   ----
  0   0
  1   5
  2   4
  3   5
  4   4
  5   5
  6   6
  7   7
Console>
```

Related Commands

clear qos cos-cos-map
clear qos cos-dscp-map
clear qos dscp-mutation-map
clear qos dscp-mutation-table-map
clear qos policed-dscp-map
set qos map
set qos cos-cos-map
set qos cos-dscp-map
set qos dscp-mutation-map
set qos dscp-mutation-table-map

show qos policer

To display microflow or aggregate policers currently configured, use the **show qos policer** command.

show qos policer {**config** | **runtime**} {**microflow** [*policer_name*] | **aggregate** [*policer_name*] | **all**}

Syntax Description

config	Displays NVRAM QoS configuration.
runtime	Shows the current QoS runtime information.
microflow	Specifies microflow policing information.
aggregate	Specifies aggregate policing rule information.
policer_name	(Optional) Name of the policer.
all	Specifies all policing information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

When a switchover occurs, you cannot view the ACLs and policers deployed using COPS-DS until the COPS-DS client on the new active supervisor engine establishes connection to the PDP and downloads the QoS policy. The runtime fields in the output display will be blank until QoS policy is downloaded to the new active supervisor engine.

Examples

This example shows how to display all currently configured policing information:

```
Console> show qos policer config all
QoS microflow policers:
Microflow name                  Avg. rate Burst size Exceed action
------------------------------- --------- ---------- -------------
mic                                    55         64 drop
                                ACL attached
                                ------------------------------------

QoS aggregate policers:
No aggregate policer found.
Console>
```

This example shows how to display microflow policing information:

```
Console> show qos policer config microflow
QoS microflow policers:
Microflow name        Average rate     Burst size       Exceed action
--------------------  ---------------  ---------------  -------------
my-micro              1000             2000             drop
Microflow name        ACL attached
--------------------  -----------------------------------------------
my-micro              my-acl
Console>
```

This example shows how to display aggregate policing information:

```
Console> show qos policer config aggregate
QoS aggregate policers:
No aggregate policer found.
Console>
```

This example shows how to display aggregate policing information for a specific policer:

```
Console> show qos policer config aggregate
QoS aggregate policers:
Aggregate name                Normal rate (kbps)  Burst size (kb) Normal action
----------------------------- ------------------  --------------- -------------
test2                                         64              100  policed-dscp
                              Excess rate (kbps)  Burst size (kb) Excess action
                              ------------------  --------------  ---------------
                                         8000000              100  policed-dscp
                              ACL attached
                              ------------------------------------
Console>
```

Related Commands

clear qos policer
set qos policer

show qos policy-source

To display the QoS policy source information, use the **show qos policy-source** command.

show qos policy-source

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command displays whether the QoS policy source is set to local or COPS.

Examples

This example shows how to view the QoS policy source:

```
Console> show qos policy-source
QoS policy source for the switch set to local.
Console>
```

Related Commands

set qos policy-source

show qos rsvp

To display RSVP information, use the **show qos rsvp** command.

show qos rsvp {**info** | **flow-info**}

Syntax Description

info	Displays RSVP status information.
flow-info	Displays RSVP flow information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The maximum number of RSVP flows displayed in the **show qos rsvp flow-info** command output are as follows:

- 1024 for switches configured with the Supervisor Engine 1 with Layer 3 Switching Engine Policy Feature Card (WS-F6K-PFC).
- 1056 for systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2)

Examples

This example shows how to display RSVP status information:

```
Console> (enable) show qos rsvp info
RSVP disabled.
RSVP policy timeout set to 30 minutes.
RSVP local policy set to forward.
Console> (enable)
```

This example shows how to display RSVP flow information:

```
Console> (enable) show qos rsvp flow-info
RSVP enabled. Only RSVP qualitative service supported.
RSVP policy timeout set to 30 minutes.

Flow # SrcAddr         DstAddr         SrcPort DstPort Prot DSCP Time Valid
------ --------------- --------------- ------- ------- ---- ---- -----------
1         172.21.23.34    177.23.45.67    3001    3101  UDP    6          30
2         172.21.23.34    177.23.45.67    3002    3102  UDP    4          15
3         172.21.23.34    177.23.45.67    3003    3103  TCP    2          68
4         172.21.34.67    177.68.89.23    4004    4005  UDP    1          23
Console> (enable)
```

Related Commands

clear qos policer
set qos rsvp

show qos statistics

To display the various QoS-related counters for a specified port, use the **show qos statistics** command.

show qos statistics {*mod*[*/port*]}

show qos statistics l3stats

show qos statistics aggregate-policer [*policer_name*]

Syntax Description

mod/port	Number of the module and, optionally, the number of the port on the module.
l3stats	Displays Layer 3 statistics information.
aggregate-policer	Displays QoS aggregate policer statistics.
policer_name	(Optional) Policer name. See the "Usage Guidelines" section for more information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

In the **show qos statistics** output, the Threshold #:Packets dropped field lists each threshold and the number of packets dropped. For example, 1:0 pkt, 2:0 pkts indicates that threshold 1 and threshold 2 dropped 0 packets.

If you do not enter a *policer_name* argument, the system displays statistics for all QoS aggregate policers.

Every 30 seconds, QoS port statistics, QoS Layer 3 statistics, and QoS aggregate policer statistics are collected and stored. Then the rate for these statistics types are averaged over a 300-second period (5 minutes). When you enter the **show qos statistics** *mod/port* command, the **show qos statistics l3stats** command, or the **show qos statistics aggregate-policer** command, the average for the last 300-second period is averaged with current statistics. This average value and the peak value over the last 300-second period is part of the command output.

Examples

This example shows how to display the QoS statistics for module 5, port 1:

```
Console> show qos statistics 5/1
Tx port type of port 5/1 : 2q2t
Q # Threshold #:Packets dropped; Packet drop rate (pps)
--- -----------------------------------------------
1   1:0 pkts; 0 pps; 0 pkts

1   2:0 pkts; 0 pps; 0 pkts
2   1:0 pkts; 0 pps; 0 pkts

2   2:0 pkts; 0 pps; 0 pkts
Console>
```

This example shows how to display the QoS Layer 3 statistics:

```
Console> show qos statistics average l3stats
                                     Total Packets Rate (pps)    Peak (packets)
                                     ------------- ------------- -------------
Packets dropped due to policing:          0             0              0
IP packets with ToS changed:              0             0              0
IP packets with CoS changed:              0             0              0
Non-IP packets with CoS changed:          0             0              0
Console>
```

This example shows how to display the QoS statistics for module 2:

```
Console> show qos statistics 2
Warning: QoS is disabled.
On Transmit:Port 2/1 has 2 Queue(s) 2 Threshold(s)
Q #  Threshold #:Packets dropped
---  -----------------------------------------------
1    1:0 pkts, 2:0 pkts
2    1:0 pkts, 2:0 pkts
On Receive:Port 2/1 has 1 Queue(s) 4 Threshold(s)
Q #  Threshold #:Packets dropped
---  -----------------------------------------------
1    1:0 pkts, 2:0 pkts, 3:0 pkts, 4:0 pkts

On Transmit:Port 2/2 has 2 Queue(s) 2 Threshold(s)
Q #  Threshold #:Packets dropped
---  -----------------------------------------------
1    1:0 pkts, 2:0 pkts
2    1:0 pkts, 2:0 pkts
On Receive:Port 2/2 has 1 Queue(s) 4 Threshold(s)
Q #  Threshold #:Packets dropped
---  -----------------------------------------------
1    1:0 pkts, 2:0 pkts, 3:0 pkts, 4:0 pkts
Console>
```

This example shows how to display statistics for a QoS aggregate policer:

```
Console> show qos statistics aggregate-policer ag1
QoS aggregate-policer statistics:
Aggregate policer               Allowed byte   Bytes exceed
                                count          excess rate
-----------------------         -------------- --------------
ag1                             12138176       4553555392

QoS aggregate-policer 5 minute rate statistics:
```

```
Aggregate policer               Allowed rate   Traffic exceeding
                                (kbps)         excess rate
------------------------------- -------------- --------------
ag1                             0              0

QoS aggregate-policer Peak statistics:

Aggregate policer               Peak byte      Peak Traffic exceeding
                                count          excess rate
------------------------------- -------------- --------------
ag1                             766514432      320562695296
Console>
```

Related Commands

set qos
set qos drop-threshold
set qos mac-cos
set qos txq-ratio
set qos wrr

show qos statistics export info

To display QoS data export configuration and statistical information, use the **show qos statistics export info** command.

show qos statistics export info

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display QoS data export configuration and statistical information:

```
Console> (enable) show qos statistics export info
QoS Statistics Status and Configuration Information
---------------------------------------------------
Export Status: disabled.
Export time interval: 35 seconds
Export destination: Stargate, UDP port 9996

Port   Export
------ --------
 1/1    enabled
 1/2   disabled
 2/2    enabled
 2/5    enabled
 2/7    enabled

Aggregate name  Export
--------------- --------
ipagg_1          enabled
ipagg_2         disabled
ipagg_3          enabled
Console> (enable)
```

Related Commands

set qos statistics export aggregate
set qos statistics export port

show qos status

To display if QoS is enabled on the switch, use the **show qos status** command.

show qos status

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display if QoS is enabled on the switch:

```
Console> (enable) show qos status
Qos is enabled on this switch.
DSCP rewrite has been globally disabled.
Console> (enable)
```

Related Commands

set qos
set qos dscp-rewrite

show radius

To display configured RADIUS parameters, use the **show radius** command.

show radius [**noalias**]

Syntax Description

noalias	(Optional) Forces the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can enter this command in normal or privileged mode, but the RADIUS key is displayed only if this command is entered in privileged mode.

Examples

This example shows how to display RADIUS information:

```
Console> show radius
Active RADIUS Server          : 0.0.0.0
RADIUS Deadtime               : 0 minutes
RADIUS Retransmit             : 2
RADIUS Timeout                : 5 seconds
Framed-Ip Address Transmit    : Disabled
RADIUS Framed MTU             : 1000 bytes
RADIUS Keepalive              : Enabled
RADIUS Keepalive Timer        : 5 minutes
RADIUS Autoinitialize Critical: Disabled

RADIUS-Server      Status  Auth-port Acct-port Resolved IP Address Operational State
------------------ ------- --------- --------- ------------------- ------------------
81.81.81.20        primary 1812      1813                          Active
10.6.89.200                1812      1813                          Dead
10.6.98.35                 1812      1813                          Checkup
Console>
```

Related Commands

set radius attribute
set radius deadtime
set radius key
set radius retransmit
set radius server
set radius timeout

show rate-limit

To display rate-limiter settings and information, use the **show rate-limit** command.

show rate-limit [**config**]

Syntax Description

config	(Optional) Displays the Layer 2 rate-limiter administrative and operation status information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

In the command output, the rate-limit status could be one of the following:

- On indicates a rate for that particular case has been set.
- Off indicates that the rate-limiter type has not been configured, and the packets for that case are not rate limited.
- On/Sharing indicates that a particular case (not manually configured) is affected by the configuration of another rate limiter belonging to the same sharing group.

The following restrictions apply if you want to enable rate limiting:

- Hardware-based rate limiters are supported on Catalyst 6500 series switches that are configured with a Distributed Forwarding Card 3A (DFC3A) or the Policy Feature Card 3 (PFC3) only.
- The Catalyst 6500 series switch cannot be in truncated mode. If you attempt to enable rate limiting and you are in truncated mode, a message appears.

If the rate limiter is enabled and some events cause the system to go from nontruncated mode to truncated mode, rate limiting is disabled and a message appears.

Examples

This example shows how to display rate-limiter settings and information:

```
Console> show rate-limit
Configured Rate Limiter Settings:
Rate Limiter Type    Status  Rate (pps)      Burst
-------------------- ------  --------------  -----
VACL LOG             On      2500            1
ARP INSPECTION       On      500             1
MCAST NON RPF        Off     *               *
MCAST DFLT ADJ       On      100000          100
MCAST DIRECT CON     Off     *               *
ACL INGRESS BRIDGE   Off     *               *
ACL EGRESS BRIDGE    Off     *               *
L3 SEC FEATURES      Off     *               *
```

```
FIB RECEIVE          Off     *              *
FIB GLEAN            Off     *              *
MCAST PARTIAL SC     Off     *              *
RPF FAIL             On      500            10
TTL FAIL             Off     *              *
No Route             On      500            10
ICMP UNREACHABLE     On      500            10
ICMP REDIRECT        Off     *              *
MTU Fail             Off     *              *
Console>
```

This example shows how to display the Layer 2 rate-limiter operational status information:

```
Console> show rate-limit
Configured Rate Limiter Settings:
Rate Limiter Type    Status  Rate (pps)     Burst
-------------------- ------ -------------- -----
VACL LOG             On      2500           1
ARP INSPECTION       On      500            1
L2 PDU               On      1000           1
L2 PROTOCOL TUNNEL   On      1000           1
L2 PORT SECURITY     On      1000           1
MCAST NON RPF        Off     *              *
MCAST DFLT ADJ       Off     *              *
MCAST DIRECT CON     Off     *              *
ACL INGRESS BRIDGE   Off     *              *
ACL EGRESS BRIDGE    Off     *              *
L3 SEC FEATURES      Off     *              *
FIB RECEIVE          Off     *              *
FIB GLEAN            Off     *              *
MCAST PARTIAL SC     Off     *              *
RPF FAIL             Off     *              *
TTL FAIL             Off     *              *
NO ROUTE             Off     *              *
ICMP UNREACHABLE     Off     *              *
ICMP REDRECT         Off     *              *
MTU FAIL             Off     *              *
Console>
```

This example shows how to display the Layer 2 rate-limiter administrative and operation status information:

```
Console> show rate-limit config

Rate Limiter Type    Admin Status Oper Status
-------------------- ------------ -----------
l2pdu                On           On
l2protocol-tunnel    On           On
l2port-security      On           On
Console>
```

Related Commands

set rate-limit

show rcp

To display rcp information, use the **show rcp** command.

show rcp

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display rcp information:

```
Console> (enable) show rcp
rcp username for VMPS       :xena
rcp username for SysInfoLog :sarahkiki
rcp username for others     :jdoe
Console> (enable)
```

Related Commands

clear rcp
set rcp username

8.6 EFT Copy

show reset

To display scheduled reset information, use the **show reset** command.

show reset

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display scheduled reset information:

```
Console> (enable) show reset
Reset schedule for Fri Jan 21 2000, 23:00:00 (in 3 days 12 hours 56 minutes 57 seconds).
Reset reason: Software upgrade
Console> (enable)
```

Related Commands

reset—switch

show rgmp group

To display all multicast groups or the count of multicast groups that are joined by RGMP-capable routers, use the **show rgmp group** command.

show rgmp group [*mac_addr*] [*vlan_id*]

show rgmp group count [*vlan_id*]

Syntax Description

mac_addr	(Optional) MAC destination address reserved for the use of RGMP packets.
vlan_id	(Optional) Number of the VLAN; valid values are from 1 to 1005.
count	Displays the total number of entries in a VLAN group that are joined by RGMP-capable routers.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example displays all multicast groups joined by RGMP-capable routers:

```
Console> show rgmp group

Vlan          Dest MAC/Route Des    RGMP Joined Router Ports
---------------------------------------------------------------------
1             01-00-5e-00-01-28          5/1,5/15
1             01-00-5e-01-01-01          5/1
2             01-00-5e-27-23-70*         3/1,5/1
Total Number of Entries=3

'*'- Configured manually
Console>
```

This example displays the total number of entries of VLAN group 1 that are joined by RGMP-capable routers:

```
Console> show rgmp group count 1
RGMP enabled.
Total Number of Entries=2
Console>
```

Related Commands

clear rgmp statistics
set rgmp
show rgmp statistics

show rgmp statistics

To display all the RGMP-related statistics for a given VLAN, use the **show rgmp statistics** command.

show rgmp statistics [*vlan*]

Syntax Description

vlan	(Optional) Number of the VLAN.

Defaults

The default is VLAN 1.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example displays RGMP-related statistics for a specific VLAN:

```
Console> show rgmp statistics 23
RGMP enabled
RGMP Statistics for vlan <23>:
Recieve:
Valid pkts:       20
Hellos:           10
Joins:            5
Leaves:           5
Join Alls:        0
Leave Alls:       0
Byes:             0
Discarded:        0
Transmit:
Total Pkts:       10
Failures:         0
Hellos:           10
Joins:            0
Leaves:           0
Join Alls:        0
Leave Alls:       0
Byes:             0
Console>
```

Related Commands

clear rgmp statistics
set rgmp
show rgmp group

show rspan

To display the remote SPAN configuration, use the **show rspan** command.

show rspan

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The fields displayed depends on the configuration. For example, if this is a source session, the Destination, Incoming Packets, and Learning fields are not displayed. If this is a destination session, the Admin Source, Oper Source, Direction, Multicast, Filter, and Max Bandwidth fields are not displayed. If there is no VLAN filtering on the source session, the Filter field is not displayed.

Examples

This example shows the display output from the **show rspan** command:

```
Console> (enable) show rspan

Destination     : -
Rspan Vlan      : 900
Admin Source    : VLAN 50
Oper Source     : Port 2/1,2/3,2/5,2/7,2/9,2/11,2/13,2/15,2/17,2/19
Direction       : receive
Incoming Packets: -
Learning        : -
Multicast       : disabled
Filter          : 10,20,30,40,500,600,700,800,900
Status          : active

--------------------------------------------

Destination     : Port 3/1
Rspan Vlan      : 901
Admin Source    : -
Oper Source     : -
Direction       : -
Incoming Packets: disabled
Learning        : disabled
Multicast       : -
Filter          : -
Status          : active
--------------------------------------------
```

```
Destination     : Port 6/1
Rspan Vlan      : 906
Admin Source    : -
Oper Source     : -
Direction       : -
Incoming Packets: disabled
Learning        : -
Multicast       : -
Filter          : -

--------------------------------------------

Destination     : -
Rspan Vlan      : 903
Admin Source    : INBAND
Oper Source     : INBAND
Direction       : transmit
Incoming Packets: -
Learning        : -
Multicast       : disabled
Filter          : -

--------------------------------------------

Destination     : Port 7/1
Rspan Vlan      : 902
Admin Source    : -
Oper Source     : -
Direction       : -
Incoming Packets: enabled
Learning        : -
Multicast       : -
Filter          : -
Console> (enable)
```

Related Commands

set rspan

show running-config

To display the configuration information currently running on the switch or the configuration for a specific ACL, use the **show running-config** command.

show running-config [**system** | *mod_num*] [**all**]

show running-config acl location

show running-config qos acl {*acl_name*| **all**}

Syntax Description

system	(Optional) Displays current system configuration.
mod_num	(Optional) Number of the module.
all	(Optional) Specifies all modules and system configuration information, including the IP address.
acl location	Displays current ACL configuration information.
qos acl *acl_name*	Displays current QoS ACL configuration information for a specific ACL.
qos acl all	Displays current QoS ACL configuration information for all ACLs.

Defaults

The default displays only nondefault configurations.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can view the entire configuration by entering the **all** keyword.

Examples

This example shows how to display the nondefault system and module configuration:

```
Console> (enable) show running-config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
..............

..................
....................

..

begin
!
```

```
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Mon Jun 11 2001, 08:22:17
!
#version 6.3(0.56)PAN
!

!
#!
#vtp
set vtp domain dan
set vtp mode transparent
set vlan 1 name default type ethernet mtu 1500 said 100001 state active
set vlan 1002 name fddi-default type fddi mtu 1500 said 101002 state active
set vlan 1004 name fddinet-default type fddinet mtu 1500 said 101004 state acti
e stp ieee
set vlan 1005 name trnet-default type trbrf mtu 1500 said 101005 state active s
p ibm
set vlan 2,10-11
set vlan 1003 name token-ring-default type trcrf mtu 1500 said 101003 state act
ve mode srb aremaxhop 7 stemaxhop 7 backupcrf off
!
#ip
set interface sc0 1 172.20.52.19/255.255.255.224 172.20.52.31

set ip route 0.0.0.0/0.0.0.0         172.20.52.1
!
#set boot command
set boot config-register 0x10f
set boot system flash bootflash:cat6000-sup2-d.6-3-0-56-PAN.bin
set boot system flash bootflash:cat6000-sup2-d.6-3-0-54-PAN.bin
set boot system flash bootflash:cat6000-sup2-d.6-3-0-46-PAN.bin
set boot system flash bootflash:cat6000-sup2-d.6-3-0-44-PAN.bin
set boot system flash bootflash:
!
#qos
set qos wred 1p2q2t tx queue 1 60:80 80:100
set qos wred 1p2q2t tx queue 2 60:80 80:100
set qos wred 1p3q1t tx queue 1 80:100
set qos wred 1p3q1t tx queue 2 80:100
set qos wred 1p3q1t tx queue 3 80:100
!
#mmls nonrpf
set mmls nonrpf timer 0
!
#security ACLs
clear security acl all
#pbf set
set pbf mac 00-01-64-61-39-c3
#adj set
set security acl adjacency ADJ2 10 00-00-00-00-00-0a 00-00-00-00-00-0b mtu 9600
#
commit security acl all
!
# default port status is enable
!
!
#module 1 empty
!
#module 2 : 2-port 1000BaseX Supervisor
!
#module 3 : 48-port 10/100BaseTX Ethernet
set vlan 10   3/1
set vlan 11   3/2
!
#module 4 empty
!
#module 5 : 0-port Switch Fabric Module
!
#module 6 empty
!
#module 7 empty
!
#module 8 empty
!
#module 9 empty
!
#module 15 empty
!
#module 16 empty
end
Console> (enable)
```

This example shows how to display the nondefault system configuration for module 3:

```
Console> (enable) show running-config 3
This command shows non-default configurations only.
Use 'show config <mod> all' to show both default and non-default configurations.
....................
begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Mon Jun 11 2001, 08:33:25
!
# default port status is enable
!
!
#module 3 : 48-port 10/100BaseTX Ethernet
set vlan 10   3/1
set vlan 11   3/2
end
Console> (enable)
```

Related Commands

clear config
show startup-config
write

show security acl

To display the contents of the VACL that are currently configured or last committed to NVRAM and hardware, use the **show security acl** command.

show security acl

show security acl [**editbuffer**]

show security acl info {*acl_name* | **adjacency** | **all**} [**editbuffer** [*editbuffer_index*] | **statistics** [*ace_index*]]

Syntax Description

editbuffer	(Optional) Displays the VACLs in the edit buffer.
info	Displays the contents of a VACL that were last committed to NVRAM and hardware.
acl_name	Name of the VACL to be displayed.
adjacency	Displays adjacency information.
all	Displays all ACL information.
editbuffer_index	(Optional) Name of the edit buffer index.
statistics	(Optional) Displays statistics for the specified ACL.
ace_index	(Optional) Name of the ACE index in the ACL list.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

In the output for the **show security acl** command, the (Statistics) field displays whether or not statistics are enabled for a specific ACL or VLAN. The field displays the following:

- Disable—Statistics are not enabled on the ACL.
- Enable—Statistics are enabled on the ACL.
- The numbers show the VLANS where per-VLAN statistics are enabled (“2-3” in the first example).

In the output for the **show security acl info** {*acl_name* | **all**} command, the redirect port for redirect entries is shown with an asterisk (*) next to it.

Examples

This example shows how to display the name and type of the VACLs currently configured:

```
Console> show security acl
ACL                               Type     VLANS      (Statistics)
```

```
--------------------------------  ----    -----     -------------------
ip1                               IP      2-9       (2-3 Enable )
ip2                               IP       10       ( Disable )
ip3                               IP       11       ( Disable )
Console>
```

This example shows how to display VACLs in the edit buffer:

```
Console> show security acl editbuffer
ACL                               Type Status
--------------------------------  ---- -------------------
ip1                               IP   Committed
ip2                               IP   Committed
ip3                               IP   Committed
ipx1                              IPX  Committed
ipx2                              IPX  Committed
ipx3                              IPX  Committed
mac2                              MAC  Committed
iplast                            IP   Committed
Console>
```

This example shows how to display the configuration for a specified VACL last committed to NVRAM and hardware:

```
Console> show security acl info ip1
set security acl ip ip1
---------------------------------------------------
1. permit any
Console>
```

This example shows how to display the configuration for all VACLs last committed to NVRAM and hardware:

```
Console> show security acl info all
set security acl adjacency a_1
---------------------------------------------------
1. 2 00-0a-0a-0a-0a-0a

set security acl adjacency a_2
---------------------------------------------------
1. 2 00-0a-0a-0a-0a-0b

set security acl adjacency a_3
---------------------------------------------------
1. 2 00-0a-0a-0a-0a-0c

set security acl adjacency a_4
---------------------------------------------------
1. 2 00-0a-0a-0a-0a-0d

set security acl adjacency b_1
---------------------------------------------------
1. 1 00-20-20-20-20-20

set security acl adjacency b_2
---------------------------------------------------
1. 1 00-20-20-20-20-21

set security acl adjacency b_3
---------------------------------------------------
1. 1 00-20-20-20-20-22

set security acl adjacency b_4
---------------------------------------------------
```

```
1. 1 00-20-20-20-20-23


set security acl ip ip1
---------------------------------------------------
arp permit
1. redirect a_1 ip host 44.0.0.1 host 43.0.0.1
2. redirect a_2 ip host 44.0.0.2 host 43.0.0.2
3. redirect a_3 ip host 44.0.0.3 host 43.0.0.3
4. redirect a_4 ip host 44.0.0.4 host 43.0.0.4
5. permit ip any any

set security acl ip ip2
---------------------------------------------------
arp permit
1. redirect b_1 ip host 43.0.0.1 host 44.0.0.1
2. redirect b_2 ip host 43.0.0.2 host 44.0.0.2
3. redirect b_3 ip host 43.0.0.3 host 44.0.0.3
4. redirect b_4 ip host 43.0.0.4 host 44.0.0.4
5. permit ip any any


Console>
```

This example shows how to display the contents of the VACL edit buffer:

```
Console> show security acl info ip1 editbuffer
set security acl ip ip1
---------------------------------------------------
1. permit any

ACL Status:Committed
Console>
```

The output of this example shows which port is the redirect port for redirect entries. The redirect port has an asterisk (*) next to it:

```
Console> (enable) show security acl info all
set security acl ip ip1
---------------------------------------------------
arp permit
1. redirect 3/1* ip any any
2. redirect 3/6 ip any any
```

This example shows how to display statistics for the specified ACL:

```
Console> show security acl info ACL1 statistics
Vlan: 1
set security acl ip ACL1 statistics
---------------------------------------------------
arp permit in: 132 out: 132
1. permit ip any any
2. permit ip any any statistics  in: 0 out: 0

Console>
```

Related Commands

clear security acl
commit
rollback

show security acl arp-inspection

To display Address Resolution Protocol (ARP) inspection information, use the **show security acl arp-inspection** command.

show security acl arp-inspection config

show security acl arp-inspection statistics [*acl_name*]

Syntax Description

config	Displays ARP inspection configuration information.
statistics	Displays the number of packets permitted and denied by the ARP inspection task.
acl_name	(Optional) ACL name.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the global ARP inspection configuration:

```
Console> show security acl arp-inspection config
ARP Inspection match-mac feature is enabled.
Address-validation feature is disabled.
Console>
```

This example shows how to display global ARP inspection statistics:

```
Console> show security acl arp-inspection statistics
ARP Inspection statistics
Packets forwarded = 0
Packets dropped = 0
RARP packets (forwarded) = 0
Packets for which Match-mac failed = 0
Packets for which Address Validation failed = 0
IP packets dropped = 0
Console>
```

Related Commands

set security acl arp-inspection

show security acl capture-ports

To display the capture port list, use the **show security acl capture-ports** command.

show security acl capture-ports

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display capture port list entries:

```
Console> (enable) show security acl capture-ports
ACL Capture Ports: 1/2,2/2
Console> (enable)
```

Related Commands

clear security acl capture-ports
set security acl capture-ports

show security acl cram

To display information about CRAM, use the **show security acl cram** command.

show security acl cram

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal

Usage Guidelines

This command displays whether or not the automatic execution of the CRAM feature is enabled. It also shows the last time the CRAM feature was successfully executed.

Examples

This example shows how display information about the CRAM feature:

```
Console> show security acl cram
Cram auto mode is enabled. Timer is 300.
Cram last run on Fri Jun 18 2004, 10:06:29
Security ACL mask usage before: 0.17%
Security ACL mask usage after: 0.12%
Total number of cram executions = 2
Console>
```

Related Commands

clear security acl cram
set security acl cram

show security acl downloaded-acl

To display information about downloaded ACLs, use the **show security acl downloaded-acl** command.

show security acl downloaded-acl

show security acl downloaded-acl user-map

show security acl downloaded-acl port [*mod/port*]

show security acl downloaded-acl ipphone-map

Syntax Description

user-map	Displays the mapping between the user and the downloaded ACL.
port	Displays the downloaded ACL information for a given port.
mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
ipphone-map	Displays the IP phone mapping information for ports with downloaded ACLs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Enabled.

Usage Guidelines

This command displays a summary of downloaded ACLs. This command also shows the date and time each ACL was downloaded. You can also display the mapping between the user and downloaded ACLs, the downloaded ACL information for a given port, and the IP phone mapping information for ports with downloaded ACLs.

Examples

This example shows how to display downloaded ACL information:

```
Console> (enable) show security acl downloaded-acl all
Downloaded ACL Summary:
    ACL Name                         Date/Time
--------------------------------------------------------------
  1.#ACSACL#-IP-test_acl2-44cf4bcd    Tue Aug 1 2006, 03:14:54
  2.#ACSACL#-IP-1pipacl-44a100c7      Tue Aug 1 2006, 03:04:56
```

This example shows detailed information about a downloaded ACL:

```
Console> (enable) show security acl downloaded-acl #ACSACL#-IP-test_acl2-44cf4bcd
Downloaded ACE's for #ACSACL#-IP-test_acl2-44cf4bcd :
  1. permit ip any host 10.1.1.1
  2. permit tcp any host 100.1.1.3
  3. permit udp any host 10.76.88.34
  4. deny ip any host 9.6.5.7
  5. deny tcp any host 2.3.4.5
  6. deny udp any host 3.4.5.5
  7. permit icmp any host 100.1.1.5
```

This example shows how to display mapping information about a downloaded ACL:

```
Console> (enable) show security acl downloaded-acl user-map
Downloaded ACL User Map:
ACL Name : #ACSACL#-IP-test_acl2-44cf4bcd
User Count : 1
Num of Aces : 7
     Ip Address                          mNo/pNo     Feature
------------------------------------------------------------
  1. 10.1.1.5                              3/13      dot1x
```

This example shows how to display host information on a port:

```
Console> (enable) show security acl downloaded-acl port 3/45
Port  IP Address       Feature    Downloaded ACL
----- ---------------- ---------- ----------------------------
3/45  9.6.2.233        dot1x      #ACSACL#-IP-testacl-44c7197a
```

This example shows how to display host information on a port:

```
Port  IP Address
----- ------------------------------
3/45  10.1.1.5
```

Related Commands

set security acl ip

show security acl feature ratelimit

To display the rate at which packets are sent by security ACL features to the supervisor engine for processing and to display the features that share this rate limit value, use the **show security acl feature ratelimit** command.

show security acl feature ratelimit

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display rate limit information:

```
Console> show security acl feature ratelimit
Rate limit value in packets per second = 1000
Features set for rate limiting = ARP Inspection, DHCP Snooping, and Dot1x DHCP
```

Related Commands

set security acl feature ratelimit

show security acl log

To display VACL log information, use the **show security acl log** command.

show security acl log config

show security acl log flow *protocol* {*src_ip_spec* | *dest_ip_spec*} [**vlan** *vlan_num*]

show security acl log flow {**ip**} {*src_ip_spec* | *dest_ip_spec*} [**vlan** *vlan_num*]

show security acl log flow {**icmp** | **1**} {*src_ip_spec* | *dest_ip_spec*} [*icmp_type* [*icmp_code*]] [**vlan** *vlan_num*]

show security acl log flow {**tcp** | **6**} {{*src_ip_spec* [*operator port* [*port*]]} | {*dest_ip_spec* [*operator port* [*port*]]}} [**vlan** *vlan_num*]

show security acl log flow {**udp** | **17**} *src_ip_spec* [*operator port* [*port*]] *dest_ip_spec* [*operator port* [*port*]] [**vlan** *vlan_num*]

show security acl log flow arp [**host** *IP_Address* [**vlan** *vlan_num*]]

Syntax Description

config	Displays the VACL log configuration information including the maximum number of the flow pattern and redirect rate.
flow	Displays the flow information specified by the arguments since its last syslog report.
protocol	Keyword or number of an IP protocol; valid numbers are from 0 to 255 representing an IP protocol number. See the "Usage Guidelines" section for the list of valid keywords.
src_ip_spec	Source IP address and the source mask. See the "Usage Guidelines" section for the format.
dest_ip_spec	Destination IP address and the destination mask. See the "Usage Guidelines" section for the format.
vlan *vlan_num*	(Optional) Number of the VLAN to be displayed; valid values are from 1 to 4094.
ip	Matches any IP packets.
icmp | **1**	Matches ICMP packets.
icmp_type	(Optional) ICMP message type name or a number; valid values are from 0 to 255. See the "Usage Guidelines" section for a list of valid names.
icmp_code	(Optional) ICMP message code name or a number; valid values are from 0 to 255. See the "Usage Guidelines" section for a list of valid names.
tcp | **6**	Matches TCP packets.
operator	(Optional) Operands; valid values include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).
port	(Optional) Number or name of a TCP or UDP port; valid port numbers are from 0 to 65535. See the "Usage Guidelines" section for a list of valid names.
udp | **17**	Matches UDP packets.
arp	Displays all logged ARP packets.
host *IP_Address*	(Optional) Specifies the IP address of an IP host.

8.6 EFT Copy

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is supported on systems configured with Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2) only.

Configurations you make by entering this command are saved to NVRAM and hardware only after you enter the **commit** command. Enter ACEs in batches and then enter the **commit** command to save them in NVRAM and in the hardware.

When you specify the source IP address and the source mask, use the form *source_ip_address source_mask* and follow these guidelines:

- The *source_mask* is required; 0 indicates a care bit, 1 indicates a don't-care bit.
- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0.

Valid *protocol* keywords include **icmp** (1), **ip**, **ipinip** (4), **tcp** (6), **udp** (17), **igrp** (9), **eigrp** (88), **gre** (47), **nos** (94), **ospf** (89), **ahp** (51), **esp** (50), **pcp** (108), and **pim** (103). The IP number is displayed in parentheses. Use the keyword **ip** to match any Internet Protocol.

ICMP packets that are matched by ICMP message type can also be matched by the ICMP message code.

Valid names for *icmp_type* and *icmp_code* are administratively-prohibited, alternate-address, conversion-error, dod-host-prohibited, dod-net-prohibited, echo, echo-reply, general-parameter-problem, host-isolated, host-precedence-unreachable, host-redirect, host-tos-redirect, host-tos-unreachable, host-unknown, host-unreachable, information-reply, information-request, mask-reply, mask-request, mobile-redirect, net-redirect, net-tos-redirect, net-tos-unreachable, net-unreachable, network-unknown, no-room-for-option, option-missing, packet-too-big, parameter-problem, port-unreachable, precedence-unreachable, protocol-unreachable, reassembly-timeout, redirect, router-advertisement, router-solicitation, source-quench, source-route-failed, time-exceeded, timestamp-reply, timestamp-request, traceroute, ttl-exceeded, and unreachable.

If the operator is positioned after the source and source-wildcard, it must match the source port. If the operator is positioned after the destination and destination-wildcard, it must match the destination port. The range operator requires two port numbers. All other operators require one port number.

TCP port names can be used only when filtering TCP. Valid names for TCP ports are bgp, chargen, daytime, discard, domain, echo, finger, ftp, ftp-data, gopher, hostname, irc, klogin, kshell, lpd, nntp, pop2, pop3, smtp, sunrpc, syslog, tacacs-ds, talk, telnet, time, uucp, whois, and www.

UDP port names can be used only when filtering UDP. Valid names for UDP ports are biff, bootpc, bootps, discard, dns, dnsix, echo, mobile-ip, nameserver, netbios-dgm, netbios-ns, ntp, rip, snmp, snmptrap, sunrpc, syslog, tacacs-ds, talk, tftp, time, who, and xdmcp.

The number listed with the protocol type is the layer protocol number (for example, **udp | 17**).

Examples

This example shows how to display VACL log information:

```
Console> (enable) show security acl log config
VACL LOG Configration
-------------------------------------------------------------
Max Flow Pattern     : 512
Redirect Rate (pps) : 1000
Console> (enable)
```

This example shows how to display the flow information:

```
Console> (enable) show security acl log flow ip vlan 1
Total matched entry number = 1
Entry No. #1, IP Packet
----------------------------------------
Vlan Number             : 1
Mod/Port Number         : 2/1
Source IP address       : 21.0.0.0
Destination IP address : 255.255.255.255
TCP Source port         : 2000
TCP Destination port    : 3000
Received Packet Number : 10
Console> (enable)
```

Related Commands

clear security acl log flow
set security acl log

show security acl map

To display ACL-to-VLAN or ACL-to-port mapping for a specific ACL, port, or VLAN, use the **show security acl map** command.

show security acl map {**config** | **runtime**} {*acl_name* | *mod/port* | *vlan* | **all** | **all-vlans** | **all-ports**}

Syntax Description

config	Displays ACL mapping that is stored in NVRAM.
runtime	Displays ACL mapping that is programmed in hardware.
acl_name	Name of the ACL to be displayed.
mod/port	Number of the module and the port on the module.
vlan	Number of the VLAN to be displayed; valid values are from 1 to 4094.
all	Displays all ACL mappings.
all-vlans	Displays all VACL mappings.
all-ports	Displays all PACL mappings.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the mappings of a specific ACL:

```
Console> show security acl map IPACL1
ACL IPACL1 is mapped to VLANs:
1
Console>
```

This example shows how to display the mappings of a specific VLAN:

```
Console> show security acl map 1
VLAN 1 is mapped to IP ACL IPACL1.
VLAN 1 is mapped to IPX ACL IPXACL1.
VLAN 1 is mapped to MAC ACL MACACL1.
Console>
```

This example shows how to display all ACL mappings that are stored in NVRAM:

```
Console> show security acl map config all
ACL Name                         Type Ports/Vlans
-------------------------------- ---- --------------
ipacl1                           IP   11
ipacl2                           IP   3/1
Console>
```

This example shows how to display ACL mappings that are stored in NVRAM for all ports:

```
Console> show security acl map config all-ports
ACL Name                         Type Ports
-------------------------------- ---- --------------
ipacl2                           IP   3/1
Console>
```

This example shows how to display the ACL mapping that is programmed in hardware for a specific port:

```
Console> show security acl map runtime 3/1
Port 3/1 is mapped to IP ACL ipacl1.
Console>
```

This example shows how to display the ACL mapping for a specific VLAN:

```
Console> show security acl map runtime 1
Vlan ACL name                         Type
---- -------------------------------- ----
   1 ipacl2                           IP
Console>
```

Related Commands

clear security acl map
commit
rollback
set security acl map

show security acl resource-usage

To display VACL management information, use the **show security acl resource-usage** command.

show security acl resource-usage

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The switch interface mapping table that associates an interface (for example, VLANs) into flows programmed in TCAM.

Hardware resources are used to calculate Layer 4 port operation; for example, if you enter the **permit tcp any lt 20 host 1.2.3.4 gt 30** command, "**lt 20**" and "**gt 30**" are the Layer 4 port operation.

Examples

This example shows how to display VACL management information:

```
Console> (enable) show security acl resource-usage
ACL resource usage:
ACL storage (mask/value) :(50%/19%)
ACL to switch interface mapping table :2%
ACL layer 4 port operators :0%
Console> (enable)
```

Table 2-86 describes the possible fields in the **show security acl resource-usage** command output.

Table 2-86 show security acl resource-usage Command Output Fields

Field	Description
ACL storage (mask/value)	Status of mask entry usage, where mask is the percentage of mask entries used, and value is the percentage of value entries currently used.
ACL to switch interface mapping table	Percentage of ACL to switch interface mapping table usage.
ACL layer 4 port operators	Percentage of ACL Layer 4 port operators.

Related Commands

clear security acl
commit
rollback

show security acl tcam interface

To display the TCAM details for a specified VLAN, use the **show security acl tcam interface** command.

show security acl tcam interface *vlan*

Syntax Description

vlan	Number of the VLAN; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display TCAM details for the specified VLAN:

```
Console> (enable) show security acl tcam interface 1
Input
0. permit arp (matches 45745)
1. deny (l3) tcp any any fragment (matches 0)
2. deny (l3) ip host 21.0.0.130 any (matches 0)
3. deny (l3) udp 1.2.2.0 0.0.0.255 any (matches 0)
4. deny (l3) tcp any any 2001 (matches 0)
5. deny (l3) ip host 21.0.0.128 any (matches 0)
6. deny ip any any (matches 3)


Output
0. permit arp (matches 0)
1. deny (l3) tcp any any fragment (matches 0)
2. deny (l3) ip host 21.0.0.130 any (matches 0)
3. deny (l3) udp 1.2.2.0 0.0.0.255 any (matches 0)
4. deny (l3) tcp any any 2001 (matches 0)
5. deny (l3) ip host 21.0.0.128 any (matches 0)
6. deny (l3) ip any any (matches 0)
Console> (enable)
```

Table 2-87 describes the possible fields in the **show security acl tcam interface** command output.

Table 2-87 show security acl tcam interface Command Output Fields

Field	Description
deny (l3)	Layer 3 traffic is denied; Layer 2 traffic is permitted.
redirect (l3)	Only Layer 3 traffic is redirected.
bridge	Traffic that hits this entry is bridged.
redirect (adj)	Traffic is rewritten by the adjacency information.

show snmp

To display SNMP information, use the **show snmp** command.

show snmp [**noalias**]

Syntax Description

noalias	(Optional) Keyword that forces the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal and privileged.

Usage Guidelines

If you enter **show snmp** in privileged mode, the output display includes information for the read-only, the read-write, and the read-write-all community strings. If you enter **show snmp** in normal mode, the display includes only information for the read-only community string.

Examples

This example shows SNMP information when you enter the **show snmp** command in normal mode:

```
Console> show snmp
RMON:                       Disabled
Extended RMON Netflow Enabled : None.
Memory usage limit for new RMON entries: 85 percent
EngineId:00:00:00:09:00:01:64:41:5e:00:00:00
Chassis Alias:my chassis
Traps Enabled:
None
Port Traps Enabled: None

Community-Access     Community-String
----------------     --------------------
read-only            public

Trap-Rec-Address                           Trap-Rec-Community
----------------------------------------   --------------------
192.122.173.42                             public
Console>
```

This example shows SNMP information when you enter the **show snmp** command in privileged mode:

```
Console> (enable) show snmp
SNMP:Enabled
RMON:Disabled
Extended RMON:Extended RMON module is not present
Extended RMON Netflow:Disabled
Extended RMON Vlanmode:Disabled
Extended RMON Vlanagent:Disabled
EngineId:00:00:00:09:00:01:64:41:5e:00:00:00
```

```
Chassis Alias:my chassis
Traps Enabled:
None
Port Traps Enabled:None
Community-Access Community-String
---------------- --------------------
read-only        public
read-write       private
read-write-all   secret
Trap-Rec-Address Trap-Rec-Community Trap-Rec-Port Trap-Rec-Owner Trap-Rec-Index
---------------- ------------------ ------------- -------------- --------------
Console> (enable)
```

Table 2-88 describes the possible fields (depending on the port type queried) in the **show snmp** command output.

Table 2-88 show snmp Command Output Fields

Field	Description
SNMP	Status of whether SNMP processing is enabled or disabled.
RMON	Status of whether RMON is enabled or disabled.
Extended RMON	Status of whether extended RMON is enabled or disabled.
Extended RMON Netflow	Status of whether extended RMON Netflow is enabled or disabled.
Extended RMON Vlanmode	Status of whether extended RMON VLAN mode is enabled or disabled.
Extended RMON Vlanagent	Status of whether extended RMON VLAN agent is enabled or disabled.
EngineId	SNMP engine identifier.
Chassis Alias	Chassis entPhysicalAlias.
Traps Enabled	Trap types that are enabled.
Port Traps Enabled	Set of ports whose linkup/linkdown trap is enabled.
Community-Access	Configured SNMP communities.
Community-String	SNMP community strings associated with each SNMP community.
Trap-Rec-Address	IP address or IP alias of trap receiver hosts.
Trap-Rec-Community	SNMP community string used for trap messages to the trap receiver.

Related Commands

set snmp
set snmp chassis-alias
set snmp rmon
set snmp trap

show snmp access

To display SNMP access information, use the **show snmp access** command.

show snmp access [**volatile** | **nonvolatile** | **read-only**]

show snmp access [**-hex**] *groupname* **security-model** {**v1** | **v2c**}

show snmp access [**-hex**] *groupname* **security-model v3** {**noauthentication** | **authentication** | **privacy**} [**context** [**-hex**] *contextname*]

Syntax Description

volatile	(Optional) Displays information for volatile storage types.
nonvolatile	(Optional) Displays information for nonvolatile storage types.
read-only	(Optional) Displays information for read-only storage types.
-hex	(Optional) Displays *groupname*, *username*, and *contextname* as a hexadecimal character.
groupname	Name of the SNMP group or collection of users who have a common access policy.
security-model v1 | **v2c** | **v3**	Specifies security model v1, v2c, or v3.
noauthentication	Displays information for security models not set to use authentication protocol.
authentication	Displays information for authentication protocol.
privacy	Displays information regarding messages sent on behalf of the user that are protected from disclosure.
context *contextname*	(Optional) Specifies the name of a context string.

Defaults

The default storage type is **volatile**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for the *groupname* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

If you do not enter a context name, a NULL context string is used.

There are three versions of SNMP:

- Version 1 (SNMPv1)—This is the initial implementation of SNMP. Refer to RFC 1157 for a full description of functionality.
- Version 2 (SNMPv2c)—The second release of SNMP, described in RFC 1902, has additions and enhancements to data types, counter size, and protocol operations.

- Version 3 (SNMPv3)—This is the most recent version of SNMP and is fully described in RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575. SNMPv3 has significant enhancements to administration and security.

The SNMP functionality on the Catalyst enterprise LAN switches for SNMP v1 and SNMP v2c remains intact; however, the functionality has greatly expanded for SNMPv3. Refer to the “Configuring SNMP” chapter of the *Catalyst 6500 Series Switch Software Configuration Guide* for more information on SNMPv3.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display all SNMP access information:

```
Console> (enable) show snmp access
Group Name:defaultROgroup
Context:
Security Model:v1
Security Level:noauthentication
Context Match:vlan-1
Read View:defaultAdminView
Write View:
Notify View:defaultAdminView
Storage Type:read-only
Row Status:active

Group Name:defaultROgroup
Context:
Security Model:v2c
Secuirty Level:noauthentication
Context Match:vlan-55
Read View:defaultAdminView
Write View:
Notify View:defaultAdminView
Storage Type:read-only
Row Status:active
```

Related Commands

clear snmp access
set snmp access
show snmp context

show snmp access-list

To display SNMP access list numbers and corresponding IP addresses and IP masks, use the **show snmp access-list** command.

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display SNMP access list numbers and corresponding IP addresses and IP masks:

```
Console> show snmp access-list
Access-Number   IP-Addresses/IP-Mask
-------------   -------------------------
1               172.20.60.100/255.0.0.0
                1.1.1.1/-
2               172.20.60.7/-
                2.2.2.2/-
3               2.2.2.2/155.0.0.0
4               1.1.1.1/2.1.2.4
                2.2.2.2/-
                2.2.2.5/-
```

Related Commands

clear snmp access-list
set snmp access-list

show snmp buffer

To display the number of SNMP packets that can be saved in the SNMP UDP socket receive buffer, use the **show snmp buffer** command.

show snmp buffer

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command

Command Modes

Normal

Examples

This example shows how to display the number of SNMP socket packets that can be saved in the SNMP UDP socket receive buffer:

```
Console> show snmp buffer
SNMP socket receive buffer:40 packets
Console>
```

Related Commands

set snmp buffer

show snmp community

To display SNMP context information, use the **show snmp community** command.

show snmp community

show snmp community [**read-only** | **volatile** | **nonvolatile**]

show snmp community index [**-hex**] {*index name*}

Syntax Description

read-only	(Optional) Specifies that the community is defined as read only.
volatile	(Optional) Specifies the community type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies the community type is defined as persistent memory and the content remains after the device is turned off and on again.
index	Specifies the index of community names.
-hex	(Optional) Displays *index name* as a hexadecimal character.
index name	Name of the community index.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal and privileged.

Usage Guidelines

If you enter the **show snmp community** command in privileged mode, the output display includes information for the read-only, the read-write, and the read-write-all community strings. If you enter the **show snmp community** command in normal mode, the display includes only information for the read-only community string.

Examples

This example shows the output when you enter the **show snmp community** command for the read-only community string in normal mode:

```
Console> show snmp community
Community Index: sysCommunityRo.0
Community Name: public
Security Name: public
Context Name:
Transport Tag:
Storage Type: read-only
Row Status: active
Console>
```

This example shows the display output when you enter the **show snmp community** command for the read-only, the read-write, and the read-write-all community strings in privileged mode:

```
Console> (enable) show snmp community
Community Index: sysCommunityRo.0
Community Name: public
Security Name: public
Context Name:
Transport Tag:
Storage Type: read-only
Row Status: active

Community Index: sysCommunityRw.0
Community Name: private
Security Name: private
Context Name:
Transport Tag:
Storage Type: read-only
Row Status: active

Community Index: sysCommunityRwa.0
Community Name: secret
Security Name: secret
Context Name:
Transport Tag:
Storage Type: read-only
Row Status: active

Console> (enable)
```

Related Commands

clear snmp community
set snmp community

show snmp context

To display SNMP context information, use the **show snmp context** command.

show snmp context

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display SNMP context information:

```
Console> (enable) show snmp context
Index Context
----- --------
    0
    1 vlan-1
    2 vlan-55
    3 vlan-1002
    4 vlan-1003
    5 vlan-1004
    6 vlan-1005
Console> (enable)
```

Related Commands

clear snmp access
set snmp access
show snmp access

show snmp counters

To display SNMP counter information, use the **show snmp counters** command.

show snmp counters [**v3** | {{*mod/port*} {**dot1d** | **dot3** | **hcrmon** | **ifmib** | **rmon**}}]

Syntax Description

v3	(Optional) Specifies SNMPv3 counters.
mod/port	(Optional) Module number and port number.
dot1d	Specifies dot1d counters.
dot3	Specifies dot3 counters.
hcrmon	Specifies HCRMON counters.
ifmib	Specifies if-MIB counters.
rmon	Specifies RMON counters.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal

Usage Guidelines

There are three versions of SNMP:

- Version 1 (SNMPv1)—This is the initial implementation of SNMP. Refer to RFC 1157 for a full description of functionality.
- Version 2 (SNMPv2c)—The second release of SNMP, described in RFC 1902, has additions and enhancements to data types, counter size, and protocol operations.
- Version 3 (SNMPv3)—This is the most recent version of SNMP and is fully described in RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575. SNMPv3 has significant enhancements to administration and security.

The SNMP functionality on the Catalyst enterprise LAN switches for SNMP v1 and SNMP v2c remains intact; however, the functionality has greatly expanded for SNMPv3. Refer to the "Configuring SNMP" chapter of the *Catalyst 6500 Series Switch Software Configuration Guide* for more information on SNMPv3.

Examples

This example shows how to display all SNMP counters:

```
Console> show snmp counters
mib2 SNMP group counters:
snmpInPkts                  = 13993
snmpOutPkts                 = 13960
snmpInBadVersions           = 0
snmpInBadCommunityNames     = 33
snmpInBadCommunityUses      = 0
```

```
snmpInASNParseErrs           = 0
snmpInTooBigs                = 0
snmpInNoSuchNames            = 0
snmpInBadValues              = 0
snmpInReadOnlys              = 0
snmpInGenErrs                = 0
snmpInTotalReqVars           = 61747
snmpInTotalSetVars           = 0
snmpInGetRequests            = 623
snmpInGetNexts               = 13337
snmpInSetRequests            = 0
snmpInGetResponses           = 0
snmpInTraps                  = 0
snmpOutTooBigs               = 0
snmpOutNoSuchNames           = 230
snmpOutBadValues             = 0
snmpOutGenErrs               = 0
snmpOutGetRequests           = 0
snmpOutGetNexts              = 0
snmpOutSetRequests           = 0
snmpOutGetResponses          = 13960
snmpOutTraps                 = 0
Console>
```

Table 2-89 describes the fields in the **show snmp counters** command output.

Table 2-89 show snmp counters Command Output Fields

Field	Description
snmpInPkts	Number of messages delivered to the SNMP entity from the transport service.
snmpOutPkts	Number of SNMP messages passed from the SNMP protocol entity to the transport service.
snmpInBadVersions	Number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version.
snmpInBadCommunityNames	Number of SNMP messages delivered to the SNMP entity that used an SNMP community name not known to said entity.
snmpInBadCommunityUses	Number of SNMP messages delivered to the SNMP entity that represented an SNMP operation not allowed by the SNMP community named in the message.
snmpInASNParseErrs	Number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
snmpInTooBigs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “tooBig.”
snmpInNoSuchNames	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “noSuchName.”
snmpInBadValues	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “badValue.”
snmpInReadOnlys[1]	Number of valid SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “readOnly.”
snmpInGenErrs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “genErr.”

Table 2-89 show snmp counters Command Output Fields (continued)

Field	Description
snmpInTotalReqVars	Number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
snmpInTotalSetVars	Number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
snmpInGetRequests	Number of SNMP Get-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInPkts	Number of messages delivered to the SNMP entity from the transport service.
snmpOutPkts	Number of SNMP messages passed from the SNMP protocol entity to the transport service.
snmpInBadVersions	Number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version.
snmpInBadCommunityNames	Number of SNMP messages delivered to the SNMP entity that used an SNMP community name not known to said entity.
snmpInBadCommunityUses	Number of SNMP messages delivered to the SNMP entity that represented an SNMP operation not allowed by the SNMP community named in the message.
snmpInASNParseErrs	Number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
snmpInTooBigs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “tooBig.”
snmpInNoSuchNames	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “noSuchName.”
snmpInBadValues	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “badValue.”
snmpInGenErrs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “genErr.”
snmpInTotalReqVars	Number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
snmpInTotalSetVars	Number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
snmpInGetRequests	Number of SNMP Get-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInGetNexts	Number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol entity.
snmpInSetRequests	Number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInGetResponses	Number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol entity.

Table 2-89 show snmp counters Command Output Fields (continued)

Field	Description
snmpInTraps	Number of SNMP Trap PDUs accepted and processed by the SNMP protocol entity.
snmpOutTooBigs	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as “tooBig.”
snmpOutNoSuchNames	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status as “noSuchName.”
snmpOutBadValues	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as “badValue.”
snmpOutGenErrs	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as “genErr.”
snmpOutGetRequests	Number of SNMP Get-Request PDUs generated by the SNMP protocol entity.
snmpOutGetNexts	Number of SNMP Get-Next PDUs generated by the SNMP protocol entity.
snmpOutSetRequests	Number of SNMP Set-Request PDUs generated by the SNMP protocol entity.
snmpOutGetResponses	Number of SNMP Get-Response PDUs generated by the SNMP protocol entity.
snmpOutTraps	Number of SNMP Trap PDUs generated by the SNMP protocol entity.

[1] It is a protocol error to generate an SNMP PDU that contains the value “readOnly” in the error-status field. This object is provided as a means of detecting incorrect implementations of the SNMP.

This example shows how to display the SNMPv3 counters:

```
Console> show snmp counters v3
snmpv3 MPD statistics:
snmpUnknownSecurityModels     = 0
snmpInvalidMsgs               = 0
snmpUnknownPDUHandlers        = 0

snmpv3 TARGET statistics:
snmpUnavailableContexts       = 0
snmpUnknownContexts           = 0

snmpv3 USM statistics:
usmStatsUnsupportedSecLevels  = 0
usmStatsNotInTimeWindows      = 0
usmStatsUnknownUserNames      = 0
usmStatsUnknownEngineIDs      = 0
usmStatsWrongDigests          = 0
usmStatsDecryptionErrors      = 0
Console>
```

show snmp engineid

To display the SNMP local engine ID, use the **show snmp engineid** command.

show snmp engineid

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If the SNMP engine ID is cleared, the system automatically regenerates a local SNMP engine ID.

The SNMP engine and the SNMP entity have a one-to-one mapping. You can also identify the SNMP entity, which is represented as hexadecimal numbers only, and must be from 5 to 32 bytes long; for example, 00:00:00:09:0a:fe:ff:12:97:33:45:12.

Examples

This example shows how to display the SNMP engine ID:

```
Console> (enable) show snmp engineid
EngineId: 00:00:00:09:00:d0:00:4c:18:00
Engine Boots: 1234455
Console> (enable)
```

Table 2-90 describes the fields in the **show snmp engineid** command output.

Table 2-90 show snmp engineid Command Output Fields

Field	Description
EngineId	String identifying the name of the SNMP copy on the device.
Engine Boots	Number of times an SNMP engine has been started or reinitialized.

Related Commands

show snmp

show snmp group

To display the name of the SNMP group or collection of users who have a common access policy, use the **show snmp group** command.

show snmp group [**volatile** | **nonvolatile** | **read-only**]

show snmp group [**-hex**] {*groupname*} [**-hex**] **user** {*username*} [**security-model** {**v1** | **v2c** | **v3**}]

Syntax Description

volatile	(Optional) Specifies the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
read-only	(Optional) Specifies that the storage type is defined as read only.
-hex	(Optional) Displays *groupname* and *username* as a hexadecimal character.
groupname	Name of the SNMP group or collection of users who have a common access policy.
user *username*	Specifies the SNMP group username.
security-model v1 | **v2c** | **v3**	(Optional) Specifies security model v1, v2c, or v3.

Defaults

The default storage type is **volatile**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for the *groupname* and *username* (nonprintable delimiters for these parameters), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

There are three versions of SNMP:

- Version 1 (SNMPv1)—This is the initial implementation of SNMP. Refer to RFC 1157 for a full description of functionality.
- Version 2 (SNMPv2c)—The second release of SNMP, described in RFC 1902, has additions and enhancements to data types, counter size, and protocol operations.
- Version 3 (SNMPv3)—This is the most recent version of SNMP and is fully described in RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575. SNMPv3 has significant enhancements to administration and security.

The SNMP functionality on the Catalyst enterprise LAN switches for SNMP v1 and SNMP v2c remains intact; however, the functionality has greatly expanded for SNMPv3. Refer to the “Configuring SNMP” chapter of the *Catalyst 6500 Series Switch Software Configuration Guide* for more information on SNMPv3.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display the SNMP group:

```
Console> (enable) show snmp group
Security Model: v1
Security Name: public
Group Name: defaultROgroup
Storage Type: volatile
Row Status: active

Security Model: v1
Security Name: secret
Group Name: defaultRWALLgroup
Storage Type: volatile
Row Status: active

Security Model: v1
Security Name: private
Group Name: defaultRWgroup
Storage Type: volatile
Row Status: active

Security Model: v2c
Security Name: public
Group Name: defaultROgroup
Storage Type: volatile
Row Status: active
Console> (enable)
```

Table 2-91 describes the fields in the **show snmp group** command output.

Table 2-91 show snmp group Command Output Fields

Field	Description
Security Model	Security model used by the group.
Security Name	Security string definition.
Group Name	Name of the SNMP group or collection of users who have a common access policy.
Storage Type	Indicates whether the settings are volatile or nonvolatile.
Row Status	Status of the entry.

Related Commands

clear snmp group
set snmp group

8.6 EFT Copy

show snmp ifalias

To display SNMP interface aliases, use the **show snmp ifalias** command.

show snmp ifalias [*ifIndex*]

show snmp ifalias module *mod*

show snmp ifalias vlan [*vlan*]

show snmp ifalias channel

Syntax Description

ifIndex	(Optional) Number of the interface index.
module	Displays module interface aliases.
mod	Number of the module.
vlan	Displays VLAN interface aliases.
vlan	(Optional) Number of the VLAN.
channel	Displays channel interface aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not enter an interface index number, all interface aliases are displayed.

Related Commands

clear snmp ifalias
set snmp ifalias

show snmp inform

To display information about the SNMP version 3 inform request feature, use the **show snmp inform** command.

show snmp inform

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display information about the inform request feature:

```
Console> show snmp inform

Inform Pending Limit: 150
SNMPv3 inform counters:
---------------------------------
Total informs created : 1001
Total inform responsed: 100
Total inform in queue : 100
Total infrom removed  : 0
Total inform timeout  : 801

Console>
```

Related Commands

clear snmp inform
set snmp inform

8.6 EFT Copy

show snmp notify

To display the snmpNotifyTable configuration, use the **show snmp notify** command.

show snmp notify [**volatile** | **nonvolatile** | **read-only**]

show snmp notify [**-hex**] {*notifyname*}

Syntax Description

volatile	(Optional) Specifies the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
read-only	(Optional) Specifies that the storage type is defined as read only.
-hex	(Optional) Displays *notifyname* as a hexadecimal character.
notifyname	A unique identifier to index the snmpNotifyTable.

Defaults

The default storage type is **nonvolatile**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for the *notifyname* value (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display the SNMP notify information for a specific *notifyname* value:

```
Console> (enable) show snmp notify snmpV1Notification
Notify Name: snmpV1Notification
Notify Tag: snmpV1Trap
Notify Type: trap
Storage Type: volatile
Row Status: active
Console> (enable)
```

8.6 EFT Copy

Table 2-92 describes the fields in the **show snmp notify** command output.

Table 2-92 show snmp notify Command Output Fields

Field	Description
Notify Name	Unique identifier used to index the snmpNotifyTable.
Notify Tag	Name of the entry in the snmpNotifyTable.
Notify Type	Type of notification.
Storage Type	Storage type (volatile or nonvolatile).
Row Status	Status of the entry.

Related Commands

clear snmp notify
set snmp notify

show snmp rmonmemory

To display the memory usage limit in percentage, use the **show snmp rmonmemory** command.

show snmp rmonmemory

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The percentage value displayed indicates that you cannot create new RMON entries or restore entries from the NVRAM if the specified memory usage is exceeded.

Examples

This example shows how to display the RMON memory limit use:

```
Console> (enable) show snmp rmonmemory
85 percent
Console> (enable)
```

Related Commands

set snmp rmonmemory

show snmp targetaddr

To display the SNMP target address entries in the snmpTargetAddressTable, use the **show snmp targetaddr** command.

show snmp targetaddr [**volatile** | **nonvolatile** | **read-only**]

show snmp targetaddr [**-hex**] {*addrname*}

Syntax Description

volatile	(Optional) Specifies the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
read-only	(Optional) Specifies that the storage type is defined as read only.
-hex	(Optional) Displays *addrname* as a hexadecimal character.
addrname	Name of the target agent; the maximum length is 32 bytes.

Defaults

The default storage type is **nonvolatile**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for the *addrname* value (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display specific target address information in the snmpTargetAddressTable:

```
Console> (enable) show snmp targetaddr cisco
Target Address Name: cisco
IP Address: 170.0.25.1
UDP Port#: 165
Timeout: 100
Retry count: 5
Tag List: tag1 tag2 tag3
Parameters: jeorge
Storage Type: nonvolatile
Row Status: active
Console> (enable)
```

8.6 EFT Copy

Table 2-93 describes the fields in the **show snmp targetaddr** command output.

Table 2-93 show snmp targetaddr Command Output Fields

Field	Description
Target Address Name	Name of the target address.
IP Address	Target IP address.
UDP Port #	Number of the UDP port of the target host to use.
Timeout	Number of timeouts.
Retry count	Number of retries.
Tag List	Tags that point to target addresses to send notifications to.
Parameters	Entry in the snmpTargetParamsTable; the maximum length is 32 bytes.
Storage Type	Storage type (volatile or nonvolatile).
Row Status	Status of the entry.

Related Commands

clear snmp targetaddr
set snmp targetaddr

show snmp targetparams

To display the SNMP parameters used in the snmpTargetParamsTable when generating a message to a target, use the **show snmp targetparams** command.

show snmp targetparams [**volatile** | **nonvolatile** | **read-only**]

show snmp targetparams [**-hex**] {*paramsname*}

Syntax Description

volatile	(Optional) Specifies that the storage type is defined as temporary memory and that the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies the storage type is defined as persistent memory and that the content remains after the device is turned off and on again.
read-only	(Optional) Specifies that the storage type is defined as read only.
-hex	(Optional) Displays *paramsname* as a hexadecimal character.
paramsname	Name of the parameter in the snmpTargetParamsTable; the maximum length is 32 bytes.

Defaults

The default storage type is **volatile**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for the *paramsname* value (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display specific target parameter information in the snmpTargetParamsTable:

```
Console> (enable) show snmp targetparams snmpV1TrapParams
Target Parameter Name: snmpV1TrapParams
Message Processing Model: v1
Security Name: public
Security Level: noauthentication
Storage Type: volatile
Row Status: active
Console> (enable)
```

Table 2-94 describes the fields in the **show snmp targetparams** command output.

Table 2-94 show snmp targetparams Command Output Fields

Field	Description
Target Parameter Name	A unique identifier used to index the snmpTargetParamsTable.
Message Processing Model	Version number used by the Message Processing Model.
Security Name	Security string definition.
Security Level	Type of security level: • Authentication—The security level is set to use the authentication protocol. • Noauthentication—The security level is not set to use the authentication protocol.
Storage Type	Status of whether the settings are volatile or nonvolatile.
Row Status	Status of the entry.

Related Commands

clear snmp targetparams
set snmp targetparams

show snmp user

To display SNMP information for a specific user, use the **show snmp user** command.

show snmp user [**volatile** | **nonvolatile** | **read-only**]

show snmp user [**-hex**] {*user*} [**remote** {*engineid*}]

show snmp user summary

Syntax Description

volatile	(Optional) Specifies the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
read-only	(Optional) Specifies that the storage type is defined as read only.
-hex	(Optional) Displays *user* as a hexadecimal character.
user	Name of the SNMP user.
remote *engineid*	(Optional) Specifies the username on a remote SNMP engine.
summary	Specifies a summary of SNMP users.

Defaults

The default storage type is **nonvolatile**, and the local SNMP engine ID is used.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for the *user* value (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display specific user information:

```
Console> (enable) show snmp user joe
EngineId: 00:11:22:33:44
User Name: joe
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: volatile
Row Status: active
Console> (enable)
```

8.6 EFT Copy

Table 2-95 describes the fields in the **show snmp user** command output.

Table 2-95 show snmp user Command Output Fields

Field	Description
EngineId	String identifying the name of the copy of SNMP on the device.
User Name	String identifying the name of the SNMP user.
Authentication Protocol	Type of authentication protocol.
Privacy Protocol	Type of privacy authentication protocol.
Storage Type	Status of whether the settings are volatile or nonvolatile.
Row Status	Status of the entry.

Related Commands

clear snmp user
set snmp user

show snmp view

To display the SNMP MIB view configuration, use the **show snmp view** command.

show snmp view [**volatile** | **nonvolatile** | **read-only**]

show snmp view [**-hex**] {*viewname*} {*subtree*}

Syntax Description

volatile	(Optional) Specifies the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Specifies the storage type is defined as persistent memory and the content remains after the device is turned off and on again.
read-only	(Optional) Specifies that the storage type is defined as read only.
-hex	(Optional) Displays the *viewname* as a hexadecimal character.
viewname	Name of a MIB view.
subtree	Name of the subtree.

Defaults

The default view is **volatile**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you use special characters for the *viewname* value (nonprintable delimiters for this parameter), you must use a hexadecimal keyword, which is one or two hexadecimal digits separated by a colon (:); for example, 00:ab:34.

A MIB subtree used with a mask defines a view subtree; it can be in OID format or a text name mapped to a valid OID.

The **read-only** keyword is supported for security model v3 only.

Examples

This example shows how to display the SNMP MIB view:

```
Console> (enable) show snmp view
View Name: defaultUserView
Subtree OID: 1.3.6.1
Subtree Mask:
View Type: included
Storage Type: volatile
Row Status: active
Control> (enable)
```

8.6 EFT Copy

Table 2-96 describes the fields in the **show snmp view** command output.

Table 2-96 show snmp view Command Output Fields

Field	Description
View Name	Name of a MIB view.
Subtree OID	Name of a MIB subtree in OID format or a text name mapped to a valid OID.
Subtree Mask	Subtree mask can be all ones, all zeros, or a combination of both.
View Type	Status of whether the MIB subtree is included or excluded.
Storage Type	Storage type (volatile or nonvolatile).
Row Status	Status of the entry.

Related Commands

clear snmp view
set snmp view

show span

To display information about the current SPAN configuration, use the **show span** command.

show span [**all**]

Syntax Description

all	(Optional) Displays local and remote SPAN configuration information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display SPAN information for the switch. In this example, the SPAN source is port 2/1 and the SPAN destination is port 2/12. Only transmit traffic is monitored. Normal incoming packets are disabled on the SPAN destination port. Monitoring multicast traffic is enabled.

```
Console> (enable) show span
---------------------------------------------------------
Destination      : Port 4/1
Admin Source     : Port 2/2
Oper Source      : Port 2/2
Direction        : transmit/receive
Incoming Packets: enabled
Learning         : -
Multicast        : enabled
Filter           : 10,20,30,40,50,60,70,80,90,100
Status           : inactive
Console> (enable)
```

Table 2-97 describes the fields in the **show span** command output.

Table 2-97 show span Command Output Fields

Field	Description
Destination	Destination port for SPAN information.
Admin Source	Source port or VLAN for SPAN information.
Oper Source	Operator port or VLAN for SPAN information.
Direction	Status of whether transmit, receive, or transmit and receive information is monitored.
Incoming Packets	Status of whether reception of normal incoming packets on the SPAN destination port is enabled or disabled.
Learning	Status of whether learning is enabled or disabled for the SPAN destination port.

Table 2-97 show span Command Output Fields (continued)

Field	Description
Multicast	Status of whether monitoring multicast traffic is enabled or disabled.
Filter	Monitored VLANs in source trunk ports.
Max. Bandwidth	Bandwidth limits for SPAN traffic, in Mbps.

Related Commands

clear config
set spantree root

8.6 EFT Copy

show spantree

To display spanning tree information for a VLAN or port, use the **show spantree** command.

show spantree [*vlan*] [**active**]

show spantree *mod/port*

Syntax Description

vlan	(Optional) Number of the VLAN; valid values are from 1 to 4094.
active	(Optional) Displays only the active ports.
mod/port	Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify the VLAN number, VLAN 1 is displayed.

If you are in MISTP mode, instance information is not displayed.

The maximum length of the channel port list can be 47. The spaces in the Port(s) column may not be enough to display the entire list in one line. If this is the case, the port list is split into multiple lines. For example, in the following display, ports 6/5-8, 6/13, 6/15, 6/17, 6/19 are channeling:

```
...
Port(s)                  Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
6/5-8,6/13,6/15,6/17,6/1 1    not-connected 2684354   32   disabled 0
9
...
```

The LACP channel protocol does not support half-duplex links. If a port is in active/passive mode and becomes half duplex, the port is suspended (and a syslog message is generated). The port is shown as “connected” using the **show port** command and as “not connected” using the **show spantree** command. This discrepancy is because the port is physically connected but never joined spanning tree. To get the port to join spanning tree, either set the duplex to full or set the channel mode to off for that port.

Examples

This example (while in PVST+ mode) shows how to display the active spanning tree port configuration for VLAN 1:

```
Console> (enable) show spantree 1 active
VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled
```

```
Designated Root             00-60-70-4c-70-00
Designated Root Priority    16384
Designated Root Cost        19
Designated Root Port        2/3
Root Max Age   14 sec   Hello Time 2  sec   Forward Delay 10 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32768
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 2/3                     1    forwarding           19   32 disabled 0
 2/12                    1    forwarding           19   32 disabled 0
Console> (enable)
```

This example (while in MISTP mode) shows how to display the active spanning tree port configuration for VLAN 1:

```
Console> (enable) show spantree 1 active
VLAN 1
Spanning tree mode          MISTP
Spanning tree type          ieee
Spanning tree enabled
VLAN mapped to MISTP Instance: 1

Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 2/3                     1    forwarding       200000   32 disabled 0
 2/12                    1    forwarding       200000   32 disabled 0
Console> (enable)
```

This example (while in Rapid PVST+ mode) shows how to display the active spanning tree port configuration for VLAN 989:

```
Console> show spantree 989 active
VLAN 989
Spanning tree mode          RAPID-PVST+
Spanning tree type          ieee
Spanning tree enabled

Designated Root             00-02-7d-a4-53-dc
Designated Root Priority    8192
Designated Root Cost        0
Designated Root Port        1/0
Root Max Age   20 sec   Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-02-7d-a4-53-dc
Bridge ID Priority          8192
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec

Port                     State         Role Cost     Prio Type
------------------------ ------------- ---- -------- ---- --------------------
 3/3                     forwarding    DESG       19   32 P2P, PEER(STP)
 5/1                     forwarding    DESG        4   32 P2P, Edge
 6/5                     forwarding    DESG        4   32 P2P
Console>
```

This example (while in Rapid PVST+ mode) shows how to display the spanning tree configuration for module 5, port 1:

```
Console> show spantree 5/1
Edge Port:        Yes, (Configured) Disable
Link Type:        P2P, (Configured) Auto
Port Guard:   Default
Port                     Vlan State         Role Cost     Prio Type
------------------------ ---- ------------- ---- -------- ---- -----------------
 5/1                     1    forwarding    DESG        4   32 P2P, Edge
 5/1                     40   forwarding    DESG        4   32 P2P, Edge
 5/1                     500  forwarding    DESG        4   32 P2P, Edge
 5/1                     501  forwarding    DESG        4   32 P2P, Edge
 5/1                     856  forwarding    DESG        4   32 P2P, Edge
 5/1                     989  forwarding    DESG        4   32 P2P, Edge
Console>
```

Table 2-98 describes the fields in the **show spantree** command output:

Table 2-98 show spantree Command Output Fields

Field	Description
VLAN	VLAN for which the spanning tree information is shown.
Spanning tree	Status of whether Spanning Tree Protocol is enabled or disabled.
Spanning tree mode	Current spanning tree mode: mistp, pvst+, mistp-pvst+, mst, or rapid pvst+.
Spanning tree type	Current spanning tree type: ieee or cisco.
Designated Root	MAC address of the designated spanning tree root bridge.
Designated Root Priority	Priority of the designated root bridge.
Designated Root Cost	Total path cost to reach the root.
Designated Root Port	Port through which the root bridge can be reached (shown only on nonroot bridges).
Root Max Age	Amount of time a BPDU packet should be considered valid.
Hello Time	Number of times the root bridge sends BPDUs.
Forward Delay	Amount of time the port spends in listening or learning mode.
Bridge ID MAC ADDR	Bridge MAC address.
Bridge ID Priority	Bridge priority.
Bridge Max Age	Bridge maximum age.
Forward Delay	Amount of time the bridge spends in listening and learning mode.
Port	Port number.
Vlan	VLAN to which the port belongs.

Table 2-98 show spantree Command Output Fields (continued)

Field	Description
Port-State	Spanning tree port state (disabled, inactive, not-connected, blocking, listening, learning, forwarding, bridging, or type-pvid-inconsistent).
Role	Port role in the spanning tree: Root, Designated, Alternate, Back-up.
Cost	Cost associated with the port.
Prio	Priority associated with the port.
Portfast	Status of whether the port is configured to use the PortFast feature.
Channel_id	Channel ID number.

Related Commands

show spantree backbonefast
show spantree blockedports
show spantree portvlancost
show spantree statistics
show spantree summary
show spantree uplinkfast

8.6 EFT Copy

show spantree backbonefast

To display whether the spanning tree BackboneFast Convergence feature is enabled, use the **show spantree backbonefast** command.

show spantree backbonefast

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is not available in MISTP mode or in MST mode.

Examples

This example shows how to display whether the spanning tree BackboneFast Convergence feature is enabled:

```
Console> show spantree backbonefast
Backbonefast is enabled.
Console>
```

Related Commands

set spantree backbonefast
show spantree defaultcostmode

show spantree blockedports

To display only the blocked ports on a per-VLAN or per-instance basis, use the **show spantree blockedports** command.

show spantree blockedports [*vlans*]

show spantree blockedports mistp-instance [*instance*]

show spantree blockedports mst [*instance*]

Syntax Description

vlans	(Optional) Number of the VLANs.
mistp-instance *instance*	Keyword and optional variable to display instance-specific information; valid values are from 1 to 16.
mst *instance*	Keyword and optional variable to display instance-specific information; valid values are from 0 to 15.

Defaults

The default is all blocked ports in all VLANs are displayed.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a VLAN number, all blocked ports in the system are displayed.

Examples

This example shows how to display the blocked ports for VLAN 1002:

```
Console> show spantree blockedports 1002
Number of blocked ports (segments) in VLAN 1002 : 0
Console>
```

This example shows how to display the blocked ports for an MISTP instance:

```
Console> show spantree blockedports mistp-instance 1
Number of blocked ports (segments) in Instance 1 : 0
Console>
```

This example shows how to display the blocked ports for an MST instance:

```
Console> show spantree blockedports mst 0
Number of blocked ports (segments) in Instance 0: 0
Console>
```

Related Commands

show spantree

show spantree bpdu-filter

To display information about BPDU filtering, use the **show spantree bpdu-filter** command.

show spantree bpdu-filter [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display information about BPDU filtering on module 1:

```
Console> show spantree bpdu-filter 1
Global BPDU Filter is disabled on the switch.
Port                     BPDU-Filter
------------------------ -----------
 1/1                     Enable
 1/2                     Default
Console>
```

Related Commands

set spantree bpdu-filter

show spantree bpdu-guard

To display information about BPDU guard, use the **show spantree bpdu-guard** command.

show spantree bpdu-guard [*mod*[/*port*]]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display information about BPDU guard on module 1:

```
Console> show spantree bpdu-guard 1
Global BPDU Guard is disabled on the switch.
Port                     BPDU-Guard
------------------------ ----------
 1/1                     Enable
 1/2                     Default
Console>
```

Related Commands

set spantree bpdu-guard

show spantree bpdu-skewing

To display BPDU skewing detection status, use the **show spantree bpdu-skewing** command.

show spantree bpdu-skewing *vlan* [*mod/port*]

show spantree bpdu-skewing {**mistp-instance** *instance*} *mod/port*

show spantree bpdu-skewing mst [*instance* | *mod/port*]

Syntax Description

vlan	Number of the VLAN; valid values are from 1 to 4094.
mod/port	(Optional) Number of the module and the port on the module.
mistp-instance *instance*	Displays instance-specific information; valid values are from 1 to 16.
mst	Displays MST instance information.
instance	(Optional) Number of the instance; valid values are from 1 to 15.
mod/port	(Optional) Number of the module and the port on the module.

Defaults

The default is the BPDU skew status for all VLANs is displayed.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is not supported by the NAM.

The **mistp-instance** *instance* options are available in MISTP mode only.

You can use this command to troubleshoot slow network convergence due to skewing. Skewing occurs when spanning tree timers lapse, expected BPDUs are not received, and spanning tree detects topology changes. The difference between the expected result and the BPDUs actually received is a *skew*. The skew causes BPDUs to reflood the network to keep the spanning tree topology database up to date.

Examples

This example shows how to display the BPDU skew status for a VLAN:

```
Console> show spantree bpdu-skewing 1

Bpdu skewing statistics for vlan 1

Port             Last Skew (ms)   Worst Skew (ms)      Worst Skew Time
--------------   ---------------  ---------------  -------------------------
8/2                        5869            108370  Tue Nov 21 2000, 06:25:59
8/4                        4050            113198  Tue Nov 21 2000, 06:26:04
8/6                      113363            113363  Tue Nov 21 2000, 06:26:05
.
.
```

```
.
8/24                       4111         113922  Tue Nov 21 2000, 06:26:05
8/26                     113926         113926  Tue Nov 21 2000, 06:26:05
8/28                       4111         113931  Tue Nov 21 2000, 06:26:05
Console> (enable)
```

This example shows how to display the BPDU skew status for a specific module and port on a VLAN:

```
Console> (enable) show spantree bpdu-skewing 1 5/9
Bpdu skewing statistics for vlan 1

Port            Last Skew (ms)   Worst Skew (ms)      Worst Skew Time
--------------  ---------------  ---------------  -------------------------
 5/9                       3992             4407  Mon Mar 26 2001, 11:31:37
Console> (enable)
```

Table 2-99 describes the fields in the **show spantree bpdu-skewing** command output.

Table 2-99 show spantree bpdu-skewing Command Output Fields

Field	Description
Last Skew (ms)	Duration of the last skew; absolute time in milliseconds.
Worst Skew (ms)	Duration of the worst skew; absolute time in milliseconds.
Worst Skew Date	Date and time of the worst skew duration.

Related Commands

set spantree bpdu-skewing
show spantree summary

show spantree conflicts

To display the MAC address of the root switch in the instance, the time remaining before the VLAN joins the instance, and the number of seconds left before the entry expires and is removed from the table, use the **show spantree conflicts** command.

show spantree conflicts *vlan*

Syntax Description

vlan	Number of the VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is available in MISTP or MISTP/PVST+ mode only.

This command is not available in MST mode.

When only one entry is printed (or when all the entries are associated to the same instance), the VLAN is mapped to that instance. If two or more entries are associated with different instances, then the VLAN has a conflict, is blocked, and is not mapped to any instance.

The time left timers associated with the mapping of a VLAN to an MISTP instance are started with the maximum age of the BPDU and can be up to the maximum age. This field can show “inactive” to indicate the MAC address is the same as the MAC address of the switch (for example, the switch is the root). In all the other cases, the entry is a number, and the timer restarts every time an incoming BPDU confirms the mapping.

The delay timer field can display the following:

- Number in seconds that represents the timer running; this timer can be up to the maximum forward delay. The timer is initialized with the fwd delay.
- If the timer is not running, “inactive” is displayed because the VLAN is already mapped to the instance or a conflict is in progress.

Examples

This example shows the output if there are no conflicts on the specified VLAN:

```
Console> (enable) show spantree conflicts 1
No conflicts for vlan 1
Inst MAC               Delay     Time left
---- ----------------- --------- ---------
 1   00-30-a3-4a-0c-00  inactive        35
Console> (enable)
```

This example shows the output if there are conflicts on the specified VLAN:

```
Console> (enable) show spantree conflicts 1
Inst MAC                Delay     Time left
---- ----------------- --------- ---------
 1   00-30-a3-4a-0c-00  inactive        35
 3   00-30-f1-e5-00-01  inactive        23
Console> (enable)
```

Table 2-100 describes the fields in the **show spantree conflicts** command output.

Table 2-100 show spantree conflicts Command Output Fields

Field	Description
Inst	Instance number that is requesting to map the VLAN.
MAC	MAC address of the root sending the BPDU claiming the VLAN, taken from the root ID of the BPDU.
Delay	Time remaining before the VLAN joins the instance.
Time left	Age of the entry, as time in seconds left before the entry expires and is removed from the table.

Related Commands

show spantree mistp-instance

show spantree defaultcostmode

To display the current default port cost mode, use the **show spantree defaultcostmode** command.

show spantree defaultcostmode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the default port cost mode:

```
Console> (enable) show spantree defaultcostmode
Portcost and portvlancost set to use 802.1d default values.
Console> (enable)
```

Related Commands

set spantree defaultcostmode

show spantree guard

To display spanning tree guard information for the VLANs or instances on a port, use the **show spantree guard** command.

show spantree guard [*vlan*]

show spantree guard [*mod/port*]

show spantree guard mistp-instance [*instance*]

show spantree guard mistp-instance [*mod/port*]

show spantree guard mst [*instance*]

show spantree guard mst [*mod/port*]

Syntax Description

vlan	(Optional) Number of the VLAN; valid values are from 1 to 4094.
mod/port	(Optional) Number of the module and the port on the module.
mistp-instance *instance*	Keyword and optional variable to display MISTP instance-specific information; valid values are from 1 to 16.
mst *instance*	Keyword and optional variable to display MST instance-specific information; valid values are from 0 to 15.

Defaults

The default is VLAN 1, and the default port list is “all the ports” in the specified or default VLAN.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

When you enable the spanning tree root guard or loop guard feature, the command works on a per-port basis. When you enable the feature on a port, a logical port is blocked on a per-VLAN basis. This means that you can specify a port (or a list of ports) and specify a VLAN, but you cannot specify both.

Examples

This example shows how to display spanning tree guard information for a specific VLAN:

```
Console> show spantree guard 1004
Port Vlan Port-State           Guard type
---- ---- -------------------  ------------
1/1  1004  root-inconsistent    root
1/2  1004  not-connected        none
2/1  1004  loop-inconsistent    loop
2/2  1004  forwarding           loop
.
.
.
Console>
```

This example shows how to display spanning tree guard information for a specific instance:

```
Console> show spantree guard mistp-instance 3
Port                     Inst Port-State    Guard Type
------------------------ ---- ------------- ----------
1/1                      3    listening     root
1/2                      3    listening     root
Console>
```

Related Commands

set spantree guard

show spantree mapping

To display VLAN and instance mapping information, use the **show spantree mapping**.

show spantree mapping [**config**]

Syntax Description

config	(Optional) Displays mappings configured on the local switch.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not enter the optional **config** keyword, the mapping information propagated from the root switch in the instance is displayed. This runtime command is available in MISTP or MISTP-PVST+ mode only. If you enter the **config** keyword, the list of mappings configured on the local switch is displayed. It is available in PVST+ mode.

If you enter this command in PVST mode, this message appears:

```
Runtime vlan and instance mapping information is only available in MISTP
or
MISTP-PVST mode. Use 'show spantree mapping config' to view mappings
configured on the local switch.
```

Examples

This example shows how to display runtime VLAN and instance mapping information:

```
Console> (enable) show spantree mapping
Inst Root Mac          Vlans
---- ----------------- --------------------------------------------------
1    00-50-3e-78-70-00 1
2    00-50-3e-78-70-00 -
3    00-50-3e-78-70-00 -
4    00-50-3e-78-70-00 -
5    00-50-3e-78-70-00 -
6    00-50-3e-78-70-00 -
7    00-50-3e-78-70-00 -
8    00-50-3e-78-70-00 -
9    00-50-3e-78-70-00 -
10   00-50-3e-78-70-00 -
11   00-50-3e-78-70-00 -
12   00-50-3e-78-70-00 -
13   00-50-3e-78-70-00 -
14   00-50-3e-78-70-00 -
15   00-50-3e-78-70-00 -
16   00-50-3e-78-70-00 -
Console> (enable)
```

This example shows how to display mappings configured on the local switch:

```
Console> (enable) show spantree mapping config
Inst Root Mac          Vlans
---- ----------------- --------------------------------------------------
1    -                 1
2    -                 -
3    -                 -
4    -                 -
5    -                 -
6    -                 -
7    -                 -
8    -                 -
9    -                 -
10   -                 -
11   -                 -
12   -                 -
13   -                 -
14   -                 -
15   -                 -
16   -                 -
Console> (enable)
```

Related Commands

set vlan

show spantree mistp-instance

To display instance information, use the **show spantree mistp-instance** command.

show spantree mistp-instance [*instance*] [**active**]

show spantree mistp-instance *mod/port*

Syntax Description

instance	(Optional) Instance number; valid values are from 1 to 16.
active	(Optional) Displays only active ports.
mod/port	Number of the module and the port on the module.

Defaults

The default instance is 1.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is available in MISTP mode only.

If you specify the *mod/port* number only, the VLAN mapping information is not displayed.

Examples

This example shows how to display information regarding active instances only:

```
Console> show spantree mistp-instance active
Instance 1
Spanning tree mode          MISTP
Spanning tree type          ieee
Spanning tree instance enabled

Designated Root             00-d0-00-4c-18-00
Designated Root Priority    32769  (root priority: 32768, sys ID ext: 1)
Designated Root Cost        0
Designated Root Port        none
VLANs mapped:               1
Root Max Age   20 sec   Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32769  (bridge priority: 32768, sys ID ext: 1)
VLANs mapped:               1
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec

Port                     Inst Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 2/3                     1    forwarding       200000   32 disabled 0
 2/12                    1    forwarding       200000   32 disabled
Console>
```

Table 2-101 describes the fields in the **show spantree mistp-instance** command output:

Table 2-101 show spantree mistp-instance Command Output Fields

Field	Description
Instance	Instance for which spanning tree information is shown.
Spanning tree mode	Spanning tree mode.
Spanning tree type	Spanning tree type.
Spanning tree instance	Status of whether spanning tree instance is enabled or disabled.
Designated Root	MAC address of the designated spanning tree root bridge.
Designated Root Priority	Priority of the designated root bridge.
Designated Root Cost	Total path cost to reach the root.
Designated Root Port	Port through which the root bridge can be reached (shown only on nonroot bridges).
VLANs mapped	Number of VLANs mapped.
Root Max Age	Amount of time a BPDU packet should be considered valid.
Hello Time	Number of times the root bridge sends BPDUs.
Forward Delay	Amount of time the port spends in listening or learning mode.
Bridge ID MAC ADDR	Bridge MAC address.
Bridge ID Priority	Part of the bridge identifier and is taken as the most significant part of the bridge ID comparisons.
Bridge Max Age	Bridge maximum age.
Topology change initiator	Module and port where the topology change was initiated.
Last topology change occurred	Date and time of the last topology change.
Topology change count	Number of topology changes that have occurred during the last change interval.
Hello Time	Amount of time the bridge sends BPDUs.
Forward Delay	Amount of time the bridge spends in listening or learning mode.
Port	Port number.
Instance	Instance to which the port belongs.
Port-State	Spanning tree port state (disabled, inactive, not-connected, blocking, listening, learning, forwarding, bridging, or type-pvid-inconsistent).
Cost	Cost associated with the port.
Prio	Priority associated with the port.
Portfast	Status of whether the port is configured to use the PortFast feature.
Channel_id	Channel ID number.

Related Commands

set spantree portinstancecost
set spantree portinstancepri

show spantree mst

To display MST information, use the **show spantree mst** command.

show spantree mst [*instance* | *mod/port*]

show spantree mst active

Syntax Description

instance	(Optional) Number of the instance; valid values are from 0 to 15.
mod/port	(Optional) Number of the module and the port on the module.
active	Displays active IST ports only.

Defaults

The default instance is instance 0 (IST).

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can use the **show spantree mst** command to display VLAN-specific spanning tree information.

Examples

This example shows how to display MST information for instance 0 (IST):

```
Console> show spantree mst
Spanning tree mode          MST
Instance                    0
VLANs Mapped: 1-1005,1025-4093

Designated Root             00-04-9b-ba-48-00
Designated Root Priority    32768  (root priority: 32768, sys ID ext: 0)
Designated Root Cost        2000000
Designated Root Port        6/48
Root Max Age   20 sec   Hello Time 2  sec   Forward Delay 15 sec

CIST Regional Root          00-10-7b-bb-2f-00
CIST Regional Root Priority 32768
CIST Internal Root Cost     0         Remaining Hops 18

Bridge ID MAC ADDR          00-10-7b-bb-2f-00
Bridge ID Priority          32768  (bridge priority: 32768, sys ID ext: 0)
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec  Max Hops 20

Topology change initiator           4/48
Last topology change occured        Mon Oct 9 2006, 11:20:28
Topology change count               3

Port                     State         Role Cost     Prio Type
------------------------ ------------- ---- -------- ---- --------------------
6/48                     forwarding    ROOT  2000000   32 Shared, Boundary(STP)
```

```
Console>
```

This example shows how to display MST instance-specific information for instance 1:

```
Console> show spantree mst 1
Spanning tree mode          MST
Instance                    1
VLANs Mapped:              1

Designated Root             00-d0-00-b3-68-00
Designated Root Priority    32769  (root priority:32768, sys ID ext:1)
Designated Root Cost        0          Remaining Hops 20
Designated Root Port        1/0

Bridge ID MAC ADDR          00-d0-00-b3-68-00
Bridge ID Priority          32769  (bridge priority:32768, sys ID ext:1)

Port                     State         Role Cost     Prio Type
------------------------ ------------- ---- -------- ---- --------------------
 5/1                     forwarding    BDRY    20000   32 P2P, Boundary(STP)
 5/2                     forwarding    BDRY    20000   32 P2P, Boundary(STP)
 7/48                    forwarding    BDRY  2000000   32 Shared, Boundary
Console>
```

This example shows how to display MST instance-specific information for port 6 on module 3:

```
Console> show spantree mst 2/1
Edge Port:          No, (Configured) Default
Link Type:         P2P, (Configured) Auto
Port Guard:    Default
Boundary:          Yes  (PVST)
Hello:               2, (Local bridge hello: 2)

Inst State         Role Cost      Prio VLANs
---- ------------- ---- --------- ---- -----------------------------------
   0 forwarding    ROOT     20000   32 1-9,11-13,15-99
  10 forwarding    MSTR     20000   32 10,100,1000
  14 forwarding    MSTR     20000   32 14
Console>
```

Related Commands

clear spantree mst
set spantree mst config
show spantree
show spantree mst config

show spantree mst config

To display the MST region information present in NVRAM and to display changes that have not been applied to the MST region configuration yet, use the **show spantree mst config** command.

show spantree mst config

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the MST region information:

```
Console> show spantree mst config
Currnet (NVRAM) MST Configuration
Configuration Name:Cisco                         Revision: 1
Instance Vlans
-------- ----------------- ------------------------
0        401-1005,1025-1999,2201-4096
1        1-50
2        51-100
3        101-300
4        -
5        -
6        2000-2200
7        301-400
8        -
9        -
10       -
11       -
12       -
13       -
14       -
15       -
===============================================
New MST Region Configuration (Not applied yet)

Region Name:Catalyst                         Revision: 6000
Instance Vlans
-------- ----------------- ------------------------
0        1-50,401-1005,1025-1999,2201-4096
1        -
2        51-100
3        101-300
4        -
5        -
6        2000-2200
```

```
7        301-400
8        -
9        -
10       -
11       -
12       -
13       -
14       -
15       -
================================================
Edit buffer is locked by: Console
Console> (enable)
```

Related Commands

clear spantree mst
set spantree mst config

show spantree portfast

To display PortFast information, use the **show spantree portfast** command.

show spantree portfast [*mod/port*]

Syntax Description

mod/port	(Optional) Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

When you enter the **show spantree portfast** command, if the designation for a port is displayed as an edge port, it is a PortFast port. Refer to Chapter 8, “Configuring Spanning Tree,” and Chapter 9, “Configuring Spanning Tree PortFast, UplinkFast, BackboneFast, and Loop Guard,” of the *Catalyst 6500 Series Switch Software Configuration Guide* for more information about PortFast.

Examples

This example shows how to display PortFast information:

```
Console> show spantree portfast
Portfast BPDU guard is disabled.
Portfast BPDU filter is disabled.
Console>
```

This example shows how to display PortFast information for a specific module and port:

```
Console> show spantree portfast 3/1
Portfast:    Default
BPDU Filter: Enable
BPDU Guard:  Default
Portfast BPDU guard is disabled.
Portfast BPDU filter is disabled.
Console>
```

Related Commands

set spantree portfast
set spantree portfast bpdu-filter
set spantree portfast bpdu-guard

show spantree portinstancecost

To show the path cost for the instances on a port, use the **show spantree portinstancecost** command.

show spantree portinstancecost *mod/port*

Syntax Description

mod/port	Number of the module and the port on the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the path cost for the MISTP instances on port 1/1:

```
Console> show spantree portinstancecost 1/1
Port 1/1 instances 1-16 have path cost 20000.
Console>
```

Related Commands

clear spantree portinstancecost
set spantree portinstancecost

show spantree portvlancost

To show the path cost for the VLANs or extended-range VLANs, use the **show spantree portvlancost** command.

show spantree portvlancost *mod/port* | **extended-range**

Syntax Description

mod/port	Number of the module and the port on the module.
extended-range	Specifies extended-range VLANs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command is valid in PVST+ mode only.

Examples

This example shows how to display the path cost for the VLANs on port 2/12:

```
Console> show spantree portvlancost 2/12
Port 2/12 VLANs 1-1005 have path cost 19.
Console>
```

Related Commands

clear spantree portvlancost
set spantree portvlancost

show spantree statistics

To show spanning tree statistical information, use the **show spantree statistics** command.

show spantree statistics *mod/port* [*vlan*]

show spantree statistics *mod/port* **mistp-instance** *instance*

show spantree statistics *mod/port* **mst** *instance*

show spantree statistics bpdu

Syntax Description

mod/port	Number of the module and the port on the module.
vlan	(Optional) Number of the VLAN; valid values are from 1 to 4094.
mistp-instance *instance*	Displays MISTP instance-specific information; valid values are from 1 to 16.
mst *instance*	Displays MST instance-specific information; valid values are from 0 to 15.
bpdu	Displays the total number of spanning tree BPDUs. See the “Usage Guidelines” section for more information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

When you enter the **show spantree statistics bpdu** command, the switch displays all transmitted, received, processed, and dropped BPDUs. The system also displays the rate of these BPDUs in seconds. All BPDU counters give BPDU statistics from the last time that the counters were cleared or from the time that the system was booted up.

Examples

This example shows how to display statistical information:

```
Console> (enable) show spantree statistics 1/2 1005

SpanningTree enabled for vlanNo = 1005

                BPDU-related parameters
port spanning tree                     enabled
state                                  disabled
port_id                                0xcccf
port number                            0x7eb
path cost                              80
message age (port/VLAN)                0(10)
designated_root                        00-10-2f-52-eb-ec
```

```
designated_cost                      0
designated_bridge                    00-10-2f-52-eb-ec
designated_port                      0xcccf
top_change_ack                       FALSE
config_pending                       FALSE

                PORT based information & statistics
config bpdu's xmitted (port/VLAN)    0(0)
config bpdu's received (port/VLAN)   0(0)
tcn bpdu's xmitted (port/VLAN)       0(0)
tcn bpdu's received (port/VLAN)      0(0)
forward trans count                  0

                Status of Port Timers
forward delay timer                  INACTIVE
forward delay timer value            0
message age timer                    INACTIVE
message age timer value              0
topology change timer                INACTIVE
topology change timer value          0
hold timer                           INACTIVE
hold timer value                     0
delay root port timer                INACTIVE
delay root port timer value          0

                VLAN based information & statistics
spanningtree type                    ibm
spanningtree multicast address       c0-00-00-00-01-00
bridge ID priority                             32768 (bridge priority: 32768, sys ID ext:
64)
bridge mac address                   00-10-2f-52-eb-ec
bridge hello time                    2 sec
bridge forward delay                 4 sec
topology change initiator:           1/0
topology change                      FALSE
topology change time                 14
topology change detected             FALSE
topology change count                0

                Other port-specific info
dynamic max age transitions          0
port bpdu ok count                   0
msg age expiry count                 0
link loading                         1
bpdu in processing                   FALSE
num of similar bpdus to process      0
next state                           0
src mac count:                       0
total src mac count                  0
curr_src_mac                         00-00-00-00-00-00
next_src_mac                         00-00-00-00-00-00
channel_src_mac                      00-00-00-00-00-00
channel src count                    0
channel ok count                     0
Console> (enable)
```

This example shows how to display instance-specific information:

```
Console> (enable) show spantree statistics 2 mistp-instance 2
Port  2/1   Instance 2

SpanningTree enabled for instance = 2

                BPDU-related parameters
port spanning tree                     enabled
state                                  forwarding
port_id                                0x8041
port number                            0x41
path cost                              20000
message age (port/inst)                1(20)
designated_root                        00-50-3e-8f-8c-00
designated_cost                        0
designated_bridge                      00-50-3e-8f-8c-00
designated_port                        0x8001
top_change_ack                         FALSE
config_pending                         FALSE
port_inconsistency                     none

                PORT based information & statistics
config bpdu's xmitted (port/inst)      0(0)
config bpdu's received (port/inst)     102(490)
tcn bpdu's xmitted (port/inst)         0(0)
tcn bpdu's received (port/inst)        0(0)
forward trans count                    0
scp failure count                      0

                Status of Port Timers
forward delay timer                    INACTIVE
forward delay timer value              15
message age timer                      ACTIVE
message age timer value                1
topology change timer                  INACTIVE
topology change timer value            0
hold timer                             INACTIVE
hold timer value                       0
delay root port timer                  INACTIVE
delay root port timer value            0
delay root port timer restarted is     FALSE

                Instance based information & statistics
spanningtree type                      ieee
spanningtree multicast address         01-80-c2-00-00-00
bridge priority                        32770
bridge mac address                     00-d0-00-b3-68-00
bridge hello time                      2 sec
bridge forward delay                   15(15) sec
topology change initiator:            15/63
last topology change occured:         Sun Jun 7 2000, 09:00:03
topology change                        FALSE
topology change time                   35
topology change detected               FALSE
topology change count                  0
topology change last recvd. from       00-00-00-00-00-00

                Other port-specific info
dynamic max age transitions            0
port bpdu ok count                     0
msg age expiry count                   0
link loading                           1
bpdu in processing                     FALSE
```

```
num of similar bpdus to process      0
received_inferior_bpdu              FALSE
next state                           3
src mac count:                      0
total src mac count                  0
curr_src_mac                         00-00-00-00-00-00
next_src_mac                         00-00-00-00-00-00
channel_src_mac                      00-00-00-00-00-00
channel src count                    0
channel ok count                     0
Console>
```

This example shows how to display MST instance-specific information:

```
Console> show spantree statistics 8/1 mst 0
Port  8/1   Instance 0

SpanningTree enabled for instance = 0

                BPDU-related parameters
port spanning tree                   enabled
state                                forwarding
port_id                              0x81c1
port number                          0x1c1
path cost                            20000
message age (port/VLAN)              0(20)
designated_root                      00-04-9b-ba-48-00
designated_cost                      33920
designated_bridge                    00-10-7b-bb-2f-00
designated_port                      0x81c1
top_change_ack                       FALSE
config_pending                       FALSE
port_inconsistency                   none

                PORT based information & statistics
config bpdu's xmitted (port/inst)    101(212)
config bpdu's received (port/inst)   101(205)
tcn bpdu's xmitted (port/inst)       0(1)
tcn bpdu's received (port/inst)      0(2)
forward trans count                  0
scp failure count                    0
root inc trans count (port/inst)     0(0)
inhibit loopguard                    FALSE
loop inc trans count (port/inst)     0(0)

                Status of Port Timers
forward delay timer                  INACTIVE
forward delay timer value            0
message age timer                    INACTIVE
message age timer value              0
topology change timer                INACTIVE
topology change timer value          0
hold timer                           INACTIVE
hold timer value                     0
delay root port timer                INACTIVE
delay root port timer value          0
delay root port timer restarted is   FALSE

                Vlan based information & statistics
spanningtree type                    ieee
spanningtree multicast address       01-80-c2-00-00-00
bridge priority                      32768
bridge mac address                   00-10-7b-bb-2f-00
bridge hello time                    2 sec
bridge forward delay                 15(15) sec
topology change initiator:          1/0
last topology change occured:       Fri Sep 7 2001, 09:52:22
topology change                      FALSE
topology change time                 35
topology change detected             FALSE
topology change count                3
topology change last recvd. from     00-00-00-00-00-00

                Other port-specific info
dynamic max age transitions          0
port bpdu ok count                   0
msg age expiry count                 0
link loading                         0
bpdu in processing                   FALSE
num of similar bpdus to process      0
received_inferior_bpdu               FALSE
next state                           3
src mac count:                      0
total src mac count                  0
curr_src_mac                         00-00-00-00-00-00
next_src_mac                         00-00-00-00-00-00
channel_src_mac                      00-00-00-00-00-00
channel src count                    0
channel ok count                     0
Console>
```

This example shows how to display transmitted, received, processed, and dropped BPDUs and the rate of BPDUs in seconds:

```
Console> show spantree statistics bpdu
              Transmitted       Received      Processed        Dropped
           -------------- -------------- -------------- --------------

Total            52943073       52016589       52016422            167

Rate(/sec)            989            971            971              0
Console>
```

Table 2-102 describes the possible fields in the **show spantree statistics** command output.

Table 2-102 show spantree statistics Command Output Fields

Field	Description
BPDU-related parameters	
port spanning tree	Status of whether Spanning Tree Protocol is enabled or disabled on the port.
state	Spanning tree port state (disabled, listening, learning, forwarding, or blocking).
port_id	Port identifier of the associated port.
port number	Port number.
path cost	Contribution of the path through this root port. This applies to the total path cost to the root for this bridge.
message age (port/VLAN)	Age of the received protocol information recorded for a port and the value of the Max Age parameter (shown in parentheses) recorded by the switch.
designated_root	MAC address of the designated spanning tree root bridge.
designated_cost	Cost of the path to the root offered by the designated port on the LAN to which this port is attached.

Table 2-102 show spantree statistics Command Output Fields (continued)

Field	Description
designated_bridge	Bridge identifier of the bridge assumed to be the designated bridge for the LAN associated with the port.
designated_port	Port identifier of the bridge port assumed to be the designated port for the LAN associated with the port.
top_change_ack	Value of the Topology Change Acknowledgement flag in the next configured BPDU to be transmitted on the associated port. The flag is set in reply to a Topology Change Notification BPDU.
config_pending	Boolean parameter set to record that a configured BPDU should be transmitted on expiration of the hold timer for the associated port.
port_inconsistency	Status of whether the port is in an inconsistent (PVID or port type) state or not.
PORT-based information and statistics	
config bpdu's xmitted (port/VLAN)	Number of BPDUs transmitted from the port. The number in parentheses is the number of configured BPDUs transmitted by the switch for this instance of spanning tree.
config bpdu's received (port/VLAN)	Number of BPDUs received by this port. The number in parentheses is the number of configured BPDUs received by the switch for this instance of spanning tree.
tcn bpdu's xmitted (port/VLAN)	Number of TCN BDPUs transmitted on this port.
tcn bpdu's received (port/VLAN)	Number of TCN BPDUs received on this port.
forward trans count	Number of times the port state transitioned to FORWARDing state.
scp failure count	Number of SCP failures.
Status of Port Timers	
forward delay timer	Status of the forward delay timer. This timer monitors the time spent by a port in the listening and learning states.
forward delay timer value	Current value of the forward delay timer.
message age timer	Status of the message age timer. This timer measures the age of the received protocol information recorded for a port.
message age timer value	Current value of the message age timer.
topology change timer	Status of the topology change timer. This timer determines the time period in which configured BPDUs are transmitted with the topology change flag set by the bridge when it is the root following the detection of a topology change.
topology change timer value	Current value of the topology change timer.
hold timer	Status of the hold timer. This timer ensures that configured BPDUs are not transmitted too frequently through any bridge port.
hold timer value	Current value of the hold timer.
delay root port timer	Status of the delay root port timer. This timer enables fast convergence on linkup when the UplinkFast feature is enabled.
delay root port timer value	Current value of the delay root port timer.

Table 2-102 show spantree statistics Command Output Fields (continued)

Field	Description
VLAN-based information and statistics	
spanningtree type	Type of spanning tree (IEEE, IBM, CISCO).
spanningtree multicast address	Destination address used to send out configured BPDUs on a bridge port.
bridge ID priority	Part of the bridge identifier and is taken as the most significant part bridge ID comparisons.
bridge mac address	Bridge MAC address.
bridge hello time	Value of the Hello Time parameter when the bridge is the root or is attempting to become the root.
bridge forward delay	Value of the Forward Delay parameter when the bridge is the root or is attempting to become the root.
topology change initiator:	Number of the port that caused the topology change.
topology change	Boolean parameter set to record the value of the topology change flag in config BPDUs to be transmitted by the bridge on LANs for which the bridge is the designated bridge.
topology change time	Time period for which BPDUs are transmitted with the topology change flag set by the bridge when it is the root following the detection of a topology change. It is equal to the sum of the bridge's Max Age and Forward Delay parameters.
topology change detected	Boolean parameter set to TRUE when a topology change has been detected by or notified to the bridge.
topology change count	Number of times the topology change has occurred.
topology change last recvd. from	MAC address of the bridge that transmitted the last TCN BPDU.
Other port-specific info	
dynamic max age transitions	Number of dynamic max age transitions.
port bpdu ok count	Number of reported port BPDU counts.
msg age expiry count	Number of message age expires.
link loading	Status of whether the link is oversubscribed.
bpdu in processing	Status of whether the BPDU is under processing.
num of similar bpdus to process	Number of similar BPDUs to process that are received on a specific port.
received_inferior_bpdu	Status of whether the port received an inferior BPDU or in response to an RLQ BPDU.
next state	Port state before it is actually set by spanning tree, to facilitate other tasks in using the new value.
src mac count:	Number of BPDUs with the same source MAC address.
total src mac count	Number of BPDUs with all the source MAC addresses.

Table 2-102 show spantree statistics Command Output Fields (continued)

Field	Description
curr_src_mac	Source MAC address of the configured BPDU received on a particular port. It should always be set to NULL for the Catalyst 6500 series switches.
next_src_mac	MAC address from the different source. It should always be set to NULL for the Catalyst 6500 series switches.
channel_src_mac	Source MAC address of the channel port. It is used to detect channel misconfiguration and avoid spanning tree loops.
channel src count	Number of times channel_src_mac gets changed and if the limit is exceeded, a channel misconfiguration is detected.
channel ok count	Number of times the channel ok condition was detected.

Related Commands

clear spantree statistics
show spantree

show spantree summary

To display a summary of spanning tree information, use the **show spantree summary** command.

show spantree summary [**novlan**]

show spantree summary {**mistp-instance** | **mst**} [**noinstance**]

Syntax Description

novlan	(Optional) Displays non-VLAN-specific information only.
mistp-instance	Displays MISTP instance-specific information only.
mst	Displays MST instance-specific information only.
noinstance	(Optional) Displays non-instance-specific information only.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If the switch is not the root for any VLANs, “none” is displayed in the “Root switch for vlans” field.

Examples

This example shows how to display a summary of spanning tree information:

```
Console> show spantree summary
Spanning tree mode: RAPID-PVST+
MAC address reduction: enabled
Root switch for vlans: none.
Global loopguard is disabled on the switch.
Global portfast is disabled on the switch.
BPDU skewing detection disabled for the bridge.
BPDU skewed for vlans:  none.
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of connected spanning tree ports by vlan

VLAN  Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
   1         0         0        0          2          2

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total        0         0        0          2          2
Console>
```

This example shows how to display non-VLAN-specific information only:

```
Console> show spantree summary novlan
Spanning tree mode: RAPID-PVST+
MAC address reduction: enabled
Root switch for vlans: none.
Global loopguard is disabled on the switch.
Global portfast is disabled on the switch.
BPDU skewing detection disabled for the bridge.
BPDU skewed for vlans:  none.
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total        0         0        0          2          2
Console>
```

This example shows how to display a summary of spanning tree instance information:

```
Console> show spantree summary mistp-instance
MAC address reduction:disabled
Root switch for vlans:1-8,10-500,911.
BPDU skewing detection enabled for the bridge
BPDU skewed for vlans:1-8,10-500,911.
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of connected spanning tree ports by mistp-instance

Inst  Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
    1        0         0        0          8          0
    2        4         0        0          4          8
    3        4         0        0          4          8
    4        4         0        0          4          8
    5        4         0        0          4          8
    6        4         0        0          4          8
    7        4         0        0          4          8
    8        4         0        0          4          8
    9        4         0        0          4          8
   10        4         0        0          4          8
   11        4         0        0          4          8
   12        4         0        0          4          8
   13        4         0        0          4          8
   14        4         0        0          4          8
   15        4         0        0          4          8
   16        0         0        0          0          0

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total       56         0        0         64        112
Console>
```

This example shows how to display a summary of spanning tree MST instance information:

```
Console> show spantree summary mst
MAC address reduction:disabled
Root switch for MST instances:none.
Global loopguard is disabled on the switch.
Global portfast is disabled on the switch.
BPDU skewing detection enabled for the bridge.
BPDU skewed for MST instances: none.
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.

Summary of connected spanning tree ports by MST instances

Inst  Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
   0         0         0        0          3          3
   1         0         0        0          0          0
   2         0         0        0          0          0
   3         0         0        0          0          0
   4         0         0        0          0          0
   5         0         0        0          0          0
   6         0         0        0          0          0
   7         0         0        0          0          0
   8         0         0        0          0          0
   9         0         0        0          0          0
  10         0         0        0          0          0
  11         0         0        0          0          0
  12         0         0        0          0          0
  13         0         0        0          0          0
  14         0         0        0          0          0
  15         0         0        0          0          0

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total        0         0        0          3          3
Console>
```

This example shows how to display a summary of spanning tree noninstance-specific MST information:

```
Console> show spantree summary mst noinstance
MAC address reduction:disabled
Root switch for MST instances:none.
Global loopguard is disabled on the switch.
Global portfast is disabled on the switch.
BPDU skewing detection enabled for the bridge.
BPDU skewed for MST instances: none.
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total        0         0        0          3          3
Console>
```

Related Commands

show spantree

show spantree uplinkfast

To show the UplinkFast feature settings, use the **show spantree uplinkfast** command.

show spantree uplinkfast [{**mistp-instance** [*instances*]} | *vlans*]

Syntax Description

mistp-instance *instances*	(Optional) Keyword and (optional) variable to display instance-specific information; valid values are from 1 to 16.
vlans	(Optional) Number of the VLAN; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **mistp-instance** *instances* keyword and optional variable are available in MISTP or MISTP/PVST+ mode only.

The *vlans* variable is available in PVST+ mode only.

You can enter a single VLAN or instance or a range of VLANs or instances separated by commas.

If you do not specify a VLAN or instance, all VLANs or instances are displayed.

This command is not available in MST mode.

Examples

This example shows how to display the UplinkFast feature settings for all VLANs:

```
Console> show spantree uplinkfast
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
VLAN port list
------------------------------------------------
1-20   1/1(fwd),1/2-1/5
21-50  1/9(fwd), 1/6-1/8, 1/10-1/12
51-100 2/1(fwd), 2/12
Console>
```

This example shows how to display the UplinkFast feature settings for a specific instance:

```
Console> show spantree uplinkfast mistp-instance 1
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
Inst   port list
------------------------------------------------
1      4/1(fwd)
Console>
```

This example shows how to display the UplinkFast feature settings when in Rapid PVST+ mode:

```
Console> show spantree uplinkfast
uplinkfast is enabled but inactive in Rapid-Pvst+ mode.
Console>
```

Related Commands

clear spantree uplinkfast
set spantree uplinkfast

show ssh

To display information about Secure Shell (SSH) sessions, use the **show ssh** command.

show ssh

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

A user ID might not be specified in the output of this command because a user ID is not mandatory for local user authentication.

Examples

This example shows how to display information about SSH sessions:

```
Console> (enable) show ssh
Session Protocol  Cipher    State                 PID      Userid   Host
------- --------  -------   --------------------- -------- -------- -------------------
0       V2        3DES      SESSION_OPEN          146      dkoya    171.69.66.45
1       V1        3DES      SESSION_OPEN          147        -      dove.cisco.com
SSH server mode :V1 and V2
Console>(enable)
```

Related Commands

clear ssh mode
set ssh mode

show startup-config

To display the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable, use the **show startup-config** command.

show startup-config

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To view specific information within the **show startup-config** output, if you enter a /*text* value and press the **Return** key at the --More-- prompt, the display starts two lines above the line containing the *text* string. If the text string is not found, “Pattern Not Found” is displayed. You can also enter **n** at the --More-- prompt to search for the last entered text string.

Examples

This example shows how to display the switch startup configuration:

```
Console> (enable) show startup-config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
..............

..................
....................

..

begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Mon Jun 11 2001, 06:56:10
!
#version 6.3(0.56)PAN
!

!
#!
```

```
#vtp
set vtp domain dan
set vtp mode transparent
set vlan 1 name default type ethernet mtu 1500 said 100001 state active
set vlan 1002 name fddi-default type fddi mtu 1500 said 101002 state active
set vlan 1004 name fddinet-default type fddinet mtu 1500 said 101004 state acti
e stp ieee
set vlan 1005 name trnet-default type trbrf mtu 1500 said 101005 state active s
p ibm
set vlan 2,10-11
set vlan 1003 name token-ring-default type trcrf mtu 1500 said 101003 state act
ve mode srb aremaxhop 7 stemaxhop 7 backupcrf off
!
#ip
set interface sc0 1 172.20.52.19/255.255.255.224 172.20.52.31

set ip route 0.0.0.0/0.0.0.0         172.20.52.1
!
#set boot command
set boot config-register 0x10f
set boot system flash bootflash:cat6000-sup2-d.6-3-0-56-PAN.bin
set boot system flash bootflash:cat6000-sup2-d.6-3-0-54-PAN.bin
set boot system flash bootflash:cat6000-sup2-d.6-3-0-46-PAN.bin
set boot system flash bootflash:cat6000-sup2-d.6-3-0-44-PAN.bin
set boot system flash bootflash:
!
#qos
set qos wred 1p2q2t tx queue 1 60:80 80:100
set qos wred 1p2q2t tx queue 2 60:80 80:100
set qos wred 1p3q1t tx queue 1 80:100
set qos wred 1p3q1t tx queue 2 80:100
set qos wred 1p3q1t tx queue 3 80:100
!
#mmls nonrpf
set mmls nonrpf timer 0
!
#security ACLs
clear security acl all
#pbf set
set pbf mac 00-01-64-61-39-c3
#adj set
set security acl adjacency ADJ2 10 00-00-00-00-00-0a 00-00-00-00-00-0b mtu 9600
#
commit security acl all
!
# default port status is enable
!
!
#module 1 empty
!
#module 2 : 2-port 1000BaseX Supervisor
!
#module 3 : 48-port 10/100BaseTX Ethernet
set vlan 10   3/1
set vlan 11   3/2
!
#module 4 empty
!
#module 5 : 0-port Switch Fabric Module
!
#module 6 empty
!
#module 7 empty
!
```

```
#module 8 empty
!
#module 9 empty
!
#module 15 empty
!
#module 16 empty
end
Console> (enable)
```

Related Commands

show running-config

show summertime

To display the current status of the summertime feature, use the **show summertime** command.

show summertime

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the current status of the **summertime** feature:

```
Console> show summertime
Summertime is disabled and set to ''
Start : Thu Apr 13 2000, 04:30:00
End   : Mon Jan 21 2002, 05:30:00
Offset: 1440 minutes (1 day)
Recurring: no
Console>
```

Related Commands

set summertime

show system

To display system information, use the **show system** command.

show system

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The switching bus traffic values that are displayed apply to a single bus.

Examples

This example shows how to display system information:

```
Console> show system
PS1-Status PS2-Status
---------- ----------
none       ok

Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
---------- ---------- ---------- -------------- ---------
ok         off        ok         1,22:38:21     20 min

PS1-Type             PS2-Type
-------------------- --------------------
none                 WS-CAC-1300W
Modem   Baud  Traffic Peak Peak-Time
------- ----- ------- ---- -------------------------
disable  9600   0%      0% Mon Jan 10 2000, 15:23:31

PS1 Capacity: 1153.32 Watts (27.46 Amps @42V)

System Name              System Location          System Contact           CC
------------------------ ------------------------ ------------------------ ---
Information Systems      Closet 230 4/F           Xena ext. 24

No active fabric module in the system.
```

```
Core Dump                Core File
------------------------  -----------------------
enabled                     bootflash:crashinfo

System Logging  Host             File                                 Interval
--------------  ---------------  -----------------------------------  --------
Disabled        -                tftp:sysinfo                         1440
Index        System Command
-----        ----------------------------------------------------------
    1        show version

Syslog Dump              Syslog File
------------------------ -----------------------
enabled                     bootflash:sysloginfo

Console>
```

This example shows how to display system information on a system configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> show system
Console> (enable) show system
PS1-Status PS2-Status
---------- ----------
ok         none

Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
---------- ---------- ---------- -------------- ---------
ok         off        ok         5,22:12:33     20 min

PS1-Type             PS2-Type
-------------------- --------------------
WS-CAC-1300W         none

Modem   Baud  Backplane-Traffic Peak Peak-Time
------- ----- ----------------- ---- -------------------------
disable  9600   0%                0% Tue Mar 5 2002, 11:44:07

PS1 Capacity: 1153.32 Watts (27.46 Amps @42V)

System Name              System Location          System Contact           CC
------------------------ ------------------------ ------------------------ ---


Fab Chan Input Output
-------- ----- ------
       0    0%     0%
       1    0%     0%
       2    0%     0%
       3    0%     0%
       4    0%     0%
       5    0%     0%
       6    0%     0%
       7    0%     0%
       8    0%     0%
       9    0%     0%
      10    0%     0%
      11    0%     0%
      12    0%     0%
      13    0%     0%
      14    0%     0%
      15    0%     0%
      16    0%     0%
      17    0%     0%
```

```
Core Dump                Core File
------------------------ -----------------------
disabled                 slot0:crashinfo

Crash Info               Crash Info File
------------------------ -----------------------
disabled                 bootflash:crashinfo

System Information Logging  Host              Interval
--------------------------  ----------------  --------
Disabled                    -                 1440

System Information Log File
----------------------------------------------------------------------
tftp:sysinfo

Index        System Information Logging Commands
-----        ---------------------------------------------------------

Syslog Dump              Syslog File
------------------------ -----------------------
enabled                     bootflash:sysloginfo

Console>
```

Table 2-103 describes the fields in the **show system** command output.

Table 2-103 show system Command Output Fields

Field	Description
PS1-Status	Status of power supply 1 (ok, fan failed, faulty, or none).
PS2-Status	Status of power supply 2 (ok, fan failed, faulty, or none).
Fan-Status	Status of the fan (ok, faulty, or other).
Temp-Alarm	Status of whether the temperature alarm is off or on.
Sys-Status	System status (ok or faulty). Corresponds to system LED status.
Uptime d, h:m:s	Amount of time in days, hours, minutes, and seconds, that the system has been up and running.
Logout	Amount of time after which an idle session is disconnected.
PS1-Type	Part number of the power supply.
PS2-Type	Part number of the redundant power supply, if present.
Modem	Status of the modem status (enable or disable).
Baud	Baud rate to which the modem is set.
Traffic	Current traffic percentage.
Peak	Peak percentage of traffic on the backplane.
Peak-Time	Time stamp when peak percentage was recorded.
PS1 Capacity	Power supply 1 maximum capacity.
PS2 Capacity	Power supply 2 maximum capacity.
PS Configuration	Power supply configuration.
System Name	System name.

Table 2-103 show system Command Output Fields (continued)

Field	Description
System Location	System location.
System Contact	System contact information.
CC	Country code string.
Core Dump	Status of the core dump feature (enable or disable).
Core File	Flash file device and core dump file name.
System Logging	Status of system information logging (enabled or disabled).
Host	IP address or IP alias of the host.
File	Type of server and name of the file.
Interval	Number of minutes in between system information logging events.
Index	Number of the show command entry in the system information logging list.
System Command	Show command whose output is logged to the TFTP or RCP server.
Syslog Dump	Status of the syslog dump feature (enable or disable).
Syslog File	Flash file device and syslog dump file name.
Backplane-Traffic	Current traffic percentage.
Fabric Chan	Number of the fabric channel.
Input	Percentage of fabric channel utilization for input.
Output	Percentage of fabric channel utilization for output.

Related Commands

set system baud
set system contact
set system core-dump
set system core-file
set system countrycode
set system crashinfo
set system location
set system modem
set system name
set system syslog-dump
set system syslog-file

show system health

To test system health and display the results of the tests, use the **show system health** command.

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Health tests are run on the following:

- Nonzero ASIC registers on all modules—Lists the nonzero registers that belong to the "errCounters" group defined for each ASIC on all modules. If the hardware design of the ASIC does not accommodate a special "errCounters" group, a predefined list of registers that might provide useful information regarding the ASIC is printed. Only Ethernet modules and supervisor engines currently support this test.
- Port-level error counters—Lists all the nonzero Catalyst 6500 series module counters. These counters are divided into three types that are based on the information that they carry: generic error counters, 802.3 error counters, and flow-control error counters.
- Software patch utilization—Counts the number of times a particular software patch is used.
- CPU and memory utilization—Warns users if the CPU is above 70 percent in the last five minutes. The test also tests the free pool of memory buffers for any possible broken links. The output lists the total available memory and the largest free block of available memory.

Examples

```
Console> show system health

Largest block available :265701552
Total Memory available  :269982080
Total Memory used       :35440704



L3 Switching Engine III:total patches:1 (1 records displayed)
Record No :1
Sun May 2 2004, 17:25:02:58
Reason:<reason>


EOB:No entries found


L2 Non zero registers -
dbus_timeout                                = 0x1
```

```
rbus_timeout                                 = 0x1

L3 Non zero registers -
none.


Inband non-zero error statistics information -
RsrcErrors                                   = 00000087


The following Driver error counters are non zero -
rx crc err                                   = 18
MC flag but UC pkt                           = 14005


Module 1 :WS-X6148X2-RJ-45 non-zero error counters -

BUS ASIC 1:
0073:SP_CC_S_LO_PKT_CNT_LO                    = 0061
0095:SP_TW_S_NEG_PLD_ERR_CNT                  = 0030
00B6:SP_RI_S_PKT_CNT_LO                       = 0061
014A:SP_TI_CFG                                = 0092
01EC:SP_CI_S_LO_PKT_CNT_HI                    = 11C7
01EE:                                         = FFFF

OUTPUT PORT ASIC 1:
none.

INPUT PORT ASIC 1:
none.

PORT ASIC 1:
none.

BUS ASIC 2:
01EC:SP_CI_S_LO_PKT_CNT_HI                    = 004D
01EE:                                         = F50E

OUTPUT PORT ASIC 2:
none.

INPUT PORT ASIC 2:
none.

PORT ASIC 2:
none.

<truncated output>
.....
Non-zero port counters for 2/2 -
18:rxHCDropEvents                             = 32
 1:rxUndersizedPkts                           = 1
 6:ifInErrors                                 = 32
 8:ifInDiscards                               = 32
......
<truncated output>
Console>
```

Related Commands

show counters
show proc
show system sanity

show system highavailability

To display the system high-availability configuration settings, use the **show system highavailability** command.

show system highavailability

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the system high-availability configuration settings:

```
Console> (enable) show system highavailability
Highavailability:disabled
Highavailability versioning:disabled
Highavailability Operational-status:OFF(high-availability-not-enabled)
Console> (enable)
```

Related Commands

set system highavailability
set system highavailability versioning

show system info-log

To display the configuration of the system information logging feature, use the **show system info-log** command.

show system info-log

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the system information logging configuration:

```
Console> (enable) show system info-log
System Logging  Host             File                                Interval
--------------  ---------------  ----------------------------------- --------
Enabled         10.5.2.10        tftp:logging                        1500
Index        System Command
-----        ----------------------------------------------------------
    1        show version
    2        show module
    3        show version
    4        show config
Console> (enable)
```

Table 2-104 describes the fields in the **show system** command output.

Table 2-104 show system info-log Command Output Fields

Field	Description
System Logging	Status of system information logging (enabled or disabled).
Host	IP address or IP alias of the host.
File	Type of server and name of the file.
Interval	Number of minutes in between system information logging events.
Index	Number of the show command entry in the system information logging list.
System Command	Show command whose output is logged to the TFTP or RCP server.

Related Commands

clear config
clear system info-log command
set system info-log

show system profile

To display the system profile configuration, use the **show system profile** command.

show system profile

Syntax Description

This command has not arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to display the system profile configuration:

```
Console> (enable) show system profile
Lockdown profile is configured on the system using bootflash:test.cfg
Block                 Configured     Status             Operation Status
-------                  -------------------------              --------------------
Global                Enable                                  complete
Module 1            Enable                                  pending
Module 2            Disable                                 none
Module 3            Enable                                  running
Console> (enable)
```

Related Commands

clear config
clear system profile
set system profile

show system sanity

To display the output for the sanity checks that the system has performed, use the **show system sanity** command.

show system sanity

Syntax Description

This command has not arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **show system sanity** command runs a series of checks on your configuration and highlights possible conditions that could lead to problems with your configuration.

Examples

This example shows how to display the output for sanity checks:

```
Console> (enable) show system sanity
Status of the default gateway is:
172.20.52.1 is alive

Please check your confreg value : 0x10f.

Invalid boot image slot0:cat6000-sup2k8.8-3-0-133-BOC.bin specified in the bootstring.
Please check your boot string.
Invalid boot image bootflash:cat6000-sup2k8.7-5-0-98.bin specified in the boot string.
Please check your boot string.
None of the images specified in the boot string are valid.
Please specify at least one valid image in the boot string to ensure the switch
is in a bootable state.

The value for Community-Access on read-only operations for SNMP is the same as default.
Please verify that this is the best value from a security point of view.

The value for Community-Access on read-write operations for SNMP is the same as
default.
Please verify that this is the best value from a security point of view.

The value for Community-Access on read-write-all operations for SNMP is the same
as default.
Please verify that this is the best value from a security point of view.

UDLD has been disabled globally - port-level UDLD sanity checks are being bypassed.

The following ports have receive flowControl disabled:
3/1,3/48
```

```
The following vlans have max age on the spanning tree root different from the default:
1-6,10,20,50,100,152,200,300,400,500,521-522,524,570,776,850,917,999

The following vlans have forward delay on the spanning tree root different from the
default:
1-6,10,20,50,100,152,200,300,400,500,521-522,524,570,776,850,917,999

The following vlans have hello time on the spanning tree root different from the default:
2-6,10,20,50,100,152,200,300,400,500,521-522,524,570,776,850,917,999

Please check the status of the following modules:2

Module 8 failed the following tests :
Port LoopBack Test

Console> (enable)
```

Related Commands

show system

show system supervisor-update

To display the Erasable Programmable Logic Device (EPLD) upgrade process configuration, use the **show system supervisor-update** command.

show system supervisor-update

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the EPLD upgrade configuration:

```
Console> show system supervisor-update
Supervisor EPLD update: disabled
Console>
```

Related Commands

set system supervisor-update

show system switchmode

To display the system switching mode setting, use the **show system switchmode** command.

show system switchmode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the system switching mode:

```
Console> show system switchmode
Switching-mode allow:truncated
Switching-mode threshold:2
Console>
```

Related Commands

set system switchmode allow

show tacacs

To display the TACACS+ protocol configuration, use the **show tacacs** command.

show tacacs [**noalias**]

Syntax Description

noalias	(Optional) Forces the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the TACACS+ protocol configuration:

```
Console> show tacacs
Login Authentication: Console Session   Telnet Session
---------------------  ----------------  ----------------
tacacs                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Enable Authentication:Console Session   Telnet Session
---------------------- ----------------- ----------------
tacacs                 disabled          disabled
local                  enabled(primary)  enabled(primary)

Tacacs login attempts:3
Tacacs timeout:5 seconds
Tacacs direct request:disabled

Tacacs-Server                              Status
----------------------------------------   -------
171.69.193.114                             primary
Console>
```

Table 2-105 describes the fields in the **show tacacs** command output.

Table 2-105 show tacacs Command Output Fields

Field	Description
Login authentication	Display of the login authentication types.
Console Session	Status of whether the console session is enabled or disabled.
Telnet Session	Status of whether the Telnet session is enabled or disabled.
Enable Authentication	Display of the enable authentication types.
Tacacs login attempts	Number of failed login attempts allowed.

Table 2-105 show tacacs Command Output Fields (continued)

Field	Description
Tacacs timeout	Time in seconds to wait for a response from the TACACS+ server.
Tacacs direct request	Status of whether TACACS+ directed-request option is enabled or disabled.
Tacacs-Server	IP addresses or IP aliases of configured TACACS+ servers.
Status	Primary TACACS+ server.

Related Commands

set tacacs attempts
set tacacs directedrequest
set tacacs key
set tacacs server
set tacacs timeout

show tech-support

To display system and configuration information you can provide to the Cisco Technical Assistance Center when reporting a problem, use the **show tech-support** command.

show tech-support [{**module** *mod*} | {**port** *mod/port*}] [**vlan** *vlan*] [**mistp-instance** *instance*] [**mst** *instance*] [**memory**] [**config**]

Syntax Description

module *mod*	(Optional) Specifies the module number of the switch ports.
port *mod/port*	(Optional) Specifies the module and port number of the switch ports.
vlan *vlan*	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
mistp-instance *instance*	(Optional) Specifies the MISTP instance number; valid values are from 1 to 16.
mst *instance*	(Optional) Specifies the MST instance number; valid values are from 0 to 15.
memory	(Optional) Displays memory and processor state data.
config	(Optional) Displays switch configuration.

Defaults

By default, this command displays the output for technical-support-related **show** commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration, memory, module, port, instance, and VLAN data.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Caution Avoid running multiple **show tech-support** commands on a switch or multiple switches on the network segment. Doing so may cause spanning tree instability.

The **show tech-support** command may time out if the configuration file output takes longer to display than the configured session timeout time. If this happens, enter a **set logout** *timeout* value of 0 to disable automatic disconnection of idle sessions or enter a longer *timeout* value.

The **show tech-support** command output is continuous; it does not display one screen at a time. To interrupt the output, press **Ctrl-C**.

If you specify the **config** keyword, the **show tech-support** command displays the output of these commands:

- **show config**
- **show flash**
- **show log**

- **show microcode**
- **show module**
- **show port**
- **show spantree active**
- **show spantree summary**
- **show system**
- **show test**
- **show trunk**
- **show version**
- **show vlan**

Note If MISTP is running, the output from the **show spantree mistp-instance active** and **show spantree summary mistp-instance** commands are displayed instead of the output from the **show spantree active** and **show spantree summary** commands.

Note If MST is running, the output from the **show spantree mst** and **show spantree summary mst** commands are displayed instead of the output from the **show spantree active** and **show spantree summary** commands.

If you specify the **memory** keyword, the **show tech-support** command displays the output of these commands:

- **ps**
- **ps -c**
- **show cam static**
- **show cam system**
- **show flash**
- **show memory buffers**
- **show microcode**
- **show module**
- **show proc**
- **show proc mem**
- **show proc cpu**
- **show system**
- **show spantree active**
- **show version**

If you specify a module, port, or VLAN number, the system displays general system information and information for the component you specified.

Related Commands

See the commands listed in the "Usage Guidelines" section.

show test

To display the errors reported from the diagnostic tests, the diagnostic level, and the action that the supervisor engine takes after a diagnostics test failure, use the **show test** command.

show test [*mod* | **all**]

show test diaglevel

show test diagfail-action

Syntax Description

mod	(Optional) Number of the module. If you do not specify a number, test statistics are given for the general system as well as for the supervisor engine.
all	(Optional) Displays errors from diagnostic tests for all modules.
diaglevel	Displays the diagnostic level.
diagfail-action	Displays the action that the supervisor engine takes after a diagnostics test failure.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Only error conditions are displayed. If there are no errors, PASS is displayed in the Line Card Status field.

Examples

This example shows the error display for module 2:

```
Console> show test 2

Module 2 : 2-port 1000BaseX Supervisor
Network Management Processor (NMP) Status: (. = Pass, F = Fail, U = Unknown)
  ROM:  .   Flash-EEPROM: .   Ser-EEPROM: .   NVRAM: .   EOBC Comm: .

Line Card Firmware Status for Module 2 : PASS

Port Status :
  Ports 1  2
  -----------
        .  .

Line Card Diag Status for Module 2  (. = Pass, F = Fail, N = N/A)

 Module 2
  Cafe II Status :
        NewLearnTest:                 .
        IndexLearnTest:               .
        DontForwardTest:          .
        DontLearnTest:            .
        ConditionalLearnTest:     .
        BadBpduTest:              .
        TrapTest:                 .
 Loopback Status [Reported by Module 2] :
  Ports 1  2
  -----------
        .  .

 Channel Status :
  Ports 1  2
  -----------
        .  .
```

This example shows the error display for module 3:

```
Console> show test 3

Module 3 : 12-port 1000BaseX Ethernet

Line Card Firmware Status for Module 3 : PASS

Port Status :
  Ports 1  2  3  4  5  6  7  8  9  10 11 12
  -----------------------------------------
        .  .  .  .  .  .  .  .  .  .  .  .
Line Card Diag Status for Module 3  (. = Pass, F = Fail, N = N/A)
 Loopback Status [Reported by Module 3] :
  Ports 1  2  3  4  5  6  7  8  9  10 11 12
  -----------------------------------------
        .  .  .  .  .  .  .  .  .  .  .  .

 Channel Status :
  Ports 1  2  3  4  5  6  7  8  9  10 11 12
  -----------------------------------------
        .  .  .  .  .  .  .  .  .  .  .  .
```

This example shows the display when errors are reported by the LCP for module 3:

```
Console> show test 3

Module 3 : 12-port 1000BaseX Ethernet

Line Card Firmware Status for Module 3 : FAIL
 Error                                                          Device Number
 ------------------------------------------------------------  ------------------------
 Port asic error                                                1,2,5,12
 CPU error                                                      0
Line Card Diag Status for Module 3  (. = Pass, F = Fail, N = N/A)
 Loopback Status [Reported by Module 1] :
  Ports 1  2  3  4  5  6  7  8  9  10 11 12
  -----------------------------------------
        .  .  .  .  .  .  .  .  .  .  .  .

 Channel Status :
  Ports 1  2  3  4  5  6  7  8  9  10 11 12
  -----------------------------------------
        .  .  .  .  .  .  .  .  .  .  .  .
```

This example shows the display if you do not specify a module:

```
Console> show test

Environmental Status (. = Pass, F = Fail, U = Unknown, N = Not Present)
  PS1:.     PS2:N     PS1 Fan:.     PS2 Fan:N
  Chassis-Ser-EEPROM:.     Fan:.
  Clock(A/B):A         Clock A:.     Clock B:.
  VTT1:.    VTT2:.    VTT3:.

Module 1 :2-port 1000BaseX Supervisor
Network Management Processor (NMP) Status:(. = Pass, F = Fail, U =
Unknown)
  ROM: .   Flash-EEPROM:.   Ser-EEPROM:.   NVRAM:.   EOBC Comm:.

Line Card Firmware Status for Module 1 :PASS

Port Status :
  Ports 1  2
  -----------
        .  .

Line Card Diag Status for Module 1  (. = Pass, F = Fail, N = N/A)

Module 1
  Earl IV Status :
        NewLearnTest:             .
        IndexLearnTest:           .
        DontForwardTest:          .
        DontLearnTest:            .
        ConditionalLearnTest:     .
        BadBpduTest:              .
        TrapTest:                 .
        MatchTest:                .
        SpanTest:                 .
        CaptureTest:              .
Loopback Status [Reported by Module 1] :
  Ports 1  2
  -----------
        .  .

Channel Status :
  Ports 1  2
  -----------
        .  .
```

This example shows how to display diagnostic level status:

```
Console> show test diaglevel
Diagnostic mode at last bootup : minimal
Diagnostic mode at next reset  : bypass
Console>
```

This example shows how to display the action that the supervisor engine takes after a diagnostics test failure:

```
Console> show test diagfail-action
Diagnostic failure action for SUP at last bootup : offline
Diagnostic failure action for SUP at next reset  : ignore
Console>
```

Table 2-106 describes the possible fields in the **show test** command output. The fields shown depend on the module type queried.

Table 2-106 show test Command Output Fields

Field	Description
Environmental Status	Test results that apply to the general system environment.
PS (3.3V)	Test results for the 3.3 V power supply.
PS (12V)	Test results for the 12 V power supply.
PS (24V)	Test results for the 24 V power supply.
PS1	Test results for power supply 1.
PS2	Test results for power supply 2.
Temperature	Test results for the temperature.
Fan	Test results for the fan.
Module #	Test results that apply to the module #. The module type is indicated as well.
Network Management Processor (NMP) Status	Test results that apply to the NMP on the supervisor engine module.
ROM	Test results for the ROM.
Flash-EEPROM	Test results for the Flash EEPROM.
Ser-EEPROM	Test results for the serial EEPROM.
NVRAM	Test results for the NVRAM.
EARL Status	Fields that display the EARL status information.
NewLearnTest	Test results for the NewLearn test (EARL).
IndexLearnTest	Test results for the IndexLearn test (EARL).
DontForwardTest	Test results for the DontForward test (EARL).
MonitorTest	Test results for the Monitor test (EARL).
DontLearn	Test results for the DontLearn test (EARL).
FlushPacket	Test results for the FlushPacket test (EARL).
ConditionalLearn	Test results for the ConditionalLearn test (EARL).
EarlLearnDiscard	Test results for the EarlLearnDiscard test (EARL).
EarlTrapTest	Test results for the EarlTrap test (EARL).
LCP Diag Status for Module 1	Test results for the specified module.
CPU	Test results for the CPU.
Sprom	Test results for the serial PROM.
Bootcsum	Test results for the Boot ROM checksum.
Archsum	Test results for the archive Flash checksum.
RAM	Test results for the RAM.
LTL	Test results for the local-target logic.
CBL	Test results for the color-blocking logic.

Table 2-106 show test Command Output Fields (continued)

Field	Description
DPRAM	Test results for the dual-port RAM.
SAMBA	Test results for the SAMBA chip.
Saints	Test results for the SAINT chips.
Pkt Bufs	Test results for the packet buffers.
Repeater	Test results for the repeater module.
FLASH	Test results for the Flash memory.
EOBC	Channel through which a module exchanges control messages with the other modules in the system.
Local Power	Status of the DC converter on a module that supplies power to the entire module except the power management block on the module.
Phoenix	Test results for the Phoenix.
TrafficMeter	Test results for the TrafficMeter.
UplinkSprom	Test results for the Uplink SPROM.
PhoenixSprom	Test results for the Phoenix SPROM.
MII Status	Test results for the MII ports.
SAINT/SAGE Status	Test results for the individual SAINT/SAGE chip.
Phoenix Port Status	Test results for the Phoenix ports.
Packet Buffer Status	Test results for the individual packet buffer.
Phoenix Packet Buffer Status	Test results for the Phoenix packet buffer.
Loopback Status	Test results for the loopback test.
Channel Status	Test results for the channel test.

Related Commands

set test diagfail-action
set test diaglevel

show time

To display the current time of day in the system clock, use the **show time** command.

show time

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the current time:

```
Console> show time
Wed Jan 12 2000, 14:18:52
Console>
```

The output shows the day of the week, month, day, year, hour, minutes, and seconds.

Related Commands

set time

show timezone

To display the current time zone and offset, use the **show timezone** command.

show timezone

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the current time zone and offset:

```
Console> show timezone
Timezone set to 'pst', offset from UTC is -8 hours
Console>
```

Related Commands

clear timezone
set timezone

show top

To start the TopN process, use the **show top** command.

show top [*N*] [*metric*] [**interval** *interval*] [*port_type*] [**background**]

Syntax Description

N	(Optional) Number of ports displayed; valid values are **1** to a maximum number of physical ports.
metric	(Optional) Port statistic to sort on; valid values are as follows: **util**—utilization **bytes**—in/out bytes **pkts**—in/out packets **bcst**—in/out broadcast packets **mcst**—in/out multicast packets **errors**—in errors **overflow**—buffer overflow
interval	(Optional) Specifies duration of sample (in seconds).
interval	(Optional) Number of seconds for sample; valid values are **0** and from 10 to 999 seconds. If the value is 0, the N topmost ports by absolute counter values are displayed.
port_type	(Optional) Type of switch ports to use for report; valid values are as follows: **all**—All port types are used **eth**—All Ethernet port types are used **10e**—10-Mbps Ethernet ports types are used **fe**—Fast Ethernet port types are used **ge**—Gigabit Ethernet port types are used **10ge**—10-Gigabit Ethernet port types are used
background	(Optional) Specifies the TopN report not to print to the screen when the task is done. Instead, a notification is sent out when the reports are ready.

Defaults

The defaults are as follows:

- Number of ports displayed is **20**.
- Port statistics to report on is **util**.
- Sample duration is **30** seconds.
- Switch port type is **all**.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

You can terminate TopN processes with the **background** option specified only by using the **clear top** [*report_num*] command.

TopN reports with the **background** option specified are not displayed on the screen unless you enter a **show top report** [*report_num*] command.

If you do not specify the **background** option, the output TopN results are dumped to the screen when the task is done, and the results are printed one time only and are not saved.

You can terminate TopN processes (without the **background** option) by pressing **Ctrl-C** in the same Telnet or console session, or by entering a **clear top** [*report_num*] command from a separate Telnet or console session. The prompt is not printed before the TopN report completely displays. Other commands are blocked until the report has displayed.

Examples

This example shows how to start the TopN process with the **background** option:

```
Console> show top 10 util interval 600 background
03/09/2000,14:05:38:MGMT-5: TopN report 2 started by telnet/172.20.22.7/.
Console>
03/09/2000,14:15:38:MGMT-5: TopN report 2 available.
```

This example shows how to start the TopN process without the **background** option:

```
Console> show top 10 util interval 600
Start Time:      03/19/2000,12:04:16
End Time:        03/19/2000,12:14:18
PortType:        all
Metric:          util
Port  Band- Uti Tx/Rx-bytes          Tx/Rx-pkts Tx/Rx-bcst Tx/Rx-mcst In-  Buf-
      width  %                                                        err  Ovflw
----- ----- --- -------------------- ---------- ---------- ---------- ---- -----
 1/1  100      0 65433                824        0          719        0     0
 5/48 10   0 3543             45       0        34       0    0
 5/47 10   0 45367           124       0        219      0    0
 5/46 10   0 23456           49        0        108      0    0
Console>
```

This example shows how to start the TopN process for a specific port type:

```
Console> show top 5 10e interval 0
Start Time:    03/09/2000,11:03:21
End Time:      03/09/2000,11:03:21
PortType:      10Mbps Ethernet
Metric:        util
Port  Band- Uti Bytes                Pkts       Bcst       Mcst       Error Over
      width  %  (Tx + Rx)            (Tx + Rx)  (Tx + Rx)  (Tx + Rx)  (Rx)  flow
----- ----- --- -------------------- ---------- ---------- ---------- ----- ----
2/1     10   0                    0          0          0          0     0    0
3/12  auto   0                    0          0          0          0     0    0
3/11  auto   0                    0          0          0          0     0    0
3/10  auto   0                    0          0          0          0     0    0
3/9   auto   0                    0          0          0          0     0    0
Console>
```

Related Commands

clear top
show top report

show top report

To list all TopN processes and specific TopN reports, use the **show top report** command.

show top report [*report_num*]

Syntax Description

report_num	(Optional) TopN report number for each process.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify the *report_num* value, this command lists all the active TopN processes and all the available TopN reports for the switch. Each process is associated with a unique report number. All TopN processes (both with and without a background option) are shown in the list.

An asterisk displayed after the pending status field indicates that it is not a background TopN and the results are not saved.

Examples

This example shows how to display all the active TopN processes and all the available TopN reports for the switch:

```
Console> show top report
Rpt  Start time          Int N   Metric      Status   Owner (type/machine/user)
---  ------------------- --- --- ----------  -------- -------------------------
  1  03/09/2000,11:34:00 60  20  Tx/Rx-Bytes done     telnet/172.20.22.7/
  2  03/09/2000,11:34:08 600 10  Util        done     telnet/172.34.39.6/
  4  03/09/2000,11:35:17 300 20  In-Errors   pending  Console//
  5  03/09/2000,11:34:26 60  20  In-Errors   pending* Console//
Console>
```

This example shows an attempt to display a TopN report 5 (shown in the first example) that is still in pending status:

```
Console> show top report 5
Rpt  Start time          Int N   Metric     Status   Owner (type/machine/user)
---  ------------------- --- --- ---------- -------- -------------------------
  5  03/09/2000,11:34:26 60  20  In-Errors   pending* Console//
Console>
```

This example shows how to display the available TopN report 2 (shown in the first example) for the switch:

```
Console> show top report 2
Start Time:     03/09/2000,11:34:00
End Time:       03/09/2000,11:34:33
PortType:       all
Metric:         util
Port  Band- Uti Tx/Rx-bytes          Tx/Rx-pkts Tx/Rx-bcst Tx/Rx-mcst In-  Buf-
      width  %                                                         err  Ovflw
----- ----- --- -------------------- ---------- ---------- ---------- ---- -----
 /15  100   88  98765432109876543210 9876543210 98765      12345      123  321
 5/48 10    75  44532                5389       87         2          0    0
 5/47 10    67  5432                 398        87         2          0    0
 5/46 10    56  1432                 398        87         2          0    0
 5/45 10    54  432                  398        87         2          0    0
 5/44 10    48  3210                 65         10         10         15   5
 5/43 10    45  432                  5398       87         2          2    0
 5/42 10    37  5432                 398        87         2          0    0
 5/41 10    36  1432                 398        87         2          0    0
 5/40 10    14  2732                 398        87         2          0    0
Console>
```

Related Commands

clear top
show top

show traffic

To display traffic and peak information, use the **show traffic** command.

show traffic

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows the traffic and peak information display on a system configured with the Supervisor Engine 1 with Layer 3 Switching Engine (WS-F6K-PFC):

```
Console> (enable) show traffic
Threshold: 100%
Traffic Peak Peak-Time
------- ---- -------------------------
  0%      0% Tue Apr 25 2000, 12:07:32
Console> (enable)
```

This example shows the traffic and peak information display on a system configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC II):

```
Console> (enable) show traffic
Threshold:100%
Backplane-Traffic Peak Peak-Time
----------------- ---- -------------------------
  0%                0% Thu Jul 27 2000, 14:03:27

Fab Chan Input Output
-------- ----- ------
       0    0%     0%
       1    0%     0%
       2    0%     0%
       3    0%     0%
       4    0%     0%
.
.
.
      14    0%     0%
      15    0%     0%
      16    0%     0%
      17    0%     0%
```

Related Commands

show system

show trunk

To display trunking information for the switch, use the **show trunk** command.

show trunk [*mod*[*/port*]] [**detail**] [**extended-range**]

Syntax Description

mod	(Optional) Number of the module.
port	(Optional) Number of the port on the module.
detail	(Optional) Shows detailed information about the specified trunk port.
extended-range	(Optional) Shows trunking information for extended-range VLANs.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Entering the **show trunk** command without specifying a module or port number displays only the actively trunking ports. To display the trunking configuration for a port that is not actively trunking, specify the module and port number of the port you want to display. The MSM port displays as a port that is always trunking, with allowed and active VLANs for each VLAN configured on the MSM.

Entering the **show trunk** command displays untagged traffic received over the dot1q trunk. For ISL trunks, packets are tagged on all VLANs (including native VLANs).

In the **show trunk detail** command output, the Peer-Port field displays either the module and port number of the peer connection or multiple or unknown. Multiple is displayed if connected to shared media, and unknown is displayed if DTP is not running on the other side.

If you enter the **show trunk** command on a trunk where a VTP domain mismatch exists, an asterisk is displayed after the trunk status and this message appears:

```
* - indicates vtp domain mismatch.
```

In the **show trunk** command output, the ports and VLANs listed in the spanning tree forward state and not pruned fields are the same regardless of whether or not VTP or GVRP is running.

Examples

This example shows how to display trunking information for the switch:

```
Console> show trunk
* - indicates vtp domain mismatch
# - indicates dot1q-all-tagged enabled on the port
Port Mode Encapsulation Status Native vlan
----- ------- ------------------- --------- ----------------
1/1 desirable dot1q trunking# 1
1/2 auto n-dot1q trunking 1
Console>
```

This example shows how to display detailed information about the specified trunk port:

```
Console> show trunk 1/1 detail
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      auto         negotiate      not-trunking  1

Port      Peer-Port  Mode         Encapsulation  Status
--------  ---------  -----------  -------------  ------------
 1/1      2/3        auto         n-isl          not-trunking

Port      TrunkFramesTx         TrunkFramesRx         WrongEncap
--------  --------------------  --------------------  ----------
 1/1                         0                     0           0

Port      Vlans allowed on trunk
--------  ----------------------------------------------------------------------
 1/1      1-1005

Port      Vlans allowed and active in management domain
--------  ----------------------------------------------------------------------
 1/1      1

Port      Vlans in spanning tree forwarding state and not pruned
--------  ----------------------------------------------------------------------
 1/1
Console>
```

This example shows how to display detailed information about the specified trunk port that has a VTP domain mismatch:

```
Console> show trunk 3/1 detail
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 3/1      auto         negotiate      not-trunking*  1

Port      Peer-Port  Mode         Encapsulation  Status
--------  ---------  -----------  -------------  ------------
 3/1      2/3        auto         n-isl          not-trunking

Port      TrunkFramesTx         TrunkFramesRx         WrongEncap
--------  --------------------  --------------------  ----------
 3/1                         0                     0           0

Port      Vlans allowed on trunk
--------  ----------------------------------------------------------------------
 3/1      1-1005
```

```
Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 3/1      2

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 3/1
Console>
```

This example shows how to include information about extended-range VLANs:

```
Console> show trunk extended-range
Port       Status            Vlans allowed on trunk
--------   --------------    --------------------------------------
1/2         Trunking          1-1005, 2000-4094
2/2         Trunking          1-1005, 2100-4094
2/3         Non-Trunking      1-1005, 1025-2000, 3001-4094
............
Console>
```

Table 2-107 describes the fields in the **show trunk** command outputs.

Table 2-107 show trunk Command Output Fields

Field	Description
Port	Module and port numbers.
Mode	Trunk administrative status of the port (on, off, auto, desirable, or nonegotiate).
Encapsulation	Trunking type configured by administration.
Status	Status of whether the port is trunking or nontrunking.
Native vlan	Number of the native VLAN for the trunk link (the VLAN for which untagged traffic can be transmitted and received over the dot1q trunk).
Vlans allowed on trunk	Range of VLANs allowed to go on the trunk (default is 1 to 1000).
Vlans allowed and active in management domain	Range of active VLANs within the allowed range.
Vlans in spanning tree forwarding state and not pruned	Range of VLANs that actually go on the trunk with Spanning Tree Protocol forwarding state.
Peer-Port	Peer connection information (module and port number of peer connection, multiple, or unknown).
TrunkFramesTx	Number of ISL/802.1Q frames transmitted on a port.
TrunkFramesRx	Number of ISL/802.1Q frames received on a port.
WrongEncap	Number of frames with the wrong encapsulation received on a port.

Related Commands

set trunk

show udld

To display UDLD information, use the **show udld** command.

show udld

show udld port [*mod*[/*port*]]

Syntax Description

port	Specifies module and ports or just modules.
mod	(Optional) Number of the module for which UDLD information is displayed.
port	(Optional) Number of the port for which UDLD information is displayed.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to find out whether or not UDLD is enabled:

```
Console> show udld
UDLD      : enabled
Message Interval  :15 seconds
Console>
```

This example shows how to display UDLD information for a specific module and port:

```
Console> show udld port 2/1
UDLD              :enabled
Message Interval  :15 seconds
Port     Admin Status  Aggressive Mode  Link State
-------- ------------  ---------------  ----------------
 2/1     enabled       disabled         undertermined
Console>
```

This example shows how to display UDLD information for all ports on a specific module:

```
Console> (enable) show udld port 1
UDLD              :enabled
Message Interval  :15 seconds
Port     Admin Status  Aggressive Mode  Link State
-------- ------------  ---------------  ----------------
1/1      disabled      disabled         not applicable
1/2      disabled      enabled          not applicable
Console>
```

Table 2-108 describes the fields in the **show udld** command output.

Table 2-108 show udld Command Output Fields

Field	Description
UDLD	Status of whether UDLD is enabled or disabled.
Port	Module and port numbers.
Admin Status	Status of whether administration status is enabled or disabled.
Aggressive Mode	Status of whether aggressive mode is enabled or disabled.
Link State	Status of the link: undetermined (detection in progress, UDLD has been disabled on the neighbors), not applicable (UDLD is not supported on the port, UDLD has been disabled on the port, or the port is disabled), shutdown (unidirectional link has been detected and the port disabled), bidirectional (bidirectional link has been detected).

Related Commands

set udld
set udld aggressive-mode
set udld interval

show users

To show if the console port is active and to list all active Telnet sessions with the IP address or IP alias of the originating host, use the **show users** command.

show users [**noalias**]

Syntax Description

noalias	(Optional) Forces the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the users of the active Telnet sessions:

```
Console> show users
Session-id    Session      User             Location
------------  ------------ ---------------  -------------------------
0           * console
1             ssh          dkoya            10.76.82.24
2             telnet       dkoya            cbin3-view2.cisco.com
Console>
```

Related Commands

disconnect

show version

To display software, hardware, and web interface version information, use the **show version** command.

show version [*mod*]

show version epld [*mod*]

Syntax Description

mod	(Optional) Number of the module.
epld	Displays the Erasable Programmable Logic Device (EPLD) upgrade process configuration for non-supervisor engine modules.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the software and hardware versions on systems configured with the Supervisor Engine 1 with Layer 3 Switching Engine (WS-F6K-PFC):

```
Console> show version
WS-C6009 Software, Version NmpSW: 6.2(0.11)KEY
Copyright (c) 1995-2000 by Cisco Systems
NMP S/W compiled on Oct  5 2000, 01:18:33

System Bootstrap Version: 5.2(1)

Hardware Version: 1.0  Model: WS-C6009  Serial #: SCA030900JA

Mod Port Model               Serial #    Versions
--- ---- ------------------- ----------- --------------------------------------
1   2    WS-X6K-SUP1A-2GE    SAD03392376 Hw : 1.0
                                         Fw : 5.2(1)
                                         Fw1: 5.1(1)CSX
                                         Sw : 6.2(0.11)KEY
                                         Sw1: 6.2(0.11)KEY
         L3 Switching Engine SAD03365068 Hw: 1.0
3   2    WS-X6380-NAM        JAB0343055Y Hw : 0.201
                                         Fw : 4B4LZ0XA
                                         Fw1: 4.2(0.24)DAY68
                                         Sw : 1.1(0.20)
                                         Sw1: 6.2(0.11)KEY
5   48   WS-X6248-RJ-45      SAD03181291 Hw : 1.0
                                         Fw : 4.2(0.24)VAI78
                                         Sw : 6.2(0.11)KEY
15  1    WS-F6K-MSFC         SAD03366264 Hw : 1.2
                                         Fw : 12.1(2)E,
                                         Sw : 12.1(2)E,
          DRAM                    FLASH                   NVRAM
   Module Total   Used    Free    Total   Used    Free    Total Used  Free
   ------ ------- ------- ------- ------- ------- ------- ----- ----- -----
   1       65408K  45402K  20006K  16384K   8683K   7701K  512K  253K  259K

   Uptime is 1 day, 19 hours, 54 minutes
   Console> (enable)
```

This example shows how to display version information for a specific module:

```
Console> (enable) show version 3
Mod Port Model               Serial #    Versions
--- ---- ------------------- ----------- --------------------------------------
3   2    WS-X6380-NAM        JAB0343055Y Hw : 0.201
                                         Fw : 4B4LZ0XA
                                         Fw1: 4.2(0.24)DAY68
                                         Sw : 1.1(0.20)
                                         Sw1: 6.2(0.11)KEY

Console> (enable)
```

This example shows how to display the software and hardware versions on systems configured with the Supervisor Engine 2 with Layer 3 Switching Engine II (PFC2):

```
Console> show version
WS-C6506 Software, Version NmpSW:6.1(0.142-Eng)
Copyright (c) 1995-2000 by Cisco Systems
NMP S/W compiled on Jul 27 2000, 18:36:52

System Bootstrap Version:6.1(194)

Hardware Version:2.0  Model:WS-C6506  Serial #:TBA04140397

Mod Port Model               Serial #    Versions
--- ---- ------------------- ----------- --------------------------------------
2   2    WS-X6K-SUP2-2GE     SAD041104M3 Hw :0.212
                                         Fw :6.1(194)
                                         Fw1:4.2(0.24)DAY84-Eng
                                         Sw :6.1(0.142-Eng)
                                         Sw1:6.1(0.142)
         L3 Switching Engine SAD04130E6X Hw :0.303
3   48   WS-X6248-RJ-45      SAD04140BZ1 Hw :1.2
                                         Fw :5.1(1)CSX
                                         Sw :6.1(0.142)
16  1    WS-F6K-MSFC2        SAD04040BP6 Hw :0.201
                                         Fw :12.1(0.11)EP1(0.43)
                                         Sw :12.1(0.11)EP1(0.43)

       DRAM                    FLASH                   NVRAM
Module Total   Used    Free    Total   Used    Free    Total Used  Free
------ ------- ------- ------- ------- ------- ------- ----- ----- -----
2      130944K  57916K  73028K  16384K  12003K   4381K  512K  257K  255K

Uptime is 0 day, 0 hour, 34 minutes
Console>
```

Table 2-109 describes the fields in the **show version** command output.

Table 2-109 show version Command Output Fields

Field	Description
NmpSW	Version number of the NMP software.
NMP S/W compiled on	Date and time that the NMP software was compiled.
System Bootstrap Version	System bootstrap version number.
Web Interface Version	Web interface version number.
Hardware Version	Hardware version number.
Model	Switch model number.
Serial #	Switch serial number.
Module	Module number.
Port	Number of ports on the module.
Model	Model number of the module.
Serial #	Serial number of the module.
Versions	Hardware, software, and firmware versions of the module.
Hw	Hardware version of the module.
Fw	Version of the boot code (for switching modules) or bootstrap (for the supervisor engine).
Fw1	Version of the firmware boot code (on the supervisor engine).
Sw	Version of the firmware runtime installed (on the switching module) or the software version (on the supervisor engine).
Sw1	Version of the firmware runtime (on the supervisor engine).
DRAM Total	Total dynamic RAM installed on the module.
Used	Amount of DRAM in use.
Free	Amount of available DRAM.
FLASH Total	Total Flash memory installed on the module.
Used	Amount of Flash memory in use.
Free	Amount of available Flash memory.
NVRAM Total	Total NVRAM installed on the module.
Used	Amount of NVRAM in use.
Free	Amount of available NVRAM.
Uptime is	Number of uninterrupted days, hours, minutes, and seconds the system has been up and running.

Related Commands

download

show vlan

To display VLAN information, use the **show vlan** command.

show vlan [**trunk**]

show vlan *vlans* [**notrunk**]

show vlan mapping

show vlan *type*

show vlan summary

show vlan firewall-vlan *mod*

Syntax Description

trunk	(Optional) Forces the display to show information only on trunk ports.
vlans	Number or range of VLANs; valid values are from 1 to 4094.
notrunk	(Optional) Forces the display to show information only on nontrunk ports.
mapping	Displays VLAN mapping table information.
type	Type of the VLAN; valid values are **ethernet**, **fddi**, **fddinet**, **trbrf**, or **trcrf**.
summary	Displays a summary of active, suspended, and extended VLANs.
firewall-vlan	Displays VLANs that are secured by a Firewall Services Module.
mod	Number of the module.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Each Ethernet switch port and Ethernet repeater group belong to only one VLAN. Trunk ports can be on multiple VLANs.

If you do not specify the VLAN number, all VLANs are displayed.

Examples

This example shows how to display information for all VLAN trunks:

```
Console> show vlan trunk
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
1    default                          active    5       2/1-2
                                                        6/4-8
10   VLAN0010                         active    18      6/1,6/3
11   VLAN0011                         active    19      6/2
```

```
20   VLAN0020                         active    20
21   VLAN0021                         active    21
30   VLAN0030                         active    22
31   VLAN0031                         active    23
1002 fddi-default                     active    6
1003 token-ring-default               active    9
1004 fddinet-default                  active    7
1005 trnet-default                    active    8       8

VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
1    enet  100001     1500  -      -      -      -    -        0      0
10   enet  100010     1500  -      -      -      -    -        0      0
11   enet  100011     1500  -      -      -      -    -        0      0
20   enet  100020     1500  -      -      -      -    -        0      0
21   enet  100021     1500  -      -      -      -    -        0      0
30   enet  100030     1500  -      -      -      -    -        0      0
31   enet  100031     1500  -      -      -      -    -        0      0
1002 fddi  101002     1500  -      -      -      -    -        0      0
1003 trcrf 101003     1500  0      0x0    -      -    -        0      0
1004 fdnet 101004     1500  -      -      0x0    ieee -        0      0
1005 trbrf 101005     1500  -      -      0x0    ibm  -        0      0


VLAN Inst DynCreated  RSPAN
---- ---- ---------- --------
1    1    static     disabled
10        static     disabled
11        static     disabled
20        static     disabled
21        static     disabled
30        static     disabled
31        static     disabled
1002 -    static     disabled
1003 1    static     disabled
1004 2    static     disabled
1005 -    static     disabled


VLAN AREHops STEHops Backup CRF 1q VLAN
---- ------- ------- ---------- -------
1003 7       7       off


Primary Secondary Secondary-Type Ports
------- --------- -------------- ------------
10      20        isolated       6/1,6/3
11      21        isolated       6/2
30      -         -
-       31        isolated
```

This example shows how to display the VLAN mapping table information:

```
Console> show vlan mapping
802.1q vlan     ISL vlan        Effective
------------------------------------------
3000            300             true
Console>
```

This example shows how to display information for a specific VLAN and type:

```
Console> show vlan 2 fddi
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
1002 fddi-default                     active    6


VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
2    fddi  101002     1500  -      -      -      -    -        0      0

VLAN Inst DynCreated  RSPAN
---- ---- ---------- --------
2    -    static     disabled
Console>
```

This example shows how to display information for nontrunk ports only on a specific VLAN:

```
Console> show vlan 2 notrunk
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
2    VLAN0002                         active    60


VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
2    enet  100002     1500  -      -      -      -    -        0      0


VLAN Inst DynCreated  RSPAN
---- ---- ---------- --------
2    -    static     disabled


VLAN AREHops STEHops Backup CRF 1q VLAN
---- ------- ------- ---------- -------

Console>
```

This example shows how to display extended-range VLANs:

```
Console> (enable) show vlan 4000
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
Unable to access VTP Vlan 4000 information.


VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
Unable to access VTP Vlan 4000 information.


VLAN Inst DynCreated  RSPAN
---- ---- ---------- --------
Unable to access VTP Vlan 4000 information.


VLAN AREHops STEHops Backup CRF 1q VLAN
---- ------- ------- ---------- -------

Console> (enable)
```

8.6 EFT Copy

This example shows how to display a summary of active, suspended, and extended VLANs:

```
Console> show vlan summary
Vlan status    Count  Vlans
-------------  ---------------------------------------------------------
VTP Active       504   1-100,102-500,1000,1002-1005

VTP Suspended      1   101

Extended           1   2000
Console>
```

Table 2-110 describes the fields in the **show vlan** command output.

Table 2-110 show vlan Command Output Fields

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
IfIndex	Number of the ifIndex.
Mod/Ports, VLANs	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN. Possible values are SRB and SRT; the default is SRB.
Inst	Instance number.
DynCreated	Status of whether the VLAN is created statically or dynamically.
RSPAN	Status of whether RSPAN is enabled or disabled.
AREHops	Maximum number of hops for All-Routes Explorer frames. Possible values are 1 through 13; the default is 7.
STEHops	Maximum number of hops for Spanning Tree Explorer frames. Possible values are 1 through 13; the default is 7.
Backup CRF	Status of whether the TrCRF is a backup path for traffic.
802.1Q Vlan	Number of the 802.1Q VLAN.
ISL Vlan	Number of the ISL VLAN.
Effective	Status of the VLAN. If the VLAN is active and its type is Ethernet, true is displayed; if not, false is displayed.
Primary	Number of the primary VLAN in a private VLAN.
Secondary	Number of the secondary VLAN in a private VLAN.

Table 2-110 show vlan Command Output Fields (continued)

Field	Description
Secondary-Type	Type of secondary VLAN port. Possible values are isolated, community, or -.
Ports	Number of the module and ports associated to a specific private VLAN pair.

Related Commands

set trunk
set vlan
show trunk

show vlan counters

To display counters for all VLANs or a range of VLANs, use the **show vlan counters** command.

show vlan counters [*vlans*]

Syntax Description

vlans	Number or range of VLANs; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The **show vlan counters** command is available only on the Supervisor Engine 2 and the Supervisor Engine 720.

Examples

This example shows how to display counters for VLAN 1:

```
Console> show vlan counters 1

Vlan    :1
L2-Unicast-Pkts                                 :3081
L3-In-Unicast-Pkts                              :0
L3-Out-Unicast-Pkts                             :0
L2-NonUnicast-Pkts + L3-In-NonUnicast-Pkts      :4021
L3-Out-NonUnicast-Pkts                          :0
L2-Unicast-Octets                               :238081
L3-In-Unicast-Octets                            :0
L3-Out-Unicast-Octets                           :0
L2-NonUnicast-Octets + L3-In-NonUnicast-Octets  :273025
L3-Out-NonUnicast-Octets                        :0
Console>
```

Table 2-111 describes the fields in the **show vlan counters** command output.

Table 2-111 show vlan counters Output Fields

Field	Description
L2-Unicast-Pkts	Layer 2 unicast packets forwarded per VLAN.
L3-In-Unicast-Pkts	Layer 3 unicast packets forwarded per input VLAN.
L3-Out-Unicast-Pkts	Layer 3 unicast packets forwarded per output VLAN.
L2-NonUnicast-Pkts + L3-In-NonUnicast-Pkts	Layer 2 nonunicast packets forwarded per VLAN and Layer 3 nonunicast packets forwarded per input VLAN.

Table 2-111 show vlan counters Output Fields (continued)

Field	Description
L3-Out-NonUnicast-Pkts	Layer 3 nonunicast packets forwarded per output VLAN.
L2-Unicast-Octets	Layer 2 unicast octets per VLAN.
L3-In-Unicast-Octets	Layer 3 unicast octets per input VLAN.
L3-Out-Unicast-Octets	Layer 3 unicast octets per output VLAN.
L2-NonUnicast-Octets + L3-In-NonUnicast-Octets	Layer 2 nonunicast octets per VLAN and Layer 3 nonunicast octets per input VLAN.
L3-Out-NonUnicast-Octets	Layer 3 nonunicast octets per output VLAN.

Related Commands

clear vlan counters

8.6 EFT Copy

show vlan verify-port-provisioning

To verify the status of the VLAN port-provisioning verification feature, use the **show vlan verify-port-provisioning** command.

show vlan verify-port-provisioning

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display the status of VLAN port-provisioning verification on all ports:

```
Console> show vlan verify-port-provisioning
Vlan Verify Port Provisioning feature disabled
Console>
```

Related Commands

set vlan verify-port-provisioning

show vmps

To display VMPS configuration information, use the **show vmps** command.

show vmps [**noalias**]

Syntax Description

noalias	(Optional) Forces the display to show IP addresses, not IP aliases.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display VMPS configuration information:

```
Console> show vmps
VMPS Server Status:
-------------------
Management Domain:     (null)
State:                 disabled
Operational Status:    inactive
TFTP Server:           default
TFTP File:             vmps-config-database.1
Fallback VLAN:         (null)
Secure Mode:           open
VMPS No Domain Req:    allow
VMPS Backup file name disk0:vmps_config_engineering
VMPS Auto-Save state   enabled

VMPS Client Status:
---------------------
VMPS VQP Version:      1
Reconfirm Interval:    60 min
Server Retry Count:    3
VMPS domain server:

No dynamic ports configured.
Console>

No dynamic ports configured.
Console>
```

Table 2-112 describes the fields in the **show vmps** command output.

Table 2-112 show vmps Command Output Fields

Field	Description
VMPS Server Status	Status of VMPS server.
Management Domain	Management domain supported by this server.
State	Status on whether VMPS is enabled or disabled.
Operational Status	VMPS status (active, inactive, or downloading).
TFTP Server	IP address of the VMPS server.
TFTP File	VMPS configuration filename.
Fallback VLAN	VLAN assigned if a VLAN is not assigned to a MAC address in the database.
Secure Mode	Secure mode status (open or secure).
VMPS No Domain Req	Status on whether the server accepts requests from clients with no domain name.
VMPS Backup file name	VMPS backup device and backup file name.
VMPS Auto-Save state	Status of the VMPS auto-save feature.
VMPS Client Status	Status of the VMPS client.
VMPS VQP Version	Version of VMPS VQP.
VMPS domain server	VMPS domain server name.

Related Commands

download
set vmps config-file
set vmps server
set vmps state

show vmps mac

To display the MAC-address-to-VLAN mapping table, use the **show vmps mac** command.

show vmps mac [*mac_addr*]

Syntax Description

mac_addr	(Optional) MAC address that allows you to see mapping information.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify a MAC address, the entire mapping table is displayed.

Examples

This example shows the entire MAC-address-to-VLAN mapping table:

```
Console> show vmps mac
MAC Address       VLAN Name Last Requestor  Port ID Last Accessed Last Response
----------------- --------- --------------- ------- ------------- -------------
00-00-c0-23-c8-34 Hardware  198.4.222.111   3/5     0, 01:25:30   Success
00-00-c0-25-c9-42 --NONE--  198.4.222.111   2/1     0, 05:20:00   Denied
Console>
```

Table 2-113 describes the fields in the **show vmps mac** command output.

Table 2-113 show vmps mac Command Output Fields

Field	Description
MAC Address	MAC address.
VLAN Name	VLAN name assigned to the MAC address.
Last Requestor	IP address of the client that last requested a VLAN assignment for this MAC address.
Port ID	Port ID in the last request.
Last Accessed	Time when the last request was processed for this MAC address.
Last Response	Response sent by the server for the last request.

Related Commands

show vmps

show vmps statistics

To display the VMPS statistics, use the **show vmps statistics** command.

show vmps statistics

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

The statistics shown are based on the results of the **reconfirm vmps** command.

Examples

This example shows how to display the VMPS statistics:

```
Console> show vmps statistics
VMPS Statistics:
Last Enabled At:                  2,01:30:05
Config Requests:                  20
Invalid Requests:                 0
Status 'Error' Responses:         0
Status 'Deny' Responses:          5
MAC Address of Last Failed Request: 00-60-00-cc-01-02
Console>
```

Table 2-114 describes the fields in the **show vmps statistics** command output.

Table 2-114 show vmps statistics Command Output Fields

Field	Description
Last Enabled At	Time when the VMPS was enabled.
Config Requests	Number of configuration requests.
Invalid Requests	Number of invalid requests.
Status ‘Error’ Responses	Number of error responses.
Status ‘Deny’ Responses	Number of “Access Denied” and “Port Shutdown” responses.
MAC Address of Last Failed Request	MAC address of the last request for which the response was not successful.

Related Commands

clear vmps statistics

show vmps vlan

To display all the MAC addresses assigned to a VLAN in the VMPS table, use the **show vmps vlan** command.

show vmps vlan *vlan_name*

Syntax Description

vlan_name	Name or number of the VLAN.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display all MAC addresses assigned to the VLAN named Hardware:

```
Console> show vmps vlan Hardware

MAC Address       VLAN Name Last Requestor  Port ID Last Accessed Last Response
----------------- --------- --------------- ------- ------------- -------------
00-00-c0-23-c8-34 Hardware  198.4.222.111   3/5     0, 01:25:30   Success
Console>
```

Table 2-115 describes the fields in the **show vmps vlan** command output.

Table 2-115 show vmps vlan Command Output Fields

Field	Description
MAC Address	MAC address.
VLAN Name	VLAN name assigned to the MAC address.
Last Requestor	IP address of the client that last requested a VLAN assignment for this MAC address.
Port ID	Port ID in the last request.
Last Accessed	Time when the last request was processed for this MAC address.
Last Response	Response sent by the server for the last request.

Related Commands

show vmps

show vtp

To display devices and conflicts between devices in the VLAN Trunk Protocol (VTP) version 3 domain, use the **show vtp** command.

show vtp {**devices** | **conflicts**}

Syntax Description

devices	Displays the VTP version 3 domain information.
conflicts	Forces the display to show only devices that are in conflict in the VTP version 3 domain.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows information about devices in the VTP version 3 domain:

```
Console> show vtp devices
Retrieving information from the domain. Waiting 5 seconds.

VTP Feature  Conf Revision Primary Server Device ID      Device Description
------------ ---- -------- -------------- -------------- ----------------------
VLAN         Yes  4        0005.3140.6400=0005.3140.6400 C6506-74-17>
VLAN         Yes  4        0005.3140.6400 00d0.0227.9c00 C6509-74-24>
Console>
```

Table 2-116 describes the fields in the **show vtp devices** command output.

Table 2-116 show vtp devices Command Output Fields

Field	Description
VTP Feature	Name of the VTP instance that propagates the VLAN database or the MST configuration database (VLAN or MST).
Conf	Indicates whether or not there is a conflict between the local device for the feature (VLAN database or MST configuration) and the answering device.
Revision	Revision number of the specified VTP feature.
Primary Server	MAC address of the primary server. If a device is configured with a database that it originated, an equal sign (=) appears between the Primary Server field and the Device ID field.
Device ID	MAC address of the device.
Device Description	Type of switch identified in the Device ID field.

Related Commands

set vtp

show vtp domain

To display VTP domain information, use the **show vtp domain** command.

show vtp domain

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display VTP domain information for a switch running VTP version 2:

```
Console> show vtp domain
Version      :running VTP2 (VTP3 capable)
Domain Name  :test                               Password  :not configured
Notifications:disabled                           Updater ID:10.6.29.20

Feature        Mode           Revision
-------------- -------------- -----------
VLANDB         Server         15
Console>
```

This example shows how to display VTP domain information for a switch running VTP version 3:

```
Console> show vtp domain
Version      :running VTP3
Domain Name  :cat-vtp3                           Password  :configured
Notifications:enabled                            Switch ID :0009.7b62.b080

Feature        Mode           Revision    Primary ID     Primary Description
-------------- -------------- ----------- -------------- ----------------------
VLAN           Primary Server 2           0009.7b62.b080 sw-fdv4
UNKNOWN        Transparent

Pruning             :disabled
VLANs prune eligible:2-1000
Console>
```

Table 2-117 describes the fields in the **show vtp domain** command output.

Table 2-117 show vtp domain Command Output Fields

Field	Description
Version	VTP version number (1, 2, or 3).
Domain Name	Name of the VTP domain.

Table 2-117 show vtp domain Command Output Fields (continued)

Field	Description
Notifications	Notifications to SNMP (enabled or disabled).
Password	Password configured, configured but hidden, or not configured.
Switch ID	MAC address of the local switch.
Feature	Database transported in the VTP domain.
Mode	VTP mode (server, client, transparent, off, or primary server).
Revision	VTP revision number used to exchange VLAN information.
Primary ID	MAC address of the primary switch.
Primary Description	Description of the primary switch.

Related Commands

set vtp
show vtp statistics

show vtp statistics

To display VTP statistics, use the **show vtp statistics** command.

show vtp statistics

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to display VTP statistics:

```
Console> show vtp statistics
VTP statistics:
summary advts received          0
subset  advts received          0
request advts received          0
summary advts transmitted       72
subset  advts transmitted       7
request advts transmitted       0
No of config revision errors    0
No of config digest errors      0

VTP pruning statistics:

Trunk    Join Transmitted Join Received Summary advts received from GVRP PDU
                                        non-pruning-capable device  Received
-------- ---------------- ------------- --------------------------  ----------
4/2       0                0             0                           0
```

Table 2-118 describes the fields in the **show vtp statistics** command output.

Table 2-118 show vtp statistics Command Output Fields

Field	Description
summary advts received	Total number of summary advts received.
subset advts received	Total number of subset advts received.
request advts received	Total number of request advts received.
summary advts transmitted	Total number of summary advts transmitted.
subset advts transmitted	Total number of subset advts transmitted.
request advts transmitted	Total number of request advts transmitted.

Table 2-118 show vtp statistics Command Output Fields (continued)

Field	Description
No of config revision errors	Number of config revision errors.
No of config digest errors	Number of config revision digest errors.
Trunk	Trunk port participating in VTP pruning.
Join Transmitted	Number of VTP-Pruning Joins transmitted.
Join Received	Number of VTP-Pruning Joins received.
Summary advts received from nonpruning-capable device	Number of Summary advts received from nonpruning-capable devices.
GVRP PDU Received	Number of GVRP messages received on VTP trunks.

Related Commands

clear vtp statistics
set vtp

show web-auth summary

To display a summary of information about the web-based proxy authentication session, use the **show web-auth summary** command.

show web-auth summary [*vlans*]

Syntax Description

vlans	(Optional) VLAN or range of VLANs; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If the **vlan** *vlan_id* keyword and argument are specified, a summary of information for the specified VLAN is displayed.

In the command output display, the following applies:

- The * indicates the RADIUS assigned value.
- The State field displays the current web-authentication state of the given host.

Examples

This example shows how to display a summary of information about the web-based proxy authentication session:

```
Console> (enable) show web-auth summary
Web-authentication enabled globally
Login-page location url http://proxyauth.cisco.com/login.html
Login-fail-page location url http://proxyauth.cisco.com/loginfail.html
session-timeout : 3600 secs
quiet timeout : 60 secs
Max Login attempt count: 3
------------------------------------------------------------------------------------------
--------------------------------
IP Address                 Interface      Web Auth State
     Session-Timeout   Leftover-Session-Time       VLAN
------------------------------------------------------------------------------------------
------------------------------------------------
9.9.150. 1                      1/1             Authenticated
              * 7200                         200                           100
9.9.150.2
                      1/2             Authenticating               3600
        -                               100
9.9.150.3                       1/3             Authentication-fai
         3600                           -                              100
9.9.160.10                     1/4             Held
               3600                           -                              200
```

```
9.9.170.15                     1/5
            Connecting                    3600                           -
               300
Console> (enable)
```

This example shows how to display a summary of information about the web-based proxy authentication session for a specific VLAN:

```
Console> (enable) show web-auth summary vlan 100
------------------------------------------------------------------------------------------
--------------------------------
IP Address                 Interface       Web Auth State
     Session-Timeout   Leftover-Session-Time
------------------------------------------------------------------------------------------
--------------------------------
9.9.150. 1                      1/1              Authenticated
             * 7200                         200
9.9.150.2                       1/2
Authenticating                3600                           -
9.9.150.3                       1/3              Held
                              3600                           -
Console> (enable)
```

Related Commands

clear web-auth
set port web-auth
set port web-auth initialize
set web-auth
set web-auth login-attempts
set web-auth login-fail-page
set web-auth login-page
set web-auth quiet-timeout
set web-auth session-timeout
show port web-auth

slip

To attach or detach Serial Line Internet Protocol (SLIP) for the console port, use the **slip** command.

slip {**attach** | **detach**}

Syntax Description

attach	Activates SLIP for the console port.
detach	Deactivates SLIP for the console port.

Defaults

The default is SLIP is not active (detached).

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can use the **slip** command from a console port session or a Telnet session.

Examples

This example shows how to enable SLIP for a console port during a console port session:

```
Console> (enable) slip attach
Console port now running SLIP.
<console port running SLIP>
```

This example shows how to disable SLIP for a console port during a Telnet session:

```
Console> (enable) slip detach
SLIP detached on Console port.
<console port back to RS-232 Console>
Console> (enable)
```

Related Commands

set interface

squeeze

To delete Flash files permanently, use the **squeeze** command.

squeeze [*m/*]*device***:**

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device***:**	Device where the Flash resides.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

Examples

These examples show how to use the **squeeze** command to delete the slot0 Flash files and then use the **show flash** command to confirm the deletion:

```
Console> squeeze slot0:
All deleted files will be removed, proceed (y/n) [n]?y
Squeeze operation may take a while, proceed (y/n) [n]?y
..........................................................
Console> show flash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
  1 .. 2        f3a3e7c1  607f80   24  6061822 Mar 31 2000 15:42:49 cat6000-sup.
5-5-1.bin
7336000 bytes available (1052608 bytes used)
Console>
```

Related Commands

dir—switch
show flash
undelete

stack

To dump a stack trace of frames, use the **stack** command.

stack [**-d** | **-m**] [*num*]

Syntax Description

-d	(Optional) Dumps the ROM monitor stack.
-m	(Optional) Specifies addresses to dump.
num	(Optional) Number of frames.

Defaults

The default for *num* is five frames.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

The frames are dumped from the kernel stack and the process stack (if one is available) of a booted image. Use the **frame** command to display an individual stack frame.

The minus sign (-) is required with the **-d** and -**m** options.

Examples

This example shows how to use the **stack** command to dump a stack trace of eight frames:

```
rommon 5 > stack 8
Kernel Level Stack Trace:
Initial SP = 0x60276a98, Initial PC = 0x60033054, RA = 0x6006d380
Frame 0 : FP= 0x60276a98, PC= 0x60033054,   0 bytes
Frame 1 : FP= 0x60276a98, PC= 0x6006d380,  24 bytes
Frame 2 : FP= 0x60276ab0, PC= 0x600e5218,  40 bytes
Frame 3 : FP= 0x60276ad8, PC= 0x600dcd48,  32 bytes
Frame 4 : FP= 0x60276af8, PC= 0x60033fdc,   0 bytes

Process Level Stack Trace:
Initial SP = 0x80007ce8, Initial PC = 0x600dfd38, RA = 0x600dfd20
Frame 0 : FP= 0x80007ce8, PC= 0x600dfd38,  24 bytes
Frame 1 : FP= 0x80007d00, PC= 0x6005b260,  32 bytes
Frame 2 : FP= 0x80007d20, PC= 0x6005c05c, 192 bytes
Frame 3 : FP= 0x80007de0, PC= 0x6005b54c,  24 bytes
Frame 4 : FP= 0x80007df8, PC= 0x600e82e0,  56 bytes
Frame 5 : FP= 0x80007e30, PC= 0x600e9484,  40 bytes
Frame 6 : FP= 0x80007e58, PC= 0x600e8b28,  24 bytes
Frame 7 : FP= 0x80007e70, PC= 0x600de224,  72 bytes
```

Related Commands

frame

switch

To switch the clock from the supervisor clock to the internal clock or from the active supervisor engine to the standby supervisor engine, use the **switch** command.

switch {**clock** | **supervisor**}

Syntax Description

clock	Switches the clock from the supervisor clock to the internal clock.
supervisor	Switches from the active supervisor engine to the standby supervisor engine.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to switch the clock:

```
Console> (enable) switch clock
This command will reset system and force a clock switch-over.
Do you want to continue (y/n) [n]?
Console> (enable)
```

This example shows how to switch to the standby supervisor engine:

```
Console> (enable) switch supervisor
This command will force a switch-over to the standby Supervisor module.
Do you want to continue (y/n) [n]?
Console> (enable)
```

8.6 EFT Copy

switch console

To switch the console connection physically to the MSFC on the active supervisor engine, use the **switch console** command.

switch console [*mNo*]

Syntax Description

mNo	(Optional) Module number.

Defaults

The default is supervisor engine console.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported on Telnet sessions.

The **switch console** command allows you to change to the MSFC that shares the slot with the active supervisor engine. To use this command, it is necessary to have active and redundant supervisor engine consoles. Otherwise, you cannot use the **switch console** command to switch to the console of the MSFC placed in the redundant supervisor engine slot.

If you place the MSFC on a supervisor engine installed in slot 1, the MSFC is recognized as module 15. If you install the supervisor engine in slot 2, the MSFC is recognized as module 16. If the optional argument *mNo* is excluded, the console will switch to MSFC on the active supervisor engine.

To exit from the router CLI back to the switch CLI, press **Ctrl-C** three times at the Router> prompt.

Examples

This example shows how to switch the console connection to the MSFC on the active supervisor engine:

```
Console> (enable) switch console 15
Trying Router-15...
Connected to Router-15.
Type ^C^C^C to switch back...
```

switch fabric

To reset the active Switch Fabric Module and allow the standby Switch Fabric Module to take over, use the **switch fabric** command.

switch fabric [*mNo*]

Syntax Description

mNo	(Optional) Switch Fabric Module number.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported on Telnet sessions.

Examples

This example shows how to reset the active Switch Fabric Module:

```
Console> (enable) switch fabric
This command will force a switch-over to the standby fabric module.
Do you want to continue (y/n) [n]?
Console> (enable)
```

sync

To write the working in-core copy of environment variables and the aliases out to NVRAM so they are read on the next reset, use the **sync** command.

sync

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Examples

This example shows how to use the **sync** command:

```
rommon 10 > sync
rommon 11 >
```

sysret

To display the return information from the last booted system image, use the **sysret** command.

sysret

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

The stack dump information displayed has a maximum of eight frames.

Examples

This example shows how to use the **sysret** command to display the return information from the last booted system image:

```
rommon 8 > sysret
System Return Info:
count: 19,  reason: user break
pc:0x60043754,  error address: 0x0
Stack Trace:
FP: 0x80007e78, PC: 0x60043754
FP: 0x80007ed8, PC: 0x6001540c
FP: 0x80007ef8, PC: 0x600087f0
FP: 0x80007f18, PC: 0x80008734
```

8.6 EFT Copy

tclquit

To exit from a tool command language (TCL) shell, use the **tclquit** command.

tclquit

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

TCL shell. This mode is indicated by the prompt Console>(tclsh)(enable).

Usage Guidelines

For more information about TCL, refer to the "Administering the Switch" chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example shows how to exit from a TCL shell and return to privileged mode:

```
Console> (tclsh)(enable) tclquit
Console> (enable)
```

Related Commands

tclsh

tclsh

To start a tool command language (TCL) shell, use the **tclsh** command.

tclsh

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

TCL is a programmable, text-based language that allows you to write command procedures that expand the capabilities of the built-in set of commands. It is used primarily with interactive programs such as text editors, debuggers, illustrators, and shells.

TCL provides a standard syntax so that once you know TCL, you can issue commands to any TCL-based application. Using the utility commands and the general programming interface of TCL, you can implement a few low-level commands and build them into more complex commands.

When you start a TCL shell, the switch prompt changes from Console> (enable) to Console> (tclsh)(enable).

All TCL commands and constructions are available once the TCL shell is active.

For a list of TCL commands and constructions, refer to the "Administering the Switch" chapter of the *Catalyst 6500 Series Switch Software Configuration Guide*.

Examples

This example shows how to start a TCL shell:

```
Console> (enable) tclsh
Console> (tclsh)(enable)
```

Related Commands

tclquit

telnet

To start a Telnet connection to a remote host or to encrypt a Telnet session, use the **telnet** command.

telnet *host* [*port*]

telnet encrypt kerberos *host*

Syntax Description

host	Name or IP address of the remote host to which you want to connect.
port	(Optional) Specific port connection on the remote host.
encrypt kerberos	Encrypts the Telnet session.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

After you authenticate to a switch using Kerberos and you make a Telnet connection to another switch or host, that connection might not be authenticated by Kerberos. Whether or not the Telnet connection is authenticated by Kerberos depends on the authentication method that the Telnet server uses. If the Telnet server uses Kerberos for authentication, you can encrypt all application data packets for the duration of the Telnet session by using the **telnet encrypt kerberos** command.

Examples

This example shows how to open and close a Telnet session with the host elvis:

```
Console> (enable) telnet elvis
Trying 192.122.174.11...
Connected to elvis.
Escape character is '^]'.

UNIX(r) System V Release 4.0 (elvis)

login: fred
Password:
Last login: Thu Oct 15 09:25:01 from forster.cisc.rum
Sun Microsystems Inc.   SunOS 5.4       Generic July 1994
You have new mail.
% logout

Console> (enable)
```

Related Commands

clear kerberos creds
disconnect
show kerberos

test cable-diagnostics

To test the condition of 10-Gigabit Ethernet links and copper cables on 48-port 10/100/1000 BASE-T modules, use the **test cable-diagnostics** command.

test cable-diagnostics prbs {**start** | **stop**} *mod/port*

test cable-diagnostics tdr *mod/port*

Syntax Description

prbs	Specifies the Pseudo Random Binary Sequence (PRBS) test on a 10-Gigabit Ethernet link.
start	Activates the test.
stop	Deactivates the test.
mod/port	Number of the module and the port on the module.
tdr	Specifies the Time Domain Reflectometer (TDR) test. See the "Usage Guidelines" section for a list of modules that support this test.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The PRBS test is currently available only on the 1-port 10GBASE-E serial 10-Gigabit Ethernet module (WS-X6502-10GE).

To run the PRBS test properly between two devices, you must start it on both ends of the cable. If the cable is looped back, a single end can generate the test sequence (on the Tx) as well as verify it and count the errors (on the Rx).

Before the PRBS test starts, the port is automatically put in errdisable state. The errdisable timeout is disabled for the port so that the port is not automatically reenabled after the timeout interval concludes. The errdisable timeout is automatically reenabled on the port after the PRBS test finishes.

When the PRBS test is running, the system will not you permit you to enter the **set port enable** and **set port disable** commands.

The TDR test is supported on these modules: WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548-GE-45AF, WS-X6748-GE-TX, WS-X6148A-GE-TX, WS-X6148-GE-45AF, WS-X6148A-GE-45AF, WS-X6148A-RJ-45, and WS-X6148A-45AF.

8.6 EFT Copy

Note When you run the TDR test, we recommend that you do not make any configurations on the port that you are testing or enter the **show port** command for that port. If you make any port-related configurations or enter the **show port** command, the TDR test results might be inaccurate or the module might fail.

Examples

This example shows how to start the PRBS test on port 1 on module 5:

```
Console> (enable) test cable-diagnostics prbs start 5/1
PRBS cable-diagnostic test started on port 5/1.
Console> (enable)
```

This example shows how to stop the PRBS test on port 1 on module 5:

```
Console> (enable) test cable-diagnostics prbs stop 5/1
PRBS cable-diagnostic test stopped on port 5/1.
Console> (enable)
```

This example shows the message that displays when the PRBS test is not supported:

```
Console> (enable) test cable-diagnostics prbs start 6/1
Feature not supported on module 6.
Console> (enable)
```

This example shows how to start the TDR test on port 1 on module 8:

```
Console> (enable) test cable-diagnostics tdr 8/1
TDR test started on port 8/1. Use show port tdr <m/p> to see the results
Console> (enable)
```

Related Commands

show port prbs
show port tdr

test snmp trap

To send an SNMP trap message to the trap receivers, use the **test snmp trap** command.

test snmp trap {*trap_num* [*specific_num*] | *trap_name*}

Syntax Description

trap_num	Number of the trap.
specific_num	(Optional) Number of a predefined trap.
trap_name	Name of the notification defined in the MIB.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You must enable the SNMP trap before testing.

Examples

This example shows how to run trap 0:

```
Console> (enable) test snmp trap 0
SNMP trap message sent. (4)
Console> (enable)
```

These examples show how to test SNMP traps by specific names:

```
Console> (enable) test snmp trap ciscoRFSwactNotif
ciscoRFSwactNotif notification was sent.
Console> (enable)

Console> (enable) test snmp trap ciscoFlashDeviceInsertedNotif
ciscoFlashDeviceInsertedNotif notification was sent.
Console> (enable)
```

Related Commands

set snmp trap
show snmp

traceroute

To display a hop-by-hop path through an IP network from the Catalyst 6500 series switch to a specific destination host, use the **traceroute** command.

traceroute [**-n**] [**-w** *wait_time*] [**-i** *initial_ttl*] [**-m** *max_ttl*] [**-p** *dest_port*] [**-q** *nqueries*] [**-t** *tos*] *host* [*data_size*]

Syntax Description

-n	(Optional) Option that prevents **traceroute** from performing a DNS lookup for each hop on the path. Only numerical IP addresses are printed.
-w *wait_time*	(Optional) Option used to specify the amount of time (in seconds) that **traceroute** will wait for an ICMP response message. The allowed range for *wait_time* is from 1 to 300 seconds.
-i *initial_ttl*	(Optional) Option that causes **traceroute** to send ICMP datagrams with a TTL value equal to *initial_ttl* instead of the default TTL of 1. This option causes **traceroute** to skip processing for hosts that are less than *initial_ttl* hops away.
-m *max_ttl*	(Optional) Option used to specify the maximum TTL value for outgoing ICMP datagrams. The allowed range for *max_ttl* is from 1 to 255.
-p *dest_port*	(Optional) Option used to specify the base UDP destination port number used in **traceroute** datagrams. This value is incremented each time a datagram is sent. The allowed range for *dest_port* is from 1 to 65535. Use this option in the unlikely event that the destination host is listening to a port in the default traceroute port range.
-q *nqueries*	(Optional) Option used to specify the number of datagrams to send for each TTL value. The allowed range for *nqueries* is from 1 to 1000.
-t *tos*	(Optional) Option used to specify the ToS to be set in the IP header of the outgoing datagrams. The allowed range for *tos* is from 0 to 255.
host	IP alias or IP address in dot notation (*a.b.c.d*) of the destination host.
data_size	(Optional) Number of bytes, in addition to the default of 40 bytes, of the outgoing datagrams. The allowed range is from 0 to 1420.

Defaults

Entering the **traceroute** *host* command without options sends three 40-byte ICMP datagrams with an initial TTL of 1, a maximum TTL of 30, a timeout period of 5 seconds, and a ToS specification of 0 to destination UDP port number 33434. For each host in the processed path, the initial TTL for each host and the destination UDP port number for each packet sent are incremented by one.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

To interrupt **traceroute** after the command has been issued, press **Ctrl-C**.

The **traceroute** command uses the TTL field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a UDP datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an ICMP "time-exceeded" message to the sender. The traceroute facility determines the address of the first hop by examining the source address field of the ICMP time-exceeded message.

To identify the next hop, traceroute again sends a UDP packet but this time with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To determine when a datagram has reached its destination, traceroute sets the UDP destination port in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram with an unrecognized port number, it sends an ICMP "port unreachable" error to the source. This message indicates to the traceroute facility that it has reached the destination.

Catalyst 6500 series switches can participate as the source or destination of the **traceroute** command. However, because they are Layer 2 devices, Catalyst 6500 series switches do not examine the TTL field in the IP header and do not decrement the TTL field or send ICMP time-exceeded messages. Thus, a Catalyst 6500 series switch does not appear as a hop in the **traceroute** command output.

Use the *tos* option to see if different types of service cause routes to change.

Examples

This example shows how to use the **traceroute** command to determine the path from the source to the destination host server10:

```
Console> (enable) traceroute server10
traceroute to server10.company.com (172.16.22.7), 30 hops max, 40 byte packets
 1  engineering-1.company.com (172.31.192.206)  2 ms  1 ms  1 ms
 2  engineering-2.company.com (172.31.196.204)  2 ms  3 ms  2 ms
 3  gateway_a.company.com (172.16.1.201)  6 ms  3 ms  3 ms
 4  server10.company.com (172.16.22.7)  3 ms  *  2 ms
Console> (enable)
```

Table 2-119 describes the fields in the **traceroute** command output.

Table 2-119 traceroute Command Output Fields

Field	Description
30 hops max, 40 byte packets	Maximum TTL value and the size of the ICMP datagrams being sent.
2 ms 1 ms 1 ms	Total time (in milliseconds) for each ICMP datagram to reach the router or host plus the time it took for the ICMP time-exceeded message to return to the host. An exclamation point following any of these values (for example, 20 ms !) indicates that the port-unreachable message returned by the destination had a TTL of 0 or 1. Typically, this occurs when the destination uses the TTL value from the arriving datagram as the TTL in its ICMP reply. The reply does not arrive at the source until the destination receives a traceroute datagram with a TTL equal to the number of hops between the source and destination.
3 ms * 2 ms	"*" indicates that the timeout period (default of 5 seconds) expired before an ICMP time-exceeded message was received for the datagram.

If **traceroute** receives an ICMP error message other than a time-exceeded or port-unreachable message, it prints one of the error codes shown in Table 2-120 instead of the round-trip time or an asterisk (*).

Table 2-120 traceroute Error Messages

ICMP Error Code	Meaning
!N	No route to host. The network is unreachable.
!H	No route to host. The host is unreachable.
!P	Connection refused. The protocol is unreachable.
!F	Fragmentation needed but do not fragment (DF) bit was set.
!S	Source route failed.
!A	Communication administratively prohibited.
?	Unknown error occurred.

Related Commands

ping

traceroute ethernet

To transmit Ethernet CFM traceroute messages to a specific destination MAC address, use the **traceroute ethernet** command.

traceroute ethernet *dest-mac* **domain** *domain-name* **vlan** *vlan*

traceroute ethernet *dest-mac* **level** *level* **vlan** *vlan*

traceroute ethernet *dest-mac* **vlan** *vlan*

Syntax Description

dest-mac	Destination MAC addess for the traceroute messages.
domain *domain-name*	Specifies that all maintenance points in a specific domain transmit the traceroute messages.
vlan *vlan*	Specifies a VLAN for the traceroute; valid values are from 1 to 4094.
level *level*	Specifies that all maintenance points at a specific maintenance level transmit the traceroute; valid values are from 0 to 7.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

This command sends out Ethernet CFM traceroute messages to a device specified by a destination MAC address. You must include a VLAN because the same device may be present in multiple VLANs.

Examples

This example specifies a ping to MAC address 00-d0-00-b3-6b-fb in VLAN 2, for maintenance points in domain sjlabf1 at level 1:

```
Console> traceroute ethernet 00-d0-00-b3-6b-fb vlan 2 domain sjlabf1 level 1
Type escape sequence to abort. TTL 255. Per-Hop Timeout is 10 seconds
--------------------------------------------------------------------------------
Hop  Host                 MAC  Ingress  Ingress   Relay  egress  egress  NextHop
                                  Port   Action  Action    Port  Action
--------------------------------------------------------------------------------
B 1  6509   00-90-6f-96-23-fb      1/2    IngOk RlyCCDB
Console>)
```

unalias

To remove the alias name and associated value from the alias list, use the **unalias** command.

unalias *name*

Syntax Description

name	Name of the alias.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

You must issue a **sync** command to save your change. Otherwise, the change is not saved and the **reset—ROM monitor** command removes your change.

Examples

This example shows how to use the **unalias** command to remove the **s** alias and then check to ensure it was removed:

```
rommon 5 > alias
r=repeat
h=history
?=help
b=boot
ls=dir
i=reset
k=stack
s=set
rommon 6 > unalias s
rommon 7 > alias
r=repeat
h=history
?=help
b=boot
ls=dir
i=reset
k=stack
rmmon 8 > s
monitor: command "s" not found
===========================================================================
```

Related Commands

alias

undelete

To recover a deleted file on a Flash memory device, use the **undelete** command. The deleted file can be recovered using its index (because there could be multiple deleted files with the same name).

undelete *index* [[*m/*]*device***:**]

Syntax Description

index	Index number of the deleted file.
m/	(Optional) Module number of the supervisor engine containing the Flash device.
*device***:**	(Optional) Device where the Flash resides.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device. See the **dir—switch** command to learn the index number of the file to be undeleted. A file cannot be undeleted if a valid file with the same name exists. You must delete the existing file before you can undelete the target file. A file can be deleted and undeleted up to 15 times. To delete all deleted files permanently on a device, use the **squeeze** command.

Examples

This example shows how to recover the deleted file with index 1 and use the **show flash** command to confirm:

```
Console> (enable) undelete 1 bootflash:
Console> (enable)
Console> (enable) show flash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
  1 .. ffffffff fec05d7a  4b3a4c   25  4667849 Mar 03 2000 08:52:09 cat6000-sup.
5-3-4-CSX.bin
  2 .. ffffffff 4e5efc31  c0fadc   30  7716879 May 19 2000 06:50:55 cat6000-sup-
d.6-1-0.bin

3605796 bytes available (12384988 bytes used)
Console> (enable)
```

Related Commands

delete
show flash
squeeze

unset=varname

To remove a variable name from the variable list, use the **unset=***varname* command.

unset=*varname*

Syntax Description

varname	Name of the variable.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

You must enter the **sync** command to save your change to NVRAM. Otherwise, the change is not saved and a **reset** removes your change.

Examples

This example shows how to use the **set** command to display the variable list, remove a variable name from the variable list, and then display the variable list to verify:

```
rommon 2 > set
PS1=rommon ! >
BOOT=
?=0
rommon 3 > unset=0
rommon 4 > set
PS1=rommon ! >
BOOT=
```

Related Commands

varname=

8.6 EFT Copy

varname=

To set the variable *VARNAME* to *varvalue*, use the *varname*= command. Note that the syntax *varname*= sets the variable to a NULL string.

varname=*value*

Syntax Description

varname=	Name of the variable.
value	Any ROM monitor command.

Defaults

This command has no default settings.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

Do not put a space before or after the equal (=) sign. If there are spaces, you must place the *value* in quotes. Spell out variable names in uppercase letters to make them conspicuous.

Examples

This example shows how to assign a variable name to a value:

```
rommon 1 > s=set
rommon 2 > s
PS1=rommon ! >
BOOT=
?=0
```

Related Commands

unset=varname

8.6 EFT Copy

verify

To confirm the checksum of a file on a Flash device, use the **verify** command.

verify [[*m/*]*device*:] *filename*

Syntax Description

m/	(Optional) Module number of the supervisor engine containing the Flash device.
device:	(Optional) Device where the Flash resides.
filename	Name of the configuration file.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

A colon (:) is required after the specified device.

Examples

This example shows how to use the **verify** command:

```
Console> verify cat6k_r47_1.cbi
..........................................................
File cat6k_r47_1.cbi verified OK.
```

wait

To cause the CLI to pause for a specified number of seconds before executing the next command, use the **wait** command. This command might be included in a configuration file.

wait *seconds*

Syntax Description

seconds	Number of seconds for the CLI to wait before executing the next command.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Normal.

Examples

This example shows how to pause the CLI for 5 seconds:

```
Console> wait 5



Console>
```

whichboot

To determine which file booted, use the **whichboot** command.

whichboot

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to use the **whichboot** command:

```
Console> whichboot
Boot image name is 'slot0:cat6000-sup.6-1-1.bin'.
Console>
```

write

To upload the current configuration to the network or display the configuration information currently in running memory, use the **write** command.

write network [**all**]

write terminal [**all**]

write {*host file*} [**all**] [**rcp**]

write memory

Syntax Description

network	Specifies interactive prompting for the IP address or IP alias of the host and the filename to upload.
all	(Optional) Specifies default and nondefault configuration settings.
terminal	Displays the nondefault configuration file on the terminal.
host	IP address or IP alias of the host.
file	Name of the configuration file.
rcp	(Optional) Uploads a software image to a host using rcp.
memory	Keyword that specifies to upload the current configuration to a specified location.

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **write terminal** command is exactly the same as the **show config** command. The **write** *host file* command is a shorthand version of the **write network** command.

You cannot use the **write network** command to upload software to the ATM module.

With the **write network** command, the file must already exist on the host (use the UNIX **touch** *filename* command to create it).

Before you can enter the **write memory** command, you must enter text configuration mode. Enter text configuration mode by entering the **set config mode text** command.

Examples

This example shows how to upload the system5.cfg file to the mercury host:

```
Console> (enable) write network
IP address or name of host? mercury
Name of configuration file to write? system5.cfg
Upload configuration to system5.cfg on mercury (y/n) [y]? y
/
Done.  Finished Network Upload.  (9003 bytes)
Console> (enable)
```

This example shows how to upload the system5.cfg file to the mercury host:

```
Console> (enable) write mercury system5.cfg
Upload configuration to system5.cfg on mercury (y/n) [y]? y
/
Done.  Finished Network Upload.  (9003 bytes)
Console> (enable)
```

This example shows how to display the configuration file on the terminal (partial display):

```
Console> (enable) write terminal
!
....
............


............

............



begin
!
#version 4.2(0.24)VAI58 set password $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set enablepass $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set prompt Console>
set length 24 default
set logout 20
set banner motd ^C^C
!
#system
set system baud  9600
set system modem disable
set system name
set system location
set system contact
!
#power
set power redundancy enable
!
#snmp
set snmp community read-only      public
set snmp community read-write     private
set snmp community read-write-all secret
set snmp rmon disable
set snmp trap disable module

...
<<<< output truncated >>>>
```

This example shows how to upload the running system configuration to a prespecified location:

```
Console> (enable) write memory
Upload configuration to bootflash:switch.cfg
7165844 bytes available on device bootflash, proceed (y/n) [n]? y
Console> (enable)
```

Related Commands

copy
set config mode
show config

8.6 EFT Copy

write tech-support

To generate a report that contains status information about your switch or upload the output of the command to a TFTP server, where you can send it to the Technical Assistance Center, use the **write tech-support** command.

write tech-support *host file* [**module** *mod*] [**vlan** *vlan*] [**mistp-instance** *instance*] [**mst** *instance*] [**memory**] [**config**]

write tech-support *host file* [**port** *mod/port*] [**vlan** *vlan*] [**mistp-instanc**e *instance*] [**mst** *instance*] [**memory**] [**config**]

Syntax Description

host	IP address or IP alias of the host.
file	Name of the configuration file.
module *mod*	(Optional) Specifies the module number.
vlan *vlan*	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
port *mod/port*	(Optional) Keyword and variables to specify the module and port on the module.
mistp-instance *instance*	(Optional) Specifies the MISTP instance number; valid values are from 1 to 16.
mst *instance*	(Optional) Specifies the MST instance number; valid values are from 0 to 15.
memory	(Optional) Specifies memory and processor state information.
config	(Optional) Specifies switch configuration information.

Defaults

By default, this command displays the output for technical-support-related **show** commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration, memory, module, port, instance, and VLAN data.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

⚠ **Caution** Avoid running multiple **write tech-support** commands on a switch or multiple switches on the network segment. Doing so may cause spanning tree instability.

Note If you press **Ctrl-C** while the **write tech-support** is outputting, the output file to the TFTP server might be incomplete.

Note If you are uploading the information to a file, make sure the file already exists in the TFTP server, the file has appropriate permissions, and the network connections are good before you issue the **write tech-support** command.

If you specify the **config** keyword, the **write tech-support** command displays the output of these commands:

- **show config**
- **show flash**
- **show log**
- **show microcode**
- **show module**
- **show port**
- **show spantree active**
- **show spantree summary**
- **show system**
- **show test**
- **show trunk**
- **show version**
- **show vlan**

Note If MISTP is running, the output from the **show spantree mistp-instance active** and **show spantree summary mistp-instance** commands are displayed instead of the output from the **show spantree active** and **show spantree summary** commands.

Note If MST is running, the output from the **show spantree mst** and **show spantree summary mst** commands are displayed instead of the output from the **show spantree active** and **show spantree summary** commands.

If you specify the **memory** keyword, the **write tech-support** command displays the output of these commands:

- **ps**
- **ps -c**
- **show cam static**
- **show cam system**
- **show flash**
- **show memory buffers**
- **show microcode**
- **show module**
- **show proc**

- **show proc mem**
- **show proc cpu**
- **show system**
- **show spantree active**
- **show version**

If you specify a module, port, or VLAN number, the system displays general system information and information for the component you specified.

Examples

This example shows how to upload the technical report:

```
Console> (enable) write tech-support 172.20.32.10 tech.txt
Upload tech-report to tech.txt on 172.20.32.10 (y/n) [n]? y
/
Finished network upload.  (67784 bytes)
Console> (enable)
```

Related Commands

show tech-support
See the commands listed in the "Usage Guidelines" section.

APPENDIX A

Acronyms

Table A-1 defines the acronyms used in this publication.

Table A-1 List of Acronyms

Acronym	Expansion
AAA	authentication, authorization, accounting
AAL	ATM adaptation layer
ACE	access control entry
ACL	access control list
AES	Advanced Encryption Standard
AFI	authority and format identifier
AMP	active monitor present
APaRT	automated packet recognition and translation
ARP	Address Resolution Protocol
AS	autonomous system
ASLB	accelerated server load balancing
ATM	Asynchronous Transfer Mode
BDD	binary decision diagram
BER	baud error rate
BES	bursty errored seconds
BIA	bottom interface adapter
BPDU	bridge protocol data unit
BRF	bridge relay function
BUS	broadcast and unknown server
CAM	content-addressable memory
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
CFM	Connectivity Fault Management
CLI	command-line interface
CMM	Communications Media Module

Table A-1 List of Acronyms (continued)

Acronym	Expansion
COPS	Common Open Policy Service
COPS-DS	COPS Differentiated Services
COPS-PR	COPS for Provisioning
CoS	class of service
CPLD	Complex Programmable Logic Device
CRAM	compression and reordering of ACL masks
CRC	cyclic redundancy check
CRF	concentrator relay function
CSID	Customer Service Instance Identifier
CTA	Cisco Trust Agent
DAI	Dynamic ARP Inspection
DCC	Data Country Code
DDR	Double Data Rate
DEC	Digital Equipment Corporation
DES	Data Encryption Standard
DFI	Domain-Specific Part Format Identifier
DHCP	Dynamic Host Configuration Protocol
DISL	Dynamic Inter-Switch Link
DMP	data movement processor
DNS	Domain Name System
DOM	Digital Optical Monitoring
DRAM	dynamic RAM
DRiP	Dual Ring Protocol
DSAP	destination service access point
DSBM	Designated Subnet Bandwidth Manager
DSCP	differentiated services code point
DSP	digital signal processing or processor
DTP	Dynamic Trunking Protocol
DWDM	dense wavelength division multiplexing
EAP	Extensible Authentication Protocol
EAPoUDP[1]	Extensible Authentication Protocol over User Datagram Protocol
EARL	Enhanced Address Recognition Logic
EEPROM	electrically erasable programmable read-only memory
EOAM	Ethernet Operation, Administration, and Maintenance
EOBC	Ethernet Out-of-Band Channel
EoU[1]	Extensible Authentication Protocol over User Datagram Protocol

Table A-1 List of Acronyms (continued)

Acronym	Expansion
EPLD	Erasable Programmable Logic Device
ESI	end-system identifier
FCS	frame check sequence
FDL	facilities data link
FEFI	far end fault indication
FIB	Forwarding Information Base
FTP	File Transfer Protocol
FWSM	Firewall Services Module
GARP	General Attribute Registration Protocol
GBIC	Gigabit Interface Converter
GDA	Group Destination Address
GMRP	GARP Multicast Registration Protocol
GSR	Gigabit Switch Router
GVRP	GARP VLAN Registration Protocol
HCRMON	High Capacity RMON
HDD	hard disk drive driver
HTTP	HyperText Transfer Protocol
IAB	Inaccessible Authentication Bypass
ICD	International Code Designator
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IDP	initial domain part
IDPROM	Serial EEPROM with FRU information
IDSM	Intrusion Detection System Module
IGMP	Internet Group Management Protocol
ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPC	interprocessor communication
IPX	Internetwork Packet Exchange
ISL	Inter-Switch Link
ISO	International Organization of Standardization
IST	Internal Spanning Tree
KDC	Key Distribution Center
LACP	Link Aggregation Control Protocol
LAN	local-area network
LANE	LAN Emulation

Table A-1 List of Acronyms (continued)

Acronym	Expansion
LCP	Link Control Protocol
LCV	line code violation seconds
LDA	LocalDirector Accelerator
LD	Local Director
LEC	LAN emulation client
LECS	LAN emulation configuration server
LEM	link error monitor
LER	link error rate
LES	LAN emulation server or line errored seconds
LLC	logical link control
LPIP	LAN Port IP
MAC	Media Access Control
MDG	multiple default gateway
MDI	media-dependent interface
MDIX	media-dependent interface in crossover mode
MEP	Maintenance End Point
MIB	Management Information Base
MII	media-independent interface
MIP	Maintenance Intermediate Point
MISTP	Multi-Instance Spanning Tree Protocol
MLS	multilayer switching
MMC	MAC move counter
MMLS	multicast multilayer switching
MOP	Maintenance Operation Protocol
MOTD	message of the day
MPID	Maintenance Point Identifier
MSFC	Multilayer Switch Feature Card
MSM	Multilayer Switch Module
MST	Multiple Spanning Tree
MTP	Media Termination Point
MTU	maximum transmission unit
MVAP	multiple VLAN access port
NAM	Network Analysis Module
NAT	network address translation
NDE	NetFlow Data Export
NMP	Network Management Processor

Table A-1 List of Acronyms (continued)

Acronym	Expansion
NSAP	network service access point
NTP	Network Time Protocol
NVRAM	nonvolatile RAM
OAM	Operation, Administration, and Maintenance
ODM	order dependent merge
OID	object identifier
OSI	Open System Interconnection
OUI	organizational unique identifier
PACL	port access control list
PAE	port access entity
PAgP	Port Aggregation Protocol
PBF	policy-based forwarding
PBR	policy-based routing
PCM	pulse code modulation
PCR	peak cell rate
PDP	policy decision point
PDU	protocol data unit
PEP	policy enforcement point
PFC	Policy Feature Card
PHY	physical sublayer
PIB	policy information base
PID	product identifier
PPP	Point-to-Point Protocol
pps	packets per second
PRBS	Pseudo Random Binary Sequence
PRID	policy rule identifiers
PROM	programmable read-only memory
PVID	port VLAN identifier
PVST	per VLAN spanning tree
QoS	quality of service
RACL	router access control list
RADIUS	Remote Access Dial-In User Service
RAM	random-access memory
rcp	Remote Copy Protocol
RGMP	Router-Ports Group Management Protocol
RIF	Routing Information Field

8.6 EFT Copy

Table A-1 List of Acronyms (continued)

Acronym	Expansion
RMON	Remote Monitoring
ROM	read-only memory
RP	route processor
RPF	reverse path forwarding
RSA	Rivest, Shamir, and Adleman (a public-key cryptographic system)
RSPAN	remote SPAN
RST	reset
RSVP	ReSerVation Protocol
SAID	Security Association Identifier
SAP	service access point
SCP	Secure Copy
SCP	Serial Communication Protocol
SIMM	single in-line memory module
SLCP	Supervisor Line-Card Processor
SLIP	Serial Line Internet Protocol
SMP	standby monitor present
SMT	station management
SN	serial number
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SRB	source-route bridging
SRT	source-route transparent bridging
SSH	Secure Shell
STE	Spanning Tree Explorer
STP	Spanning Tree Protocol
SVC	switched virtual circuit
TAC	Technical Assistance Center (Cisco)
TACACS+	Terminal Access Controller Access Control System Plus
TCAM	Ternary Content Addressable Memory
TCL	tool command language
TCP/IP	Transmission Control Protocol/Internet Protocol
TDR	Time Domain Reflectometer
TFTP	Trivial File Transfer Protocol
TGT	ticket granting ticket
TOS	type of service

Table A-1 List of Acronyms (continued)

Acronym	Expansion
TLV	type-length value
TrBRF	Token Ring Bridge Relay Function
TrCRF	Token Ring Concentrator Relay Function
TTL	time to live
UART	Universal Asynchronous Receiver/Transmitter
UDI	Unique Device Identifier
UDLD	UniDirectional Link Detection
UDLP	UniDirectional Link Protocol
UDP	User Datagram Protocol
UNI	User-Network Interface
UTC	Coordinated Universal Time
VACL	VLAN access control list
VCC	virtual channel connection (in ATM technology), virtual channel circuit
VCI	virtual circuit identifier
VCR	virtual configuration register
VID	version identifier
VID	VLAN ID
VIP	virtual IP address
VLAN	virtual LAN
VMPS	VLAN Membership Policy Server
VoIP	Voice over IP
VTP	VLAN Trunk Protocol
VVID	voice VLAN identifier
WRED	weighted random early detection

1. EAPoUDP and EoU both refer to Extensible Authentication Protocol over User Datagram Protocol.

APPENDIX B

Acknowledgments for Open-Source Software

The Catalyst operating system software pipe command uses Henry Spencer's regular expression library (regex). The most recent version of the library has been modified slightly in the Catalyst operating system software to maintain compatibility with earlier versions of the library.

Henry Spencer's regular expression library (regex). Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

INDEX

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy

8.6 EFT Copy