Catalyst 6000 Family Command Reference

Software Release 5.5

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

Customer Order Number: DOC-7810558=
Text Part Number: 78-10558-02

CONTENTS

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 6000 family switches.

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Command-Line Interfaces	Describes the two types of CLIs found on Catalyst 6000 family switches
Chapter 2	Catalyst 6000 Family Switch and ROM Monitor Commands	Lists alphabetically and provides detailed information for all Catalyst 6000 family switch and ROM-monitor commands
Appendix A	Acronyms	Defines the acronyms used in this publication

Related Documentation

Other documents in the Catalyst 6000 family switch documentation set include:

- *Catalyst 6000 Family Installation Guide*
- *Catalyst 6000 Family Module Installation Guide*
- *Catalyst 6000 Family Software Configuration Guide*
- *System Message Guide—Catalyst 6000 Family, 5000 Family, 4000 Family, Catalyst 2926G Series, Catalyst 2948G, and Catalyst 2980G Switches*
- *Catalyst 6000 Family Quick Software Configuration*

- *Catalyst 6000 Family Multilayer Switch Feature Card and Policy Feature Card Configuration Guide*
- *Release Notes for Catalyst 6000 Family Software Release 6.1*
- *ATM Software Configuration Guide and Command Reference for the Catalyst 5000 Family and 6000 Family Switches*

For information about MIBs, refer to:

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

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands 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.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at http://www.cisco.com/cgi-bin/subcat/kaojump.cgi.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value your comments.

CHAPTER 1

Command-Line Interfaces

This chapter describes the command-line interfaces (CLI) available on the Catalyst 6000 family switches and contains these sections:

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

Switch CLI

The Catalyst 6000 family 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 6000 family 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.

Note The Catalyst 6000 family consists of the Catalyst 6000 and 6500 series switches. The Catalyst 6000 series consists of the Catalyst 6006 and 6009 switches; the Catalyst 6500 series consists of the Catalyst 6506 and 6509 switches. Throughout this publication and all Catalyst 6000 family documents, the phrase *Catalyst 6000 family switches* refers to all four switches, unless otherwise noted.

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:

	Task	Command
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.	*<password>*
Step 3	Enter the necessary commands to complete your desired tasks.	Appropriate commands
Step 4	When finished, exit the session.	**quit**

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

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

	Task	Command
Step 1	From the remote host, enter the **telnet** command and the name or IP address of the switch you want to access.	**telnet** *hostname* | *ip_addr*
Step 2	At the prompt, enter the password for the CLI. If no password has been configured, press **Return**.	*<password>*
Step 3	Enter the necessary commands to complete your desired tasks.	Appropriate commands
Step 4	When finished, exit the Telnet session.	**quit**

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 mistake when entering a command; reenter 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 6000 family 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.

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.

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**.

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
?	**help**
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** or **?** in normal or privileged mode. Context-sensitive help (usage and syntax information) for individual commands can be seen by appending **help** or **?** 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** or **?** to a command category displays a list of commands in that category.

Top-Level Commands and Command Categories

In normal mode, use the **help** or **?** 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 message
history             Show contents of history substitution buffer
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, use 'set help' for more info
show                Show, 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>
Console>
```

In privileged mode, enter the **help** or **?** 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
configure           Configure system from network
copy                Copy files between TFTP/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 message
history             Show contents of history substitution buffer
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
session             Tunnel to ATM or Router module
set                 Set, use 'set help' for more info
show                Show, 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, use 'test help' for more info
traceroute          Trace the route to a host
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** or **?** 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** or **?** 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 6000 family 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 hostnames instead of IP addresses. For information on configuring DNS, refer to the *Software Configuration Guide* for your switch.

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

The command completion feature consists of these functions:

- Command self-repeat
- Keyword lookup or partial keyword lookup
- Command completion

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 example below, 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
```

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, eight parameters are used by the **set mls** command. To see these parameters, enter **set mls ?** at the privileged prompt. In the example below, notice how the system repeats the command entered without the **?**:

```
Console> (enable) set mls ?
  agingtime                 Set agingtime for MLS cache entry
  disable                   Disable MLS in the switch
  enable                    Enable MLS in the switch
  nde                       Configure Netflow Data Export
  flow                      Set minimum flow mask
  include                   Include MLS-RP
  multicast                 Set MLS feature for multicast
  statistics                Add protocols to protocol statistics list
Console> (enable) set mls
```

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?
configure                 Configure system from network
copy                      Copy files between TFTP/RCP/module/flash devices
Console> (enable) co
```

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.

ROM Monitor CLI

The ROM monitor is a ROM-based program that executes upon platform power-up, 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 6000 family software.

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 6000 Family Switch and ROM Monitor Commands

This chapter contains an alphabetical listing of all switch and ROM monitor commands available on the Catalyst 6000 family switches.

For information regarding ATM module-related commands, refer to the *ATM Configuration Guide* for the Catalyst 6000 family switches.

alias

Use the **alias** command to set and display aliases.

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 setting.

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

Use the **boot** command to boot up an external process.

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

Syntax Description

-x	(Optional) Load the image but do not execute.
-v	(Optional) Toggle verbose mode.
*device***:**	(Optional) ID of the device.
imagename	(Optional) Name of the image.

Defaults

This command has no default setting.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

With no arguments, **boot** will boot the first image in bootflash. Specify an image by typing its name. Specify the device by typing the device ID.

If no device is given with an *imagename*, 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 6000 family switch.

Examples

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

```
rommon 2 > boot bootflash:cat6000-sup.5-5-1.bin
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Uncompressing file:
############################################################################################
############################################################################################
#################################################################################
```

cd

Use the **cd** command to set the default Flash device for the system.

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.

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

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 alias

Use the **clear alias** command to clear the shorthand versions of commands.

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

Syntax Description

name	Alternate identifier of the command.
all	Keyword that clears every alternate identifier previously created.

Defaults

This command has no default setting.

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

Use the **clear arp** command to delete a specific entry or all entries from the ARP table.

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

Syntax Description

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

Defaults

This command has no default setting.

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 banner motd

Use the **clear banner motd** command to clear the message-of-the-day banner.

clear banner motd

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

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

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

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 setting.

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

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

clear boot device *mod*

Syntax Description

mod	Number of the module containing the Flash device.

Defaults

This command has no default setting.

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

Use the **clear boot system** command set to clear the contents of the BOOT environment variable and the configuration register setting.

clear boot system all [*mod*]

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

Syntax Description

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

Defaults

This command has no default setting.

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:

```
Console> (enable) clear boot system flash bootflash:cat6000-sup.5-5-1.bin
BOOT variable = bootflash:cat6000-sup.5-2-1.bin,1;bootflash:cat6000-sup.4-5-2.
bin,1;
Console> (enable)
```

Related Commands

set boot system flash
show boot

clear cam

Use the **clear cam** command to delete a specific entry or all entries from the CAM table.

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

Syntax Description

mac_addr	One or more MAC addresses.
dynamic	Keyword to clear the dynamic CAM entries from the CAM table.
static	Keyword to clear the static CAM entries from the CAM table.
permanent	Keyword to clear the permanent CAM entries from the CAM table.
vlan	(Optional) Number of the VLAN; valid values are 1 to 1005.

Defaults

This command has no default setting.

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 channel statistics

Use the **clear channel statistics** command to clear PAgP statistical information.

clear channel statistics

Syntax Description This command has no arguments or keywords.

Defaults This command has no default setting.

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

Use the **clear config** command to clear the system or module configuration information stored in NVRAM.

clear config {*mod* | **rmon** | **all** | **snmp** | **acl** {**nvram**}}

Syntax Description

mod	Number of the module.
rmon	Keyword to clear all RMON configurations, including the historyControlTable, the alarmTable, the eventTable, and the ringStation ControlTable.
all	Keyword to clear all module and system configuration information, including the IP address.
snmp	Keyword to clear all SNMP configurations.
acl nvram	Keywords to clear all ACL configurations.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When using an MSM, **clear config** clears the portion of the MSM configuration kept by the Catalyst 6000 series switch supervisor engine. The portion of the configuration kept by the MSM must be cleared at the router level (router> prompt).

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

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 6000 family 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 6000 family switches:

```
Console> (enable) clear config snmp
This command will clear SNMP 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)
```

Related Commands

configure
show config

clear config pvlan

Use the **clear config pvlan** command to clear all private VLAN configurations in the system including port mappings.

clear config pvlan

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

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

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

clear cops

Use the **clear cops** command to clear COPS configurations.

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

clear cops all-roles

clear cops server all

clear cops server *ipaddress* [**primary**] [**diff-serv** | **rsvp**]

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

clear cops *domain-name*

Syntax Description

roles *role#*	Keyword and variable to specify the roles to clear.
all-roles	Keyword to clear all roles.
server	Keyword to specify the COPS server.
all	Keyword to clear all servers.
ipaddress	Keyword and variable to specify the IP address or IP alias of the server.
primary	(Optional) Keyword to specify the primary server.
diff-serv	(Optional) Keyword to specify the differentiated services server table.
rsvp	(Optional) Keyword to specify the RSVP+ server table.
domain-name	Domain name of the server.

Defaults

This command has no default setting.

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

show cops
set cops

clear counters

Use the **clear counters** command to clear MAC and port counters.

clear counters

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

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)
```

Related Commands

show counters
show port counters

clear gmrp statistics

Use the **clear gmrp statistics** command to clear all the GMRP statistics information from a specified VLAN or all VLANs.

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

Syntax Description

vlan	Number of the VLAN.
all	Keyword to specify all VLANs.

Defaults

This command has no default setting.

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
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

Use the **clear gvrp statistics** command to clear all the GVRP statistics information.

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

Syntax Description

mod/port	Number of the module and port.
all	Keyword to specify all ports.

Defaults

This command has no default setting.

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

show gvrp configuration
set gvrp

clear igmp statistics

Use the **clear igmp statistics** command to clear IGMP snooping statistical information.

clear igmp statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

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

Use the **clear ip alias** command to clear IP aliases set using the **set ip alias** command.

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

Syntax Description

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

Defaults

This command has no default setting.

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

Use the **clear ip dns domain** command to clear the default DNS domain name.

clear ip dns domain

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

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

Use the **clear ip dns server** command to remove a DNS server from the DNS server listing.

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	Keyword to specify all the IP addresses in the DNS server listing to be removed.

Defaults

This command has no default setting.

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

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

clear ip permit {*ip_addr*} [*mask*] [**snmp** | **telnet** | **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.
snmp	(Optional) Keyword to specify removal from the SNMP IP permit list.
telnet	(Optional) Keyword to specify removal from the Telnet IP permit list.
all	(Optional) Keyword to specify all entries in the IP permit list to be removed.

Defaults

This command has no default setting.

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 **snmp**, **telnet**, 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 specified 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
show port counters

clear ip route

Use the **clear ip route** command to delete IP routing table entries.

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 route 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

Use the **clear kerberos clients mandatory** command to disable mandatory Kerberos authentication for services on the network.

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

Use the **clear kerberos credentials forward** command to disable credentials forwarding.

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 TGT and are authenticated to a Kerberized switch, you can use the TGT to authenticate to a host on the network. However, if forwarding is not enabled and you try to list credentials after authenticating to a host, the output will show no Kerberos credentials 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 credentials forward
set kerberos clients mandatory
show kerberos creds

clear kerberos creds

Use the **clear kerberos creds** command to delete all the Kerberos credentials.

clear kerberos creds

Syntax Description This command has no arguments or keywords.

Defaults The command has no default setting.

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

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

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

Syntax Description

dns_domain	DNS domain name.
host	Host name.
kerberos-realm	IP address or name of Kerberos realm.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

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 realm
set kerberos local-realm
show kerberos

clear kerberos server

Use the **clear kerberos server** command to clear a specified KDC entry.

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

Syntax Description

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

Defaults

This command has no default setting.

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

Use the **clear key config-key** command to remove a private DES key.

clear key config-key *string*

Syntax Description

string	Name of the DES key; should be no longer than 8 bytes.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove a private DES key:

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

Related Commands

set key config-key

clear lda

Use the **clear lda** command set to remove the ASLB MLS entries or MAC addresses from the switch.

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	Keyword to remove configured LDs.
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) Keyword and variable to specify 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) Keyword and variable to specify 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) Keyword and variable to specify 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	Keywords to remove all VIP couples (set using the **set lda** command).
vip *vip*	Keyword and variable to specify a VIP.
vip *vip tcp_port*	Keyword and variables to specify a VIP and port couple.
mac all	Keywords to clear all ASLB router MAC addresses.
mac *router_mac_address*	Keyword and variable to clear a specific router MAC address.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

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
show lda
set lda

clear log

Use the **clear log** command set to delete module, system error log, or dump log entries.

clear log [*mod*]

clear log dump

Syntax Description

mod	(Optional) Module number.
dump	Keyword to clear dump log entries.

Defaults

This command has no default setting.

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 logging buffer

Use the **clear logging buffer** command to clear the system logging buffer.

clear logging buffer

Syntax Description This command has no arguments or keywords.

Defaults This command has no default setting.

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 server

Use the **clear logging server** command to delete a syslog server from the system log server table.

clear logging server *ip_addr*

Syntax Description

ip_addr	IP address of the syslog server to be deleted.

Defaults

This command has no default setting.

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 mls

Use the **clear mls** command set to clear the IP or IPX MLS features in the Catalyst 6000 family switches.

clear mls statistics

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

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*] [**source** *ipx_net_addr*]

Syntax Description

statistics	Keyword to clear total packets switched and total packets exported (for NDE).
statistics protocol	Keywords to clear protocols for statistics collection.
protocol	Number of the protocol in the protocol statistics list.
port	Number of the port.
all	Keyword to clear all entries from the statistics protocol list.
entry	Keyword to purge the specified MLS entry or all entries if **all** is specified. All matching MLS entries are purged.
ip	(Optional) Keyword to specify IP MLS.
ipx	(Optional) Keyword to specify IPX MLS.
destination	(Optional) Keyword to specify 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) Keyword to specify the source IP address.
protocol *protocol*	(Optional) Keyword and variable to specify 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) Keyword and variable to specify the source port IP address.
dst-port *dst_port*	(Optional) Keyword and variable to specify the destination port IP address.
ipx_addr_spec	(Optional) Full IPX address or a subnet address in these formats: *src_net/*[*mask*], *dest_net.dest_node*, or *dest_net/mask*.
ipx_net_addr	(Optional) Source IPX net address.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

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)

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 6000 family switches.
- The Catalyst 6000 family 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.

A 0 value for *source_port* and *destination_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 6000 family switch without MLS, this warning message displays:

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

When you remove an MSM from the Catalyst 6000 family 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 disable IP MLS for the Stargate router (IP address 172.20.15.1):

```
Console> (enable) clear mls include Stargate
Multilayer switching is disabled for router 172.20.15.1 (Stargate)
Console> (enable)
```

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 statistics collection:

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

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

set mls agingtime
set mls exclude protocol
set mls nde
set mls statistics protocol
show mls

clear mls exclude protocol

Use the **clear mls exclude protocol** command to remove a protocol port that has been been excluded from shortcutting using the **set mls exclude protocol** command.

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

Syntax Description

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

Defaults

This command has no default setting.

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

show mls exclude protocol
set mls exclude protocol

clear mls multicast statistics

Use the **clear mls multicast statistics** command to remove MLS multicast statistical information from the MSFC.

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 setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter the **clear mls multicast statistics** command on a Catalyst 6000 family 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, then the MFSC is recognized as module 15. If you install the supervisor engine in slot 2, the MFSC is recognized as module 16.

Examples

This example shows how to clear MLS multicast statistics:

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

Related Commands

show mls multicast

clear mls nde flow

Use the **clear mls nde flow** command to reset the NDE filters in the Catalyst 6000 family switches.

clear mls nde flow

Syntax Description This command has no arguments or keywords.

Defaults This command has no default setting.

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 **show mls exclude protocol**
set mls nde

clear module password

Use the **clear module password** command to clear the password set by the **password** [*username*] NAM command.

clear module password *mod*

Syntax Description

mod	Number of the NAM.

Defaults

This command has no default setting.

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

clear multicast router

Use the **clear multicast router** command to clear manually configured multicast router ports from the multicast router port list.

clear multicast router {*mod/port* | **all**}

Syntax Description

mod/port	Number of the module and the port on the module.
all	Keyword to specify 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

Use the **clear ntp server** command to remove one or more servers from the NTP server table.

clear ntp server {*ip_addr* | **all**}

Syntax Description

ip_addr	IP address of the server to remove from the server table.
all	Keyword to specify 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

show ntp
set ntp server

clear port broadcast

Use the **clear port broadcast** command to disable broadcast/multicast suppression on one or more ports.

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

Use the **clear port cops** command set to clear port roles.

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#*	Keyword and variable to specify the roles to clear.
all-roles	Keyword to clear all roles.

Defaults

This command has no default setting.

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 qos cos

Use the **clear port qos cos** command to return the values set by the **set port qos cos** command to the factory-set default values for all specified ports.

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 factory-set default values 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

Use the **clear port security** command to clear all MAC addresses or a specific MAC address from the list of secure MAC addresses on a port.

clear port security *mod*/*port* {*mac_addr* | **all**}

Syntax Description

mod/*port*	Number of the module and the port on the module.
mac_addr	MAC address to be deleted.
all	Keyword to remove all MAC addresses.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to remove a specific MAC address from a port's list of secure addresses:

```
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)
```

Related Commands

set port securityy
show port security

clear pvlan mapping

Use the **clear pvlan mapping** command set to delete a private VLAN mapping.

clear pvlan mapping {*primary_vlan*}{*isolated_vlan* | *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.
mod/port	Number of the module and promiscuous port.

Defaults

This command has no default setting.

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

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

clear qos acl

Use the **clear qos acl** command set to remove various ACL configurations.

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*}

clear qos acl map {*acl_name* | *mod/port* | *vlan* | **all**}

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	Keyword to remove default actions.
ip	Keyword to clear IP ACE default actions.
ipx	Keyword to clear IPX ACE default actions.
mac	Keyword to clear MAC-layer ACE default actions.
all	Keyword to clear all ACE default actions.
map	Keyword to detach an ACL.
mod/port	Number of the module and the port on the module.
vlan	Number of the VLAN.
all	Keyword to detach an ACL from all interfaces.

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.

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)
```

Related Commands

show qos acl editbuffer
commit
rollback

clear qos config

Use the **clear qos config** command to return the values set by the **set qos** command to the factory-set default values and delete the CoS assigned to MAC addresses.

clear qos config

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 factory-set default values 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-dscp-map

Use the **clear qos cos-dscp-map** command to clear CoS-to-DSCP mapping set by the **set qos cos-dscp-map** command and return to the default setting.

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 2-1.

Table 2-1 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

Use the **clear qos dscp-cos-map** command to clear DSCP-to-CoS mapping set by the **set qos dscp-cos-map** command and return to the default setting.

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 2-2.

Table 2-2 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 ipprec-dscp-map

Use the **clear qos ipprec-dscp-map** command to reset the mapping set by the **set qos ipprec-dscp-map** command to the default setting.

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 2-3.

Table 2-3 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

clear qos mac-cos

Use the **clear qos mac-cos** command to clear the values set by the **set 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.
all	Keyword to clear CoS values for all MAC/VLAN pairs.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If the *vlan* number 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 factory-set default values 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 factory-set default values 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

Use the **clear qos map** command to return the values to the factory-set default values.

clear qos map *port_type* **tx** | **rx**

Syntax Description

port_type	Port type; valid values are **2q2t** and **1p2q2t** for transmit and **1p1q4t** for receive.
tx | **rx**	Keyword to specify the transmit or receive queue.

Defaults

The default mappings for all ports are shown in Table 2-4 and Table 2-5 and applies to all ports.

Table 2-4 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 2-5 Default Receive Drop Threshold Mapping of CoS Values

Port Type	Threshold 1 (highest drop possibility)	Threshold 2	Threshold 3	Threshold 4 (lowest drop possibility)	Priority Queue
1q4t	0, 1	2, 3	4, 5	6, 7	N/A
1p1q4t	0, 1	2, 3	4, 5	7	6

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to return the values to the factory-set default values:

```
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

Use the **clear qos policed-dscp-map** to reset the policer-to-dscp mapping table to the defaults.

clear qos policed-dscp-map

Syntax Description

This command has no arguments or keywords.

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.

Examples

This example shows how to reset the mapping to the defaults:

```
Console> (enable) clear qos policed-dscp-map
QoS policed-dscp-map setting restored to default.
Console> (enable)
```

Related Commands

set qos policed-dscp-map
show qos maps

clear qos policer

Use the **clear qos policer** command set to clear policing rules from NVRAM.

clear qos policer microflow *microflow_name* | **all**

clear qos policer aggregate *aggregate_name* | **all**

Syntax Description

microflow *microflow_name*	Keyword and variable to specify the name of the microflow policing rule.
aggregate *aggregate_name*	Keyword and variable to specify the name of the aggregate policing rule.
all	Keyword to clear all policing rules.

Defaults

This command has no default setting.

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.

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 microflow 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

Use the **clear qos statistics** command to clear QoS statistic counters.

clear qos statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the QoS statistic counters:

```
Console> (enable) clear qos statistics
QoS statistical cleared.
Console> (enable)
```

Related Commands

show qos statistics

clear radius

Use the **clear radius** command set to clear one or all of the RADIUS servers from the RADIUS server table.

clear radius server all

clear radius server *ipaddr*

clear radius key

Syntax Description

server	Keyword to specify RADIUS servers.
all	Keyword to specify all RADIUS servers.
ipaddr	Number of the IP address or IP alias.
key	Keyword to specify the RADIUS shared key.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

ipaddr 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 rgmp statistics

Use the **clear rgmp statistics** command to clear RGMP statistics information for all VLANs.

clear rgmp statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

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

show rgmp statistics
set rgmp

clear security acl

Use the **clear security acl** command set to remove a specific ACE or all ACEs from an ACL and delete the ACLs from the edit buffer.

clear security acl all

clear security acl *acl_name*

clear security acl *acl_name* [*editbuffer_index*]

Syntax Description

all	Keyword to remove ACEs for all the ACLs.
acl_name	Name of the VACL whose ACEs are to be removed.
editbuffer_index	(Optional) Index number of the ACE in the ACL.

Defaults

This command has no default setting.

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 ACL list.

Examples

This example shows how to remove ACEs for all the ACLs:

```
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 ACL:

```
Console> (enable) clear security acl IPACL1 2
IPACL1 editbuffer modified. Use ‘commit’ command to apply changes.
Console> (enable)
```

Related Commands

commit
show security acl
rollback

clear security acl capture-ports

Use the **clear security acl capture-ports** command to remove a port from the capture port list.

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 setting.

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 a given number of 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

show security acl capture-ports
set security acl capture-ports

clear security acl map

Use the **clear security acl map** command set to remove VACL-to-VLAN mapping.

clear security acl map *acl_name vlan*

clear security acl map {*acl_name* | *vlan* | **all**}

Syntax Description

acl_name	Name of the VACL whose VLAN is to be deleted.
vlan	Number of the VLAN whose mapping is to be deleted.
all	Keyword to remove all VACL-to-VLAN mappings.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Changes you make by entering this command are saved to NVRAM and do not require you 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
show security acl
rollback

clear snmp access

Use the **clear snmp access** command set to remove the access rights of an SNMP group with a specific security model and security level.

clear snmp access [**-hex**] {*groupname*} {**security-model** {**v1** | **v2c**}}

clear snmp access {**security-model v3** {**noauthentication** | **authentication** | **privacy**}}

Syntax Description

-hex	(Optional) Keyword to display the *groupname* as a hexadecimal format.
groupname	SNMP access table name.
security-model v1 | **v2c**	Keywords to specify the security model v1 or v2c.
security-model v3	Keywords to specify security model v3.
noauthentication	Keyword to specify groups with security model type set to noauthentication.
authentication	Keyword to specify groups with security model type authentication protocol.
privacy	Keyword to specify groups with security model type privacy.

Defaults

This command has no default setting.

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.

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

clear snmp group

Use the **clear snmp group** command to remove the SNMP user from an SNMP group.

clear snmp group [**-hex**] {*groupname*} **user** [**-hex**] {*username*}
{**security-model** {**v1** | **v2c** | **v3**}}

Syntax Description

-hex	(Optional) Keyword to display the *groupname* and *username* as a hexadecimal format.
groupname	Name of the SNMP group that defines an access control.
user	Keyword to specify the SNMP group user name.
username	Name of the SNMP user.
security model v1 | **v2c** | **v3**	Keywords to specify 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 *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 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 notify

Use the **clear snmp notify** command to clear the SNMP notifyname in the snmpNotifyTable.

clear snmp notify [**-hex**] {*notifyname*}

Syntax Description

-hex	(Optional) Keyword to display the *notifyname* as a hexadecimal format.
notifyname	Identifier to index the snmpNotifyTable.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *notifyname* (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

Use the **clear snmp targetaddr** command to clear the SNMP target address entry in the TargetAddressTable.

clear snmp targetaddr [**-hex**] {*addrname*}

Syntax Description

-hex	(Optional) Keyword to display the *addrname* as a hexadecimal format.
addrname	Name of the target agent; the maximum length is 32 bytes.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *addrname* (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

Use the **clear snmp targetparams** command to clear the SNMP target parameters used in the snmpTargetParamsTable.

clear snmp targetparams [**-hex**] {*paramsname*}

Syntax Description

-hex	(Optional) Keyword to display the *paramsname* as a hexadecimal format.
paramsname	Name of the target parameter in the snmpTargetParamsTable; maximum length is 32 bytes.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you use special characters for *paramsname* (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

Use the **clear snmp trap** command to clear an entry from the SNMP trap receiver table.

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) Keyword to specify 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

Use the **clear snmp user** command to remove an SNMP user.

clear snmp user [**-hex**] {*username*} [**remote** {*engineid*}]

Syntax Description

-hex	(Optional) Keyword to display the *username* as a hexadecimal format.
username	Name of the user on the host that connects to the agent.
remote *engineid*	(Optional) Keyword and variable to specify the *username* 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 *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.

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

clear snmp view

Use the **clear snmp view** command to remove the MIB view entry from the vacmViewTreeFamilyTable.

clear snmp view [**-hex**] {*viewname*} {*subtree*}

Syntax Description

-hex	(Optional) Keyword to display the *viewname* as a hexadecimal format.
viewname	Name of a MIB view.
subtree	Name of the subtree.

Defaults

This command has no default setting.

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 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 portvlancost

Use the **clear spantree portvlancost** command to restore the default path cost to a VLAN on a port.

clear spantree portvlancost *mod/port* [*vlan_list*]

Syntax Description

mod/port	Number of the module and the port on the module.
vlan_list	(Optional) List of VLANs to clear. If not specified, all VLANs are cleared.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

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 portfast
show spantree statistics

clear spantree portvlanpri

Use the **clear spantree portvlanpri** command to reset the spanning tree port VLAN priority.

clear spantree portvlanpri *mod/port* [*vlans*]

Syntax Description

mod/port	Number of the module and the port on the module.
vlans	(Optional) One or more VLANs.

Defaults

This command has no default setting.

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

Use the **clear spantree root** command to restore the switch priority and Spanning Tree Protocol parameters to the factory-set default values.

clear spantree root [*vlan_list*]

Syntax Description

vlan_list	(Optional) List of the VLAN numbers to clear.

Defaults

The default configuration has the switch priority set to 32768.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to clear the spantree 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 spantree 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)
```

Related Commands

set spantree root
show spantree

clear spantree statistics

Use the **clear spantree statistics** command to clear the spanning tree statistics.

clear spantree statistics [*vlan_list*]

Syntax Description

vlan_list	(Optional) List of the VLAN numbers to clear.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

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)
```

Related Commands

show spantree statistics

clear spantree uplinkfast

Use the **clear spantree uplinkfast** command to turn off the UplinkFast feature and to return the switch priority and port costs to the factory-set default values.

clear spantree uplinkfast

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command could cause load balancing on the switch to be lost in some cases.

Examples

This example shows how to turn off the UplinkFast feature and to return the switch priority to the factory-set default values:

```
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 tacacs key

Use the **clear tacacs key** command to remove the key setting used for TACACS+ authentication and encryption.

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

Use the **clear tacacs server** command to remove a host from the list of TACACS+ servers.

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 setting.

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

Use the **clear timezone** command to return the time zone to its default, UTC.

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

Use the **clear top** command to stop the TopN process.

clear top {**all** | *report_num*}

Syntax Description

all	Keyword to stop all nonpending TopN results.
report_num	TopN report number to kill; valid values are from 1 to 5.

Defaults

This command has no default setting.

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/console session, or by entering the **clear top** [*report_num*] command from a separate Telnet/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

Use the **clear trunk** command 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.

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 1000 and 1025 to 4094.

Defaults

For all ports except 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.

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 how to clear the trunk on port 2 of module 1:

```
Console> (enable) clear trunk 1/2
Port(s) 1/2 trunk mode set to auto.
Port(s) 1/2 trunk type set to isl.
Console> (enable)
```

Related Commands

set trunk
show trunk

clear vlan

Use the **clear vlan** command to delete an existing VLAN from a management domain.

clear vlan *vlan_num*

Syntax Description

vlan_num	Number of the VLAN; vaild values are from 2 to 1000.

Defaults

This command has no default setting.

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.
- To delete a Token Ring TrBRF VLAN, you must first reassign its child TrCRFs to another parent TrBRF, or delete the child TrCRFs.

Caution 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 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.

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.

Examples

This example shows how to clear existing VLAN 4 from a management domain:

```
Console> (enable) clear vlan 4
This command will de-activate all ports on vlan 4
in the entire management domain
Do you want to continue(y/n) [n]? y
VTP: VLAN 4 deletion successful
Console> (enable)
```

Related Commands **set vlan**
show vlan

clear vlan mapping

Use the **clear vlan mapping** command to delete existing 802.1Q VLAN to ISL VLAN-mapped pairs.

clear vlan mapping dot1q *1q_vlan_num* | **all**

Syntax Description

dot1q	Keyword to specify the VLAN type as 802.1Q.
1q_vlan_num	Number identifying the 802.1Q VLAN.
all	Keyword to clear the mapping table of all entries.

Defaults

This command has no default setting.

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 still configured on that VLAN are also reactivated.

Examples

This example shows how to clear an existing mapped VLAN (VLAN 4) from the 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)
```

Related Commands

set vlan
show vlan

clear voicevlan

Use the **clear voicevlan** command to put all ports back to the 802.1p default values.

clear voicevlan {*mod/port* | *vlan*}

Syntax Description

mod/port	Number of the module and the port on the module.
vlan	Number of the auxiliary VLAN; valid values are from 1 to 4094.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you specify the *mod* or *port*, only those specific modules or ports are changed to the 802.1p default value. The internal value is 0.

Examples

This example shows how to return all ports to the 802.1p default values for a specific auxiliary VLAN:

```
Console> (enable) clear voicevlan 2993
Voicevlan 2993 cleared. All ports belong to it configured for 802.1p.
Console> (enable)
```

This example shows how to return all ports to the 802.1p default values for a specific module and port:

```
Console> (enable) clear voicevlan 3/4
Port 3/4 cleared from voicevlan 2993 and configured for 802.1p
Console> (enable)
```

This example shows how to return all ports to the 802.1p default values for a specific module and range of ports:

```
Console> (enable) clear voicevlan 3/6-9
Ports 3/6-9 cleared from voice vlan 2993 and configured for 802.1p.
Console> (enable)
```

clear vtp pruning

Use the **clear vtp pruning** command to specify which VLANs in the VTP domain are ineligible for pruning.

clear vtp pruning *vlan_num*

Syntax Description

vlan_num	Number of VLANs to make pruning ineligible.

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 pruning** command to make VLANs pruning ineligible.

If VLANs are pruning ineligible, use the **set vtp pruneeligible** command to make the VLANs pruning eligible again.

Examples

This example shows how to make VLANs 200 through 500 pruning ineligible:

```
Console> (enable) clear vtp pruning 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

Use the **clear vtp statistics** command to delete VTP statistics.

clear vtp statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

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

commit

Use the **commit** command to commit all or a specific ACE in NVRAM that have not been written to hardware.

commit qos acl *acl_name* | **all**

commit security acl *acl_name* | **all**

Syntax Description

qos acl	Keywords to specify QoS ACEs.
acl_name	Name that identifies the VACL whose ACEs are to be committed.
all	Keyword to commit ACEs for all the ACLs.
security acl	Keywords to specify security ACEs.

Defaults

This command has no default setting.

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 are deleted. We recommend that you enter ACEs in batches and issue 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)
```

Related Commands

rollback

commit lda

Use the **commit lda** command to commit ASLB configuration that has not been written to hardware to NVRAM.

commit lda

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

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

set lda
show lda
clear lda

configure

Use the **configure** command to download a configuration file from an rcp server or the network and execute each command in that file.

configure {*host file*}[**rcp**]

configure network

Syntax Description

host	IP address or IP alias of the host.
file	Name of the file.
rcp	(Optional) Keyword to specify rcp as the file transfer method.
network	Keyword to specify interactive prompting for the host and the file.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Refer to the *Catalyst 6000 Family 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

show config
copy

confreg

Use the **confreg** command to configure the configuration register utility.

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 setting.

Command Types

ROM monitor command.

Command Modes

Normal.

Usage Guidelines

Executed with the argument *num*, **confreg** changes the VCR 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

Use the **context** command to display the context of a loaded image.

context

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

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
```

copy

Use the **copy** command set to upload or download a Flash image or a switch configuration to or from a Flash device, rcp server, or TFTP server.

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**]

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	Keyword to allow you to copy to or from a TFTP server.
rcp	Keyword to specify the file be copied to or from an rcp server.
flash	Keyword to support downloading of multiple modules.
config	Keyword to allow you to copy the configuration to Flash memory, another Flash device, or a file on a TFTP server.
acl config	Keywords to copy the ACL configuration manually to a file. See the "Usage Guidelines" section before using this command.
cfg1	Keyword to specify the first startup configuration file on the supervisor engine.
cfg2	Keyword to specify the second startup configuration file on the supervisor engine.
all	(Optional) Keyword to specify that the entire configuration be copied to the specified destination configuration file.

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.

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.

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).

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)
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
...........
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 6000 family 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.5-5-1.bin
Flash device [bootflash]?
Name of file to copy to [cat6000-sup-d.5-5-1.bin]?

4369664 bytes available on device bootflash, proceed (y/n) [n]? y
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
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 config-acl 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)
```

Related Commands

write
configure
set boot config-register
set boot config-register auto-config

delete

Use the **delete** command to delete a configuration file.

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 setting.

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.5-5-1.bin
  2 .. ffffffff 762950d6  6234d0   25  3093399 Jan 13 2000 12:33:14
cat6000-sup-d.5-5-1.bin

1428272 bytes available (6173904 bytes used)
Console> (enable)
```

Related Commands

show flash
dir—switch
undelete
squeeze

dev

Use the **dev** command to list the device IDs available on a switch.

dev

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

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
```

dir—ROM monitor

Use the **dir** command to list the files of the named device.

dir *device*

Syntax Description

device	ID of the device.

Defaults

This command has no default setting.

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

Use the **dir** command to display a list of files on a Flash memory device.

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) Keyword to display all files, deleted or not.
deleted	(Optional) Keyword to display only deleted files.
long	(Optional) Keyword to display files that have not been deleted, in long format.

Defaults

This command has no default setting.

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 2-6.

Table 2-6 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 2-7.

Table 2-7 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.5-5-1.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.
5-5-1.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

Use the **disable** command to return to normal mode from privileged mode.

disable

Syntax Description This command has no arguments or keywords.

Defaults This command has no default setting.

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

Use the **disconnect** command to close an active console port or Telnet session.

disconnect {*ip_addr* | **console**}

Syntax Description

ip_addr	IP address or IP alias.
console	Keyword to denote an active console port.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If multiple sessions from the same IP address exist, the **disconnect** command checks if the current process is also from the same IP address. If it is not, all Telnet sessions from the specified IP address are disconnected. If it is, all sessions, other than the current session, are disconnected. The system prompts whether to disconnect the current Telnet session. You can answer **n** and remain connected or answer **y** and be disconnected.

Examples

This example shows how to close a Telnet session to host 198.134.214.4:

```
Console> (enable) disconnect 198.134.214.4
Telnet session from 198.134.214.4 disconnected. (1)
Console> (enable)
```

This example shows how to close the current console session:

```
Console> (enable) disconnect console
Console session disconnected.
Console> (enable)
```

Related Commands

telnet

download

Use the **download** command to copy a software image from a specified host to the Flash memory of a designated module.

download *host file* [*mod*] [**rcp**]

download serial

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) Keyword to specify rcp protocol as the file transfer method.
serial	Keyword to specify download through a serial port.

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

The Catalyst 6000 family 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 6000 family 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.

If you specify the module number, the download goes to the specified module, but the download will fail if the module is of a different type than 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 leave the switch in a problematic state. If this occurs, reboot the switch.

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)
```

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%
```

Related Commands

reset—switch
show flash
upload

enable

Use the **enable** command to activate privileged mode. 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 setting.

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

Use the **format** command to mat bootflash or a Flash PC card (a Flash device must be formatted before it can be used).

format [**spare** *spare-num*] [*m/*]*device1***:** [[*device2***:**][*monlib-filename*]]

Syntax Description

spare *spare_num*	(Optional) 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 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

Note When the system cannot find a monlib file, the system terminates the formatting process.

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

Use the **frame** command to display an individual stack frame.

frame [**-d** | **-p**] [*num*]

Syntax Description

-d	(Optional) Keyword to specify a monitor context.
-p	(Optional) Keyword to specify 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—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
```

history—ROM monitor

Use the **history** command to display the command history (the last 16 commands executed in the ROM monitor environment). 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 setting.

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

Use the **history** command to show the contents of the command history buffer.

history

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

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.

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>
```

meminfo

Use the **meminfo** command to display information about the main memory, packet memory, and NVRAM. With the **-l** option, the supported DRAM configurations are displayed.

meminfo [**-l**]

Syntax Description

-l	(Optional) Keyword to specify long listing—displays DRAM configurations.

Defaults

This command has no default setting.

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

Use the **ping** command to send ICMP echo-request packets to another node on the network.

ping [**-s**] *host* [*packet_size*] [*packet_count*]

Syntax Description

-s	(Optional) Keyword to cause **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.

Defaults

The default *packet_size* is 56 bytes.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

Press **Ctrl-C** to stop pinging.

Following are sample results of the **ping** command:

- Normal response—The normal response occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond—If the host does not respond, a “no answer from host” appears in 10 seconds.
- Destination unreachable—The gateway for this destination indicates that the destination is unreachable.
- Network or host unreachable—The switch found no corresponding entry in the route table.

The actual packet size will be 8 bytes larger than the size you specify because the switch adds header information.

The **ping** command returns output only when a response is received.

Examples

This example shows how to ping a host with IP alias elvis a single time:

```
Console> ping elvis
elvis is alive
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>
```

Related Commands

set interface
set ip route
show interface
show ip route

pwd

Use the **pwd** command to show the current setting of the **cd** 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

Use the **quit** command to exit a CLI session.

quit

Syntax Description This command has no arguments or keywords.

Defaults This command has no default setting.

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%
```

reload

Use the **reload** command to force a module to accept a download via SCP. 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 setting.

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.

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

Use the **repeat** command to repeat a 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

Use the **reset** ROM monitor command to perform a soft reset of the switch.

reset [-**s**]

Syntax Description

-s	(Optional) Keyword to reset 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 6000 family 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

Use the **reset** command set to restart the system or an individual module, schedule a system reset, or cancel a scheduled reset.

reset [*mod* | **system** | **mindown**]

reset [**mindown**] **at** {*hh:mm*} [*mm/dd*] [*reason*]

reset [**mindown**] **in** [*hh*:] {*mm*} [*reason*]

reset [**cancel**]

reset {*nam_mod*} [*bootdevice*[,*bootdevice*]]

Syntax Description

mod	(Optional) Number of the module to be restarted.
system	(Optional) Keyword to reset the system.
mindown	(Optional) Keyword to perform a reset as part of a minimal downtime software upgrade in a system with a redundant supervisor engine.
at	Keyword to schedule 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	Keyword to schedule 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) Keyword to cancel the scheduled reset.
nam_mod	Number of the NAM.
bootdevice	(Optional) Boot device identification; for format guidelines, see the "Usage Guidelines" section.

Defaults

This command has no default setting.

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 standby 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 redundant supervisor engine. For complete information on performing a minimal downtime software upgrade, refer to the *Catalyst 6000 Family Software Configuration Guide*.

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 standby supervisor engine is reset, but any changes 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 standby supervisor engine.

If you reset an intelligent module (such as the Catalyst 6000 family 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

Examples

This example shows how to reset the supervisor engine on a Catalyst 6000 family 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 schedule reset:

```
Console> (enable) reset cancel
Reset cancelled.
Console> (enable)
```

Related Commands **show reset**
commit

rollback

Use the **rollback** command set to clear changes made to the ACL edit buffer since its last save. The ACL is rolled back to its state at the last **commit** command.

rollback qos acl *acl_name*

rollback security acl *acl_name*

Syntax Description

qos acl	Keyword to specify QoS ACEs.
security acl	Keywords to specify security ACEs.
acl_name	Name that identifies the VACL whose ACEs are to be affected.

Defaults

This command has no default setting.

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

show qos acl info
commit

session

Use the **session** command to open a session with a module (for example, the MSM or ATM), allowing you to use the module-specific CLI.

session *mod*

Syntax Description

mod	Number of the module.

Defaults

This command has no default setting.

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 6000 Family Switches*.

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

switch console
quit

set

Use the **set** command to display all of the ROM monitor variable names with their values.

set

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

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

Use the **set accounting commands** command set to enable command event accounting on the switch.

set accounting commands enable {**config** | **all**} [**stop-only**] {**tacacs+**}

set accounting commands disable

Syntax Description

enable	Keyword to enable the specified accounting method for commands.
config	Keyword to permit accounting for configuration commands only.
all	Keyword to permit accounting for all commands.
stop-only	(Optional) Keyword to apply the accounting method at the command end.
tacacs+	Keyword to specify TACACS+ accounting for commands.
disable	Keyword to disable 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

Use the **set accounting connect** command set to enable accounting of outbound connection events on the switch.

set accounting connect enable {**start-stop** | **stop-only**} {**tacacs+** | **radius**}

set accounting connect disable

Syntax Description

enable	Keyword to enable the specified accounting method for connection events.
start-stop	Keyword to specify the accounting method applies at the start and stop of the connection event.
stop-only	Keyword to specify the accounting method applies at the end of the connection event.
tacacs+	Keyword to specify TACACS+ accounting for connection events.
radius	Keyword to specify RADIUS accounting for connection events.
disable	Keyword to disable 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

Use the **set accounting exec** command set to enable accounting of normal login sessions on the switch.

set accounting exec enable {**start-stop** | **stop-only**} {**tacacs+** | **radius**}

set accounting exec disable

Syntax Description

enable	Keyword to enable the specified accounting method for normal login sessions.
start-stop	Keyword to specify the accounting method applies at the start and stop of the normal login sessions.
stop-only	Keyword to specify the accounting method applies at the end of the normal login sessions.
tacacs+	Keyword to specify TACACS+ accounting for normal login sessions.
radius	Keyword to specify RADIUS accounting for normal login sessions.
disable	Keyword to disable 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

set accounting suppress

Use the **set accounting suppress** command to enable or disable suppression of accounting information for a user who has logged in without a username.

set accounting suppress null-username {**enable** | **disable**}

Syntax Description

null-username	Keyword to specify users must have a user ID.
enable	Keyword to enable suppression for a specified user.
disable	Keyword to disable 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 usernames' 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

Use the **set accounting system** command set to enable accounting of system events on the switch.

set accounting system enable {**start-stop** | **stop-only**} {**tacacs+** | **radius**}

set accounting system disable

Syntax Description

enable	Keyword to enable the specified accounting method for system events.
start-stop	Keyword to specify the accounting method applies at the start and stop of the system event.
stop-only	Keyword to specify the accounting method applies at the end of the system event.
tacacs+	Keyword to specify TACACS+ accounting for system events.
radius	Keyword to specify RADIUS accounting for system events.
disable	Keyword to disable 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

Use the **set accounting update** command to configure the frequency of accounting updates.

set accounting update {**new-info** | {**periodic** [*interval*]}}

Syntax Description

new-info	Keyword to specify update when new information in available.
periodic	Keyword to 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 alias

Use the **set alias** command to define aliases (shorthand versions) of commands.

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.

For additional information about *parameter*, 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

Use the **set arp** command set to add IP address-to-MAC address mapping entries to the ARP table and to set the ARP aging time for the table.

set arp [**dynamic** | **permanent** | **static**] {*ip_addr hw_addr*}

set arp agingtime *agingtime*

Syntax Description

dynamic	(Optional) Keyword to specify that entries are subject to ARP aging updates.
permanent	(Optional) Keyword to specify that permanent entries are stored in NVRAM until they are removed by the **clear arp** or **clear config** command.
static	(Optional) Keyword to specify 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	Keyword to set 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*, 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

Use the **set authentication enable** command set to enable authentication using the TACACS+, RADIUS, or Kerberos server to determine if you have privileged access permission.

set authentication enable tacacs {**enable** | **disable**} [**all | console** | **http**] [**telnet**] [**primary**]

set authentication enable radius {**enable** |**disable**} [**all** | **console** | **http**] [**telnet**] [**primary**]

set authentication enable local {**enable** | **disable**} [**all** | **console** | **http**] [**telnet**] [**primary**]

set authentication enable kerberos {**enable** | **disable**} [**all** | **console** | **http**] [**telnet**] [**primary**]

Syntax Description

tacacs	Keyword to specify TACACS+ authentication for login.
enable	Keyword to enable the specified authentication method for login.
disable	Keyword to disable the specified authentication method for login.
all	(Optional) Keyword to apply the authentication method to all session types.
console	(Optional) Keyword to specify the authentication method for console sessions.
http	(Optional) Keyword to specify the specified authentication method HTTP sessions.
telnet	(Optional) Keyword to specify the authentication method for Telnet sessions.
primary	(Optional) Keyword to specify the specified authentication method be tried first.
radius	Keyword to specify RADIUS authentication for login.
local	Keyword to specify local authentication for login.
kerberos	Keyword to specify Kerberos authentication for login.

Defaults

The default is local authentication is enabled for console and Telnet sessions. RADIUS, TACACS+, and Kerberos are disabled for all session types.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Use authentication configuration for both console and Telnet connection attempts unless you use the **console** and **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 sessio
n as primary authentication method.
Console> (enable)
```

Related Commands

set authentication login
show authentication

set authentication login

Use the **set authentication login** command set to enable TACACS+, RADIUS, or Kerberos as the authentication method for login.

set authentication login local {**enable** | **disable**} [**all** | **console** | **http** | **telnet**]

set authentication login tacacs {**enable** | **disable**} [**all** | **console** | **http** | **telnet**] [**primary**]

set authentication login radius {**enable** | **disable**} [**all** | **console** | **http** | **telnet**] [**primary**]

set authentication login kerberos {**enable** | **disable**} [**all** | **console** | **http** | **telnet**] [**primary**]

Syntax Description

local	Keyword to specify local password to determine if you have access permission to the switch.
enable	Keyword to enable the specified authentication method for login.
disable	Keyword to disable the specified authentication method for login.
all	(Optional) Keyword to specify the authentication method for all session types.
console	(Optional) Keyword to specify the authentication method for console sessions.
http	(Optional) Keyword to specify the authentication method for HTTP sessions or to set HTTP sessions as the primary authentication method.
telnet	(Optional) Keyword to specify the authentication method for Telnet sessions.
tacacs	Keyword to specify the use of the TACACS+ server password to determine if you have access permission to the switch.
radius	Keyword to specify the use of the RADIUS server password to determine if you have access permission to the switch.
kerberos	Keyword to specify the Kerberos server password to determine if you have access permission to the switch.

Defaults

The default is 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 authentification method for the web interface. If you configure the authentification 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 that 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)
```

Related Commands

set authentication enable
show authentication

set authorization commands

Use the **set authorizaton commands** command set to enable authorization of command events on the switch.

set authorization commands enable {**config** | **all**} {*option*} {*fallbackoption*} [**console** | **telnet** | **both**]

set authorization commands disable [**console** | **telnet** | **both**]

Syntax Description

enable	Keyword to enable the specified authorization method for commands.
config	Keyword to permit authorization for configuration commands only.
all	Keyword to permit 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.
console	(Optional) Keyword to specify the authorization method for console sessions.
telnet	(Optional) Keyword to specify the authorization method for Telnet sessions.
both	(Optional) Keyword to specify the authorization method for both console and Telnet sessions.
disable	Keyword to disable authorization of command events.

Defaults

The default is authorization is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you define the *option* and *fallbackoption* values:

- **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

Use the **set authorization enable** command set to enable authorization of privileged mode sessions on the switch.

set authorization enable enable {*option*} {*fallbackoption*} [**console** | **telnet** | **both**]

set authorization enable disable [**console** | **telnet** | **both**]

Syntax Description

enable	Keyword to enable 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.
console	(Optional) Keyword to specify the authorization method for console sessions.
telnet	(Optional) Keyword to specify the authorization method for Telnet sessions.
both	(Optional) Keyword to specify the authorization method for both console and Telnet sessions.
disable	Keyword to disable the authorization method.

Defaults

The default is authorization is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you define the *option* and *fallbackoption* values:

- **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

Use the **set authorization exec** command set to enable authorization of exec, normal login mode, session events on the switch.

set authorization exec enable {*option*} {*fallbackoption*} [**console** | **telnet** | **both**]

set authorization exec disable [**console** | **telnet** | **both**]

Syntax Description

enable	Keyword to enable 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.
console	(Optional) Keyword to specify the authorization method for console sessions.
telnet	(Optional) Keyword to specify the authorization method for Telnet sessions.
both	(Optional) Keyword to specify the authorization method for both console and Telnet sessions.
disable	Keyword to disable authorization method.

Defaults

The default is authorization is denied.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you define the *option* and *fallbackoption* values:

- **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 login mode, sessions:

```
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 banner motd

Use the **set banner motd** command to program an MOTD banner to appear before session login.

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 setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The banner may contain no 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 boot auto-config

Use the **set boot auto-config** command to specify one or more configuration files to use to configure the switch at bootup. 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

Use the **set boot config-register** command set to configure the boot configuration register value.

set boot config-register 0x*value* [*mod*]

set boot config-register baud {**1200** | **2400** | **4800** | **9600**} [*mod*]

set boot config-register ignore-config {**enable** | **disable**} [*mod*]

set boot config-register boot {**rommon** | **bootflash** | **system**} [*mod*]

Syntax Description

0x*value*	Keyword to set the 16-bit configuration register value.
mod	(Optional) Module number of the supervisor engine containing the Flash device.
baud 1200 | **2400** | **4800** | **9600**	Keywords to specify the console baud rate.
ignore-config	Keywords to set the ignore-config feature.
enable	Keyword to enable the specified feature.
disable	Keyword to disable the specified feature.
boot	Keyword to specify the boot image to use on the next restart.
rommon	Keyword to specify booting from the ROM monitor.
bootflash	Keyword to specify booting from the bootflash.
system	Keyword to specify 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 to 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).

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

set config acl
set boot auto-config
set boot system flash
show boot
copy
show config

set boot config-register auto-config

Use the **set boot config-register auto-config** command set to configure auto-config file dispensation.

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	Keyword to set 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	Keyword to set 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	Keyword to cause the auto-config file to overwrite the NVRAM configuration.
append	Keyword to cause the auto-config file to append to the file currently in the NVRAM configuration.
sync enable | **disable**	Keywords to enable or disable 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 file(s) on the supervisor engine, the files will also be deleted on the standby supervisor engine.

If you enable synchronization, the CONFIG_FILE variable from the active file is made identical on the standby supervisor engine. Each auto-config file on the active supervisor engine is compared against each corresponding auto-config file on the standby supervisor engine. Two files are considered identical if the 'CRC' is the same. If a file on the standby and active supervisor engine is not identical, a new file is generated on the standby supervisor engine. If a file already exists on the standby supervisor engine, it is overwritten with the file from the active supervisor engine.

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** commands 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

Use the **set boot device** command to set the NAM boot environment.

set boot device *bootseq*[**,***bootseq*] *mod*

Syntax Description

bootseq	Device where the startup configuration file resides; see the "Usage Guidelines" section for format guidelines. The second *bootseq* is optional.
mod	Number of the module containing the Flash device.

Defaults

This command has no default setting.

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 you enter the *bootseq*, use the following guidelines:

- *bootseq* = *bootdevice*[**:***bootdevice-qualifier*]
- *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 for **pcmcia**, valid values are slot0 or slot1.
- The colon between *bootdevice* and *bootdevice-qualifier* is required.
- You can enter multiple *bootseq* 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 simply stores the boot device list in NVRAM.

This command is supported by the NAM module 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 system flash

Use the **set boot system flash** command to set the BOOT environment variable that specifies a list of images the switch loads at startup.

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) Keyword to place 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 setting.

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 fail-safe 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

Use the **set cam** command set to add entries into the CAM table and set the aging time for the CAM table.

set cam {**dynamic** | **static** | **permanent**} {*unicast_mac* | *route_descr*} *mod/port* [*vlan*]

set cam {**static** | **permanent**} {*multicast_mac*} *mod/ports..* [*vlan*]

set cam agingtime *vlan agingtime*

Syntax Description

dynamic	Keyword to specify that entries are subject to aging.
static	Keyword to specify that entries are not subject to aging.
permanent	Keyword to specify that 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.
multicast_mac	MAC address of the destination host used for a multicast.
mod/ports..	Number of the module and the ports on the module.
agingtime	Keyword to set the period of time after which an entry is removed from the table.
agingtime	Number of seconds (0 to 1,000,000) that dynamic entries remain in the table before being deleted. Setting the aging time to 0 disables aging.

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 NMP). The default aging time for all configured VLANs is 300 seconds.

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 **set cam** command does not support the MSM.

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 *vlan* number 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 port(s) are trunk ports, you must specify the VLAN.

Static (nonpermanent) entries will remain in the table until the active supervisor engine is reset.

The *route_descr* variable is entered as two hexadecimal bytes in the following format: 004F. Do not use a "-" to separate the bytes.

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)
```

Related Commands

clear cam
show cam

set cdp

Use the **set cdp** command set to enable, disable, or configure CDP features globally on all ports or on specified ports.

set cdp {**enable** | **disable**} {*mod/ports...*}

set cdp interval *interval*

set cdp holdtime *holdtime*

set cdp version v1 | **v2**

Syntax Description

enable	Keyword to enable the CDP feature.
disable	Keyword to disable the CDP feature.
mod/ports..	Number of the module and the ports on the module.
interval	Keyword to specify 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	Keyword to specify the global Time-To-Live value.
holdtime	Number of seconds for the global Time-To-Live value; valid values are from 10 to 255 seconds.
version v1 | **v2**	Keywords to specify the CDP version number.

Defaults

The default system configuration has CDP enabled. The message interval is set to 60 seconds for every port; the default Time-To-Live value has the message interval globally set to 180 seconds. The default CDP version is version 2.

Command Types

Switch command.

Command Modes

Privileged.

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 CDP is globally enabled, 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/port* 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 Time-To-Live value:

```
Console> (enable) set cdp holdtime 200
CDP holdtime set to 200 seconds.
Console> (enable)
```

Related Commands

show cdp

set channel cost

Use the **set channel cost** command to set the channel path cost and adjust the port costs of the ports in the channel automatically.

set channel cost *channel_id* | **all** [*cost*]

Syntax Description

channel_id	Number of the channel identification.
all	Keyword to configure all channels.
cost	(Optional) Port costs of the ports in the channel.

Defaults

The default is the port cost is updated automatically based on the current port costs.

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 costs of the channeling ports. If you change the channel cost, member ports in the channel might be modified and saved to NVRAM. If this is the case, a message appears to list the ports whose port path costs were updated due to the channel cost modification.

Examples

This example shows how to set the channel 768 path cost to 23:

```
Console> (enable) set channel cost 768 23
Port(s) 1/1-2,7/3,7/5 port path cost are updated to 60.
Channel 768 cost is set to 23.
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 channel cost all 15
Port(s) 4/1-4 port path cost are updated to 39.
Channel 768 cost is set to 15.
Warning:channel cost may not be applicable if channel is broken.
```

Related Commands

show channel

set channel vlancost

Use the **set channel vlancost** command to set the channel VLAN cost and automatically adjust the port VLAN costs of the ports in the channel.

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.

If you change the channel VLAN cost, member ports in the channel might be modified and saved to NVRAM. If this is the case, a message appears to list the ports whose port path costs were updated due to the channel cost modification.

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)
```

Related Commands

show channel

set config acl

Use the **set config acl** command to delete the ACL configuration from the NVRAM configuration and save the ACL to a specified file.

set config acl {**nvram**}

Syntax Description

nvram	Keyword to copy the ACL configuration to NVRAM.

Defaults

The default is NVRAM.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Once the configuration is moved to a Flash file, you must set up the auto-config feature by using the overwrite and append options from the **set boot config-register auto-config** command. You can also set the recurrence on other supervisor engines and switches by using this command.

If you specify multiple configuration files, you must separate the files with a semicolon (;).

If the ACL configuration location is set to **flash**, the following message displays after every commit operation for either Security or QoS:

```
Warning: Use the copy commands to save your ACL configuration to Flash.
```

If you reset the system and there were one or more commits done but no 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.
```

Examples

This example shows how to copy the ACL configuration to the bootflash file:

```
Console> (enable) set config acl flash switchapp.cfg
Upload ACL configuration to bootflash:switchapp.cfg
2843644 bytes available on device bootflash, proceed (y/n) [n]? y
Configuration has been copied successfully.
WARNING: Use the 'set boot config-register auto-config' commands to configure the
auto-config feature.
Console> (enable)
```

This example shows how to copy the ACL configuration to NVRAM:

```
Console> (enable) set config acl nvram
ACL configuration copied to NVRAM.
WARNING: Use the 'set boot config-register auto-config' commands to disable the
auto-config feature.
Console> (enable)
```

Related Commands

set boot config-register
set boot system flash
show boot
copy
clear config

set cops

Use the **set cops** command set to configure COPS functionality.

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	Keyword to set 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) Keyword to specify the primary server.
diff-serv	(Optional) Keyword to set the COPS server for differentiated services.
rsvp	(Optional) Keyword to set the COPS server for RSVP+.
domain-name *domain_name*	Keyword and variable to specify the domain name of the switch.
retry-interval	Keyword to specify 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 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 default portstatus

Use the **set default portstatus** command to set the default port status.

set default portstatus {**enable** | **disable**}

Syntax Description

enable	Keyword to activate default port status.
disable	Keyword to deactivate default port status.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you enter the **clear config all** command or in the event of a configuration loss, all ports collapse into VLAN 1. This might cause a security and network instability problem. Entering the **set default portstatus** command puts all ports into a disable state and blocks the traffic flowing through the ports during a configuration loss. You can then manually configure the ports back to the enable state.

After you enter the **set default portstatus** command, you must reset the system so the new configuration setup can take effect.

This command is not saved in the configuration file.

Once 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.
WARNING: Please reset the system to have new setup in effect.
Console> (enable)
```

Related Commands

show default

set enablepass

Use the **set enablepass** command to change the password for the privileged level of the CLI.

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

set errdisable-timeout

Use the **set errdisable-timeout** command to configure a timeout for ports in errdisable state, after which the ports are reenabled automatically.

set errdisable-timeout {**enable** | **disable**} {*reason*}

set errdisable-timeout interval {*interval*}

Syntax Description

enable	Keyword to enable errdisable timeout.
disable	Keyword to disable errdisable timeout.
reason	Reason for the port being in the errdisable state; valid values are **bpdu-guard**, **channel-misconfig**, **duplex-mismatch**, **udld**, **other**, and **all**.
interval *interval*	Timeout interval; valid values are from 30 to 86400 seconds (30 seconds to 24 hours).

Defaults

The default is **disable** and the *interval* is 300 seconds.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The errdisable timeout feature allows you to configure a timeout period for ports in errdisable state. When this feature is enabled, ports are reenabled automatically after the timeout interval has elapsed.

A port enters errdisable state for the following reasons (these reasons appear as configuration options with the set errdisable-timeout enable command):

- Channel misconfiguration
- Duplex mismatch
- BPDU port-guard
- UDLD
- Other (reasons other than the above)
- All (apply errdisable timeout to all reasons)

You can enable or disable errdisable timeout for each of the above listed reasons. The ports in errdisable state for reasons other than the first four reasons are considered "other." If you specify other, all ports errdisabled by causes other than the first four reasons are enabled for errdisable timeout. If you specify "all," all ports errdisabled for any reason are enabled for errdisable timeout.

Examples

This example shows how to enable an errdisable timeout for BPDU guard causes:

```
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)
```

Related Commands

show errdisable-timeout

set errordetection

Use the **set errordetection** command set to enable or disable various error detections.

set errordetection inband {**enable** | **disable**}

set errordetection memory {**enable** | **disable**}

Syntax Description

enable	Keyword to enable the specified error detection.
disable	Keyword to disable the specified error detection.
inband	Keyword to specify inband error detection.
memory	Keyword to specify memory error detection.

Defaults

The default is portcounters error detection is enabled, and memory and inband error detection is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **inband** keyword is not supported.

Examples

This example shows how to enable memory error detection:

```
Console> (enable) set errordetection memory enable
Memory error detection enabled.
Console> (enable)
```

Related Commands

show errordetection

set feature mdg

Use the **set feature mdg** command to enable or disable the multiple default gateway feature.

set feature mdg {**enable** | **disable**}

Syntax Description

enable	Keyword to enable the multiple default gateway.
disable	Keyword to disable the multiple default gateway.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privilege.

Usage Guidelines

If you enable the multiple default gateway feature, the Catalyst 6000 family switch pings the default gateways every 10 seconds to verify 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)
```

set garp timer

Use the **set garp timer** command to adjust the values of the join, leave, and leaveall timers.

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 default is the join timer default is 200 ms, the leave timer default is 600 ms, and the leaveall timer default is 10000 ms.

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 ms 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 to 300 ms 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)
```

This example shows how to set the leaveall timer value to 20000 ms for all the ports on all the VLANs:

```
Console> (enable) set garp timer leaveall 20000
GMRP/GARP LeaveAll timer value is set to 20000 milliseconds.
Console> (enable)
```

Related Commands

set gmrp timer
set gvrp timer
show gmrp timer

set gmrp

Use the **set gmrp** command to enable or disable GMRP on the switch in all VLANs on all ports.

set gmrp {**enable** | **disable**}

Syntax Description

enable	Keyword to enable GMRP on the switch.
disable	Keyword to disable 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

Use the **set gmrp fwdall** command to enable or disable the Forward All feature on a specified port or module and port list.

set gmrp fwdall {**enable** | **disable**} *mod/port...*

Syntax Description

enable	Keyword to enable GMRP Forward All on a specified port.
disable	Keyword to disable 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

Use the **set gmrp registration** command to specify the GMRP registration type.

set gmrp registration {**normal** | **fixed** | **forbidden**} *mod/port...*

Syntax Description

normal	Keyword to specify dynamic GMRP multicast registration and deregistration on the port.
fixed	Keyword to specify 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	Keyword to specify 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

Use the **set gmrp timer** command to adjust the values of the join, leave, and leaveall timers.

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 ms, the leave timer is 600 ms, and the leaveall timer is 10000 ms.

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 ms 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 ms 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 ms 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 **show gmrp timer**
set gvrp timer
set garp timer

set gvrp

Use the **set gvrp** command to enable or disable GVRP globally in the switch or on a per-port basis.

set gvrp {**enable** | **disable**} [*mod/port*]

Syntax Description

enable	Keyword to enable GVRP on the switch.
disable	Keyword to disable 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

show gmrp timer
show gvrp configuration
set gvrp timer
set garp timer

set gvrp applicant

Use the **set gvrp applicant** command to specify whether or not a VLAN is declared out of blocking ports.

set gvrp applicant {**normal** | **active**} {*mod/port*...}

Syntax Description

normal	Keyword to disallow the declaration of any VLAN out of blocking ports.
active	Keyword to enforce 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 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

Use the **set gvrp dynamic-vlan-creation** command to enable or disable dynamic VLAN creation.

set gvrp dynamic-vlan-creation {**enable** | **disable**}

Syntax Description

enable	Keyword to enable dynamic VLAN creation.
disable	Keyword to disable 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

Use the **set gvrp registration** command to set the administrative control of an outbound port and apply to all VLANs on the trunk. GVRP registration commands are entered on a per-port basis.

set gvrp registration {**normal** | **fixed** | **forbidden**} *mod/port..*

Syntax Description

normal	Keyword to allow dynamic registering and deregistering each VLAN (except VLAN 1) on the port.
fixed	Keyword to support manual VLAN creation and registration, prevent VLAN deregistration, and register all VLANs known to other ports.
forbidden	Keyword to specify 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 is administrative control is normal.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

When you set VLAN registration, you are telling the switch that the VLAN is interested in the user(s) connecting to this port and the VLAN's broadcast and multicast traffic is allowed to send 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

Use the **set gvrp timer** command to adjust the values of the join, leave, and leaveall timers.

set gvrp timer {*timer_type*} {*timer_value*}

Syntax Description

timer_type	Type of timer; valid values are **join**, **leave,** and **leaveall**.
timer_value	TimTimer values in milliseconds; valid values are from 1 to 2147483647 milliseconds.

Defaults

The default is the join timer is 200 ms, the leave timer is 600 ms, and the leaveall timer is 10000 ms.

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 ms 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 ms 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 ms 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

Use the **set igmp** command to enable or disable IGMP snooping on the switch.

set igmp {**enable** | **disable**}

Syntax Description

enable	Keyword to enable IGMP snooping on the switch.
disable	Keyword to disable 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.

Examples

This example shows how to enable IGMP snooping on the switch:

```
Console> (enable) set igmp enable
IGMP Snooping is 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
show igmp statistics
set rgmp

set igmp fastleave

Use the **set igmp fastleave** command to enable or disable IGMP fastleave processing.

set igmp fastleave {**enable** | **disable**}

Syntax Description

enable	Keyword to enable IGMP fastleave processing.
disable	Keyword to disable 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
show igmp statistics
set igmp

set igmp mode

Use the **set igmp mode** command to set the IGMP snooping mode.

set igmp mode {**igmp-only** | **igmp-cgmp** | **auto**}

Syntax Description

igmp-only	Keyword to specify IGMP snooping only.
igmp-cgmp	Keyword to specify IGMP and CGMP modes.
auto	Keyword to override the dynamic switching of IGMP snooping modes.

Defaults

The default 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 inlinepower defaultallocation

Use the **set inlinepower defaultallocation** command to set the default power allocation for a port.

set inlinepower defaultallocation *value*

Syntax Description

value	Default power allocation; valid values are from 2000 to 12500 mW.

Defaults

The default is 7000 mW.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the default power allocation to 2000 mW:

```
Console> (enable) set inlinepower defaultallocation 2000
Default inline power allocation set to 9500 mWatt per applicable port.
Console> (enable)
```

Related Commands

show environment power
show port inlinepower

set interface

Use the **set interface** command set to configure the in-band and SLIP interfaces on the switch.

set interface {**sc0** | **sl0**} {**up** | **down**}

set interface sc0 [*vlan*] [*ip_addr*[*/netmask*] [*broadcast*]]

set interface sl0 *slip_addr dest_addr*

set interface sc0 dchp {**renew** | **release** | **requestnew**}

Syntax Description

sc0	Keyword to specify the in-band interface.
sl0	Keyword to specify the SLIP interface.
up	Keyword to bring the interface into operation.
down	Keyword to bring the interface out of operation.
vlan	(Optional) Number of the VLAN to be assigned to the interface.
ip_addr	(Optional) IP address.
/netmask	(Optional) Subnet mask.
broadcast	(Optional) Broadcast address.
slip_addr	IP address of the console port.
dest_addr	IP address of the host to which the console port will be connected.
dhcp	Keyword to perform DHCP operations on the sc0 interface.
renew	Keyword to renew the lease on a DHCP-learned IP address.
release	Keyword to release a DHCP-learned IP address back to the DHCP IP address pool.
requestnew	Keyword used to request a new lease on a DHCP-learned IP address.

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.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Two configurable network interfaces are on a Catalyst 6000 family 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 via 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 via 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*, this indicates the number of bits allocated to subnetting in the hostid 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 hostid bits for this Class B address is 16. Any number of bits in the hostid bits can be allocated to the subnet field. If you do not enter the netmask, the number of bits is assumed to be the natural netmask.

The **set interface sc0 dchp** command is valid only when the address is learned from the DHCP server and available in privileged mode only.

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 request a new lease on a DHCP-learned IP address:

```
Console> (enable) set interface sc0 dhcp requestnew
Requesting new IP address...Done
Console> (enable)
```

Related Commands **show interface**
slip

set ip alias

Use the **set ip alias** command to add aliases of IP addresses.

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

Use the **set ip dns** command to enable or disable DNS.

set ip dns {**enable** | **disable**}

Syntax Description

enable	Keyword to enable DNS.
disable	Keyword to disable 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

set ip dns domain

Use the **set ip dns domain** command to set the default DNS domain name.

set ip dns domain *name*

Syntax Description

name	DNS domain name.

Defaults

This command has no default setting.

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 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

Use the **set ip dns server** command to set the IP address of a DNS server.

set ip dns server *ip_addr* [**primary**]

Syntax Description

ip_addr	IP address of the DNS server.
primary	(Optional) Keyword to configure a DNS server as the primary server.

Defaults

This command has no default setting.

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

Use the **set ip fragmentation** command to enable or disable the fragmentation of IP packets bridged between FDDI and Ethernet networks. Note that FDDI and Ethernet networks have different MTUs.

set ip fragmentation {**enable** | **disable**}

Syntax Description

enable	Keyword to permit fragmentation for IP packets bridged between FDDI and Ethernet networks.
disable	Keyword to disable fragmentation for IP packets bridged between FDDI and Ethernet networks.

Defaults

The default value is IP fragmentation enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If IP fragmentation is disabled, packets are dropped.

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

Use the **set ip http port** command to configure the TCP port number for the HTTP server.

set ip http port {**default** | *port-num*}

Syntax Description

default	Keyword to specify the default HTTP server port number (80).
port-num	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

Use the **set ip http server** command to enable or disable the HTTP server.

set ip http server {**enable** | **disable**}

Syntax Description

enable	Keyword to enable the HTTP server.
disable	Keyword to disable 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

Use the **set ip permit** command set to enable or disable the IP permit list and to specify IP addresses to be added to the IP permit list.

set ip permit {**enable** | **disable**}

set ip permit {**enable** | **disable**} [**telnet** | **snmp**]

set ip permit *ip_addr* [*mask*] [**telnet** | **snmp** | **all**]

Syntax Description

enable	Keyword to enable the IP permit list.
disable	Keyword to disable the IP permit list.
telnet	(Optional) Keyword to specify removal from the Telnet IP permit list.
snmp	(Optional) Keyword to specify removal from the SNMP IP permit list.
all	Keyword to specify all entries in the IP permit list be removed.
ip_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.

Defaults

The default is IP permit list is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The same functionality of the IP permit list can be achieved by using VACLs. VACLs are handled by hardware (PFC) and the processing is considerably faster. For VACL configuration information, refer to the *Catalyst 6000 Family Multilayer Switch Feature Card and Policy Feature Card 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 specfiy the **snmp**, **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
IP permit list enabled.
Console> (enable)
```

This example shows how to disable the IP permit list:

```
Console> (enable) set ip permit disable
IP permit list disabled.
Console> (enable)
```

Related Commands

clear ip permit
show ip permit

set ip redirect

Use the **set ip redirect** command to enable or disable ICMP redirect messages on the Catalyst 6000 family switches.

set ip redirect {**enable** | **disable**}

Syntax Description

enable	Keyword to permit ICMP redirect messages to be returned to the source host.
disable	Keyword to prevent 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

Use the **set ip route** command to add IP addresses or aliases to the IP routing table.

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) Keyword 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 is now the secondary default IP gateway.

You can only specify the **primary** keyword for a default route.

When you enter the *destination* or *gateway*, enter it in dot notation, for example, a.b.c.d.

When you specify the *netmask*, this indicates the number of bits allocated to subnetting in the hostid 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 hostid bits for this Class B address is 16. Any number of bits in the hostid bits can be allocated to the netmask field. If you do not enter the *netmask*, 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 unreachable

Use the **set ip unreachable** command to enable or disable ICMP unreachable messages on the Catalyst 6000 family switch.

set ip unreachable {**enable** | **disable**}

Syntax Description

enable	Keyword to allow IP unreachable messages to be returned to the source host.
disable	Keyword to prevent 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

Use the **set kerberos clients mandatory** command to make Kerberos authentication mandatory for authenticating to services on the network.

set 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

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

set kerberos credentials forward
clear kerberos clients mandatory
show kerberos

set kerberos credentials forward

Use the **set kerberos credentials forward** command to configure clients to forward users' credentials as they connect to other hosts in the Kerberos realm.

set kerberos credentials forward

Syntax Description

This command has no arguments or keywords.

Defaults

Forwarding is disabled by default.

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 credentials forward
set kerberos clients mandatory
show kerberos creds

set kerberos local-realm

Use the **set kerberos local-realm** command to configure a switch to authenticate users defined in the Kerberos database.

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 Kerberos realms in 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

set kerberos realm
clear kerberos realm
show kerberos

set kerberos realm

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

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 setting.

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

set kerberos local-realm
clear kerberos realm
show kerberos

set kerberos server

Use the **set kerberos server** command to specify which KDC to use on the switch.

set kerberos server *kerberos_realm* {*hostname* | *ip_address*} [*port*]

Syntax Description

kerberos_realm	Keyword specifying 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 setting.

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

set kerberos server
clear kerberos server
show kerberos

set kerberos srvtab entry

Use the **set kerberos srvtab entry** command to enter the SRVTAB file directly into the switch from the command line.

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 setting.

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 DES 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

Use the **set kerberos srvtab remote** command to provide the switch with a copy of the SRVTAB file from the KDC that contains the secret key.

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 setting.

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

set kerberos srvtab entry
clear kerberos creds
show kerberos

set key config-key

Use the **set key config-key** command to define a private DES key.

set key config-key *string*

Syntax Description

string	DES key name.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can define a private DES key for the switch. You can use the private DES key to encrypt the secret key that the switch shares with the KDC. If you set the DES 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 DES key:

```
Console> (enable) set key config-key abcd
Kerberos config key set to abcd
Console> (enable)
```

Related Commands

clear key config-key

set lcperroraction

Use the **set lcperroraction** command to configure how your system handles LCP errors when a module reports an ASIC problem to the NMP.

set lcperroraction *action*

Syntax Description

action	Action for handling LCP errors. See "Usage Guidelines" 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

Use the **set lda** command set to configure the ASLB information on the Catalyst 6000 family switch.

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**	Keyword to enable or disable the ASLB feature.
vip *server_virtual_ip destination_tcp_port*	Keyword and variables to specify 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*	Keyword and variables to specify the LD MAC address.
mac router *mac_address...*	Keyword and variable to specify the router MAC address.
router *router_vlan*	Keyword and variable to specify 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*	Keyword and variable to specify the server VLAN.
udpage *udpagetime*	Keyword and variable to specify the UDP aging time for LocalDirector acceleration.

Defaults

The default is the ASLB is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can enter a zero (0) as a wildcard (don't care) digit for the *destination_tcp_port*.

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* is specified in milliseconds; values are from 0 ms to 2024000 ms.

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

commit lda
show lda
clear lda

set length

Use the **set length** command to configure the number of lines in the terminal display screen.

set length *number* [**default**]

Syntax Description

number	Number of lines to display on the screen; valid values are from 0 to 512.
default	(Optional) Keyword to set 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, it 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 factory-set 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 logging console

Use the **set logging console** command to enable and disable the sending of system logging messages to the console.

set logging console {**enable** | **disable**}

Syntax Description

enable	Keyword to enable system message logging to the console.
disable	Keyword to disable 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.
```

Related Commands

set logging level
set logging session
show logging
show logging buffer

set logging history

Use the **set logging history** command to set the size of the syslog history table.

set logging history *syslog_history_table_size*

Syntax Description

syslog_history_table_size	Size of the syslog history table; valid values are from 0 to 500.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

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)
```

Related Commands

show logging
clear logging buffer

set logging level

Use the **set logging level** command to set the facility and severity level used when logging system messages.

set logging level *facility severity* [**default**]

Syntax Description

facility	Value that specifies the type of system messages to capture; facility types are listed in Table 2-8.
severity	Value that specifies the severity level of system messages to capture; severity level definitions are listed in Table 2-9.
default	(Optional) Keyword to cause the specified logging level to apply to all sessions.

Table 2-8 Facility Types

Facility Name	Definition
all	All facilities
acl	ACL facility
cdp	Cisco Discovery Protocol
dtp	Dynamic Trunking Protocol
drip	DRIP facility
earl	Enhanced Address Recognition Logic
fddi	FDDI 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
radius	Remote Access Dial-In User Service
security	Security
snmp	Simple Network Management Protocol

Table 2-8 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
vtp	Virtual Terminal Protocol

Table 2-9 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

show logging
show logging buffer

set logging server

Use the **set logging server** command set to enable and disable system message logging to configured syslog servers and to add a syslog server to the system logging server table.

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	Keyword to enable system message logging to configured syslog servers.
disable	Keyword to disable system message logging to configured syslog servers.
ip_addr	IP address of the syslog server to be added to the configuration.
severity *severity*	Keyword and variable to globally set the syslog maximum severity control for all message types; severity level definitions are listed in Table 2-9.
facility	Type of system messages to capture; server facility types are listed in Table 2-10.

Table 2-10 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 **set logging level** command. The server severity level must be greater than or equal to the default severity level of those message facility that you expect to receive in syslog messages on the syslog server.

An IP alias or a host name that can be resolved through DNS can also be used.

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

Use the **set logging session** command to enable or disable the sending of system logging messages to the current login session.

set logging session {**enable** | **disable**}

Syntax Description

enable	Keyword to enable the sending of system logging messages to the current login session.
disable	Keyword to disable 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 logout

Use the **set logout** command to set the number of minutes until the system disconnects an idle session automatically.

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.

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)
```

set mls agingtime

Use the **set mls agingtime** command to specify the MLS aging time of shortcuts to an MLS entry in the Catalyst 6000 family switches.

set mls agingtime [**ip** | **ipx**] {*agingtime*}

set mls agingtime fast {*fastagingtime*} {*pkt_threshold*}

Syntax Description

ip	(Optional) Keyword to specify IP MLS.
ipx	(Optional) Keyword to specify IPX MLS.
agingtime	MLS aging time of shortcuts to an MLS entry; valid values are multiples of 8 to any value in the range of 8 to 2032 seconds.
fast	Keyword to specify 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 multiples of 8 to any value in the range from 0 to 128 seconds.
pkt_threshold	Packet threshold value; valid values are 0, 1, 3, 7, 15, 31, 63, and 127 packets.

Defaults

The default *agingtime* is 256 seconds. The default *fastagingtime* is 0, no fast aging. The default *pkt_threshold* is 0.

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 use the **ipx** keyword, you are specifying a shortcut for IPX MLS.

If you enter *fastagingtime* **0**, 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 6000 family switch without MLS, this warning message displays:

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

agingtime can be configured as multiples of 8 in the range of 8 to 2024 seconds. The values are picked up in numerical order to achieve efficient aging. Any value for *agingtime* that is not a multiple of 8 seconds is adjusted to the closest one. For example, 65 is adjusted to 64, while 127 is adjusted to 128.

fastagingtime can be configured as multiples of 8 to any value in the range of 0 to 128 seconds.

The default *pkt_threshold* is 0. It can be configured as 0, 1, 3, 7, 15, 31, 63, or 127 (the values picked for efficient aging). 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).

Agingtime 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/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 32K. If the number of MLS entries exceed 32K, some flows (less than 1 percent) are sent to the router.

To keep the number of MLS cache entries below 32K, 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 32K, decrease the normal aging time in 64-second increments from the 256-second default.

Examples

These examples show how to set the agingtime:

```
Console> (enable) set mls agingtime 512
IP Multilayer switching aging time set to 512 seconds.
Console> (enable)

Console> (enable) set mls agingtime ipx 512
IPX Multilayer switching aging time set to 512
Console> (enable)
```

This example shows how to set the fast agingtime:

```
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)
```

Related Commands

clear mls
show mls

set mls exclude protocol

Use the **set mls exclude protocol** command to add a protocol port to be excluded from being shortcut.

set mls exclude protocol {**tcp** | **udp** | **both**} {*port*}

Syntax Description

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

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter any of the **set mls** commands on a Catalyst 6000 family switch without MLS, this warning message displays:

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

You can add a maximum of four protocol ports to the exclude table.

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)
```

This example shows the output if you exceed the exclude table maximum:

```
Console> (enable) set mls exclude protocol tcp 6019
Failed to exclude protocol. Exclude table full.
Use 'clear mls exclude' command to remove an existing entry.
Console> (enable)
```

Related Commands **clear mls**
show mls

set mls multicast

Use the **set mls multicast** command to enable or disable the IP multicast MLS feature.

set mls multicast enable | **disable**

Syntax Description

enable	Keyword to enable IP multicast MLS functions on the switch and allow new shortcut entries to be established.
disable	Keyword to disable IP multicast MLS functions on the Catalyst 6000 family switches, delete any existing shortcut entries, and prevent new shortcut entries from being established.

Defaults

The default is the IP multicast MLS feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

IPX MLS is disabled globally by default, but can be enabled and disabled on a specified interface. To enable or disable IPX MLS on a specified interface, refer to the *Catalyst 6000 Family Multilayer Switch Feature Card and Policy Feature Card Configuration Guide*.

Your system needs to be configured with a Layer 3 switching engine-based system to enable MLS.

If you enter any **set mls multicast** commands on a Catalyst 6000 family switch without MLS, this warning message displays:

```
This feature is not supported on this device
```

If you enter any **set mls multicast** services on a Catalyst 6000 family switch and none of the multicast protocols (such as IGMP snooping, CGMP, and GMRP) are enabled, this warning message displays:

```
Enable IGMP Snooping/CGMP/GMRP to make this feature operational.
```

You can configure a maximum of two participating routers, but they must be internally or directly attached to a Catalyst 6000 family switch. Refer to the *Catalyst 6000 Family Software Configuration Guide* for router configuration information.

Use the **set mls include** command to specify routers for IP multicast MLS.

Examples

This example shows how to use the **set mls multicast** command to enable MLS for IP multicast traffic:

```
Console> (enable) set mls multicast enable
Multilayer switching for Multicast is enabled for this device.
Console> (enable)
```

This example shows how to use the **set mls multicast** command to disable MLS for IP multicast traffic:

```
Console> (enable) set mls multicast disable
Multilayer switching for Multicast is disabled for this device.
Console> (enable)
```

Related Commands

show mls multicast

set mls nde

Use the **set mls nde** command set to configure the NDE feature in the Catalyst 6000 family switches to allow command-exporting statistics to be sent to the preconfigured collector.

set mls nde {**enable** | **disable**}

set mls nde {*collector_ip* | *collector_name*} {*udp_port_num*}

set mls nde version {**1** | **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*]

Syntax Description

enable	Keyword to enable NDE.
disable	Keyword to disable 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	Keyword to specify the version of the Netflow Data Export; valid versions are 1, 7, and 8.
1 | **7** | **8**	Version of the NDE feature.
flow	Keyword to add filtering to NDE.
exclude	(Optional) Keyword to allow exporting of all flows except the flows matching the given filter.
include	(Optional) Keyword to allow exporting of all flows matching the given filter.
destination	(Optional) Keyword to specify 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) Keyword to specify the source IP address.
protocol	(Optional) Keyword to specify 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) Keyword and variable to specify 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) Keyword and variable to specify 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 defaults are Netflow Data Export version 7, and all expired flows are exported until the filter is specified explicitly.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter any **set mls nde** commands on a Catalyst 6000 family switch without MLS, this warning message displays:

```
mls not supported on feature card.
```

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.

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.

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.

Examples

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 only expired flows from a specific host to a specific destination port are exported:

```
Console> (enable) set mls nde flow include source 171.69.194.140 dst_port 23
NDE destination filter set to 171.69.194.140/32, source port filter set to 23.
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 specify that all flows are exported:

```
Console> (enable) clear mls nde flow both
NDE filter cleared.
Console> (enable)
```

Related Commands

clear mls nde flow
show mls

set mls statistics protocol

Use the **set mls statistics protocol** command to add protocols to the protocols statistics list.

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 setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

If you enter any **set mls** commands on a Catalyst 6000 family switch without MLS, this warning message displays:

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

You can configure a maximum of 64 ports using the **set mls statistics protocol** command.

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
show mls statistics

set module

Use the **set module** command to enable or disable a module.

set module enable | **disable** *mod*

Syntax Description

enable	Keyword to enable a module.
disable	Keyword to disable 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 via a Telnet session; if you disable your session, you will disconnect your Telnet session.

If there are no other network connections to a Catalyst 6000 family 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 via the console port:

```
Console> (enable) set module disable 3
Module 3 disabled.
Console> (enable)
```

This example shows how to disable module 2 when connected via 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.
```

Related Commands **show module**

set module name

Use the **set module name** command to set the name for a module.

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 RSM. Additional **set module** commands are not supported by the RSM.

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

Use the **set module power** command to turn on or shut off the power to a module.

set module power up | **down** *mod*

Syntax Description

up	Keyword to turn on the power to a module.
down	Keyword to turn off the power to a module.
mod	Number of the module.

Defaults

The default is power is on to a module.

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 displays:

```
Module 4 could not be powered up due to insufficient power.
```

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

show environment

set module shutdown

Use the **set module shutdown** command to shutdown the NAM and IDS modules.

set module shutdown all | *mod*

Syntax Description

all	Keyword to shutdown all NAM and IDS modules.
mod	Number of the module.

Defaults

This command has no default setting.

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 6000 family 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 IDS:

```
Console> (enable) set module shutdown 2


Console> (enable)
```

set msmautostate

Use the **set msmautostate** command to enable or disable the line protocol state determination of the MSMs due to port state changes.

set msmautostate {**enable** | **disable**}

Syntax Description

enable	Keyword to activate the line protocol state determination.
disable	Keyword to deactivate 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 6000 family 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
Console> (enable)
```

This example shows how to disable the line protocol state determination of the MSM:

```
Console> (enable) set msmautostate disable
Console> (enable)
```

Related Commands

show msmautostate

set multicast router

Use the **set multicast router** command to configure a port manually as a multicast router port.

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 router
show multicast group count

set ntp broadcastclient

Use the **set ntp broadcastclient** command to enable or disable NTP in broadcast-client mode.

set ntp broadcastclient {**enable** | **disable**}

Syntax Description

enable	Keyword to enable NTP in broadcast-client mode.
disable	Keyword to disable 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 6000 family 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

Use the **set ntp broadcastdelay** command to configure a time-adjustment factor so the Catalyst 6000 family switch can receive broadcast packets.

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 ms.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the NTP broadcast delay to 4000 ms:

```
Console> (enable) set ntp broadcastdelay 4000
NTP broadcast delay set to 4000 microseconds.
Console> (enable)
```

Related Commands

show ntp

set ntp client

Use the **set ntp client** command to enable or disable a Catalyst 6000 family switch as an NTP client.

set ntp client {**enable** | **disable**}

Syntax Description

enable	Keyword to enable a Catalyst 6000 family switch as an NTP client.
disable	Keyword to disable a Catalyst 6000 family 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 6000 family switch. The client mode assumes that the client (a Catalyst 6000 family 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

Use the **set ntp server** command to configure the IP address of the NTP server.

set ntp server *ip_addr*

Syntax Description

ip_addr	IP address of the NTP server providing the clock synchronization.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The client mode assumes that the client (a Catalyst 6000 family 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 password

Use the **set password** command to change the login password on the CLI.

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 port auxiliaryvlan

Use the **set port auxiliaryvlan** command to configure the auxiliary VLAN ports.

set port auxiliaryvlan *mod*[*/ports*] {*vlan* | **untagged** | **dot1p** | **none**}

Syntax Description

mod [*/ports*]	Number of the module and (optional) ports.
vlan	Number of the VLAN; valid values are from 1 to 1000.
untagged	Keyword to specify the IP Phone 7960 send untagged packets without 802.1p priority.
dot1p	Keyword to specify the IP Phone 7960 send packets with 802.1p priority.
none	Keyword to specify that the switch does not send any auxiliary VLAN information in the CDP packets from that port.

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 IP Phone 7960 send packets tagged with a specific VLAN.

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

Use the **set port broadcast** command to set the broadcast suppression for one or more ports. The broadcast threshold limits the backplane traffic received from the module.

set port broadcast *mod/port threshold***%**

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 broadcast traffic.

Defaults

The default is broadcast suppression is disabled (no broadcast limit).

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to limit broadcast traffic to 20 percent to all ports on module 4:

```
Console> (enable) set port broadcast 4/3 20%
Port 4/1-24 broadcast traffic limited to 20.00%.
Console> (enable)
```

This example shows how to allow unlimited broadcast traffic to all ports on module 4:

```
Console> (enable) set port broadcast 4/3 100%
Port 4/1-24 broadcast traffic unlimited.
Console> (enable)
```

Related Commands

clear port broadcast
show port broadcast

set port channel

Use the **set port channel** command set to configure EtherChannel on Ethernet module ports.

set port channel *mod/port* [*admin_group*]

set port channel *mod/port* **mode** {**on** | **off** | **desirable** | **auto**} [**silent** | **non-silent**]

set port channel all distribution {ip | mac} [source | destination | both]

Syntax Description

mod/port	Number of the module and the port on the module.
admin_group	(Optional) Number of administrative group; valid values are from 1 to 1024.
mode	Keyword to specify the EtherChannel mode.
on	Keyword to enable and force specified ports to channel without PAgP.
off	Keyword to prevent ports from channeling.
desirable	Keyword to set 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	Keyword to set 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) Keyword to use 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) Keyword to use with **auto** or **desirable** when traffic is expected from the other device.
all distribution	Keywords to apply frame distribution to all ports in the switch.
ip	Keyword to specify the frame distribution method using IP address values.
mac	Keyword to specify the frame distribution method using MAC address values.
source	(Optional) Keyword to specify the frame distribution method using source address values.
destination	(Optional) Keyword to specify the frame distribution method using destination address values.
both	(Optional) Keyword to specify the frame distribution method using source and destination address values.

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.

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 6000 Family 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 admin group, the original ports associated with the admin group will move to an automatically picked new admin group. You cannot add ports to the same admin group.

If you do not enter an *admin_group*, it means that you want to create a new administrative group with *admin_group* selected automatically. The next available *admin_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.

This command is not supported by non-EtherChannel-capable modules.

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.
```

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 admin 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 admin 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 admin 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 port channel
show channel
show channel group

set port cops

Use the **set port cops** command to create port roles.

set port cops *mod/port* **roles** *role1* [*role2*]...

Syntax Description

mod/port	Number of the module and the port on the module.
roles *role#*	Keyword and variable to specify 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

set port disable

Use the **set port disable** command to disable a port or a range of ports.

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 duplex

Use the **set port duplex** command to configure the duplex type of an Ethernet port or a range of ports.

set port duplex *mod/port* {**full** | **half**}

Syntax Description

mod/port	Number of the module and the port on the module.
full	Keyword to specify full-duplex transmission.
half	Keyword to specify 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.

Gigabit ports only support full-duplex mode.

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

Use the **set port enable** command to enable a port or a range of ports.

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 flowcontrol

Use the **set port flowcontrol** command to configure a port to send or receive pause frames. 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	Keyword to specify a port processes pause frames.
send	Keyword to specify a port sends pause frames.
off	Keyword to prevent a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
on	Keyword to enable a local port to receive and process pause frames from remote ports or send pause frames to remote ports.
desired	Keyword to obtain 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 100BaseFX and 48-port 10/100 BaseTX 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 100BaseFX and 48-port 10/100 BaseTX 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 2-11 describes guidelines for different configurations of the **send** and **receive** keywords.

Table 2-11 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

Use the **set port gmrp** command to enable or disable GMRP on the specified ports in all VLANs.

set port gmrp {*mod/port*} {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to enable GVRP on a specified port.
disable	Keyword to disable 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

Use the **set port gvrp** command to enable or disable GVRP on the specified ports in all VLANs.

set port gvrp {*mod/port*} {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to enable GVRP on a specified port.
disable	Keyword to disable 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 **show gvrp configuration**
set gvrp
clear gvrp statistics

set port host

Use the **set port host** command to optimize the port configuration for a host connection.

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 setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

The **set port host** command sets channel mode to off, enables spanning tree PortFast, and sets the trunk mode to off. 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.
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

Use the **set port inlinepower** command to set the inline power mode of a port or group of ports.

set port inlinepower *mod/ports* {**off** | **auto**}

Syntax Description

mod/ports	Number of the module and the ports on the module.
off	Keyword to not power up the port even if an unpowered phone is connected.
auto	Keyword to power up the port only if the switching module has discovered the phone.

Defaults

The default is **auto**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

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.

An inline power-capable device can still be detected even if the inlinepower mode is set to off.

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 inlinepower 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 inlinepower 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 defaultallocation
show environment power
show port inlinepower

set port jumbo

Use the **set port jumbo** command to enable or disable the jumbo frame feature on a per-port basis.

set port jumbo {*mod/port*} {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to enable jumbo frames on a specified port.
disable	Keyword to disable 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.

You can use the jumbo frame feature to transfer large frames or jumbo frames through Catalyst 6000 family switches to optimize server-to-server performance.

The jumbo frames feature is only supported on Layer 2-switched frames.

The MSFC and MSM do not support the routing of jumbo frames; if jumbo frames are sent to these routers, router performance is significantly degraded.

The GSR supports jumbo frames.

To enable the jumbo frame feature on a port, the port must meet the following conditions:

- The port must be a Gigabit Ethernet port.
- The trunking mode on the port must be set to OFF.
- The channeling mode on the port must be set to OFF.

For information on how to set the jumbo frame MTU size, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com.

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)
```

This example shows what happens if you try to enable the jumbo frames feature on a port that is not a Gigabit Ethernet port:

```
Console> (enable) set port jumbo 3/1 enable
Feature not supported on port 3/1.
Console> (enable)
```

This example shows what happens if you try to enable the jumbo frames feature on a port that does not have the trunking mode set to OFF:

```
Console> (enable) set port jumbo 6/1 enable
Failed to enable the port jumbo frame feature on port 6/1.
The trunking mode for jumbo enabled ports must be set to off.
Console> (enable)
```

This example shows what happens if you try to enable the jumbo frames feature on a port that does not have the channeling mode set to OFF:

```
Console> (enable) set port jumbo 6/2 enable
Failed to enable the port jumbo frame feature on port 6/2.
The channelling mode for jumbo enabled ports must be set to off.
Console> (enable)
```

Related Commands

set port channel
set trunk
show port jumbo

set port membership

Use the **set port membership** command to set the VLAN membership assignment to a port.

set port membership *mod/port* {**dynamic** | **static**}

Syntax Description

mod/port	Number of the module and the port on the module.
dynamic	Keyword to specify the port become a member of dynamic VLANs.
static	Keyword to specify the port become a member of static VLANs.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

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 vlan
set vlan mapping
set pvlan
set pvlan mapping

set port name

Use the **set port name** command to configure a name for a port.

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 module.

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.

If you do not specify the name string, 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

show port

set port negotiation

Use the **set port negotiation** command to enable or disable the link negotiation protocol on the specified port.

set port negotiation *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to enable the link negotiation protocol.
disable	Keyword to disable the link negotiation protocol.

Defaults

The default is link negotiation protocol is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The **set port negotiation** command is supported on 1000Base (SX, LX, and ZX) modules only.

If the port does not support this command, the following message appears:

```
Feature not supported on Port N/N.
```

where N/N is the module and port number.

When you enable link negotiation, the system autonegotiates flow control, duplex mode, and remote fault information.

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

Use the **set port protocol** command to enable or disable protocol membership of ports.

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	Keyword to specify IP.
ipx	Keyword to specify IPX.
group	Keyword to specify VINES, AppleTalk, and DECnet protocols.
on	Keyword to indicate the port will receive all the flood traffic for that protocol.
off	Keyword to indicate the port will not receive any flood traffic for that protocol.
auto	Keyword to indicate the port will not receive any flood traffic for that protocol.

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**

set port qos

Use the **set port qos** command to specify whether an interface is interpreted as a physical port or as a VLAN.

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	Keyword to interpret the interface as a physical port.
vlan-based	Keyword to interpret the interface as part of a VLAN.

Defaults

The default is ports are port-based.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Changing a port from port-based to VLAN-based QoS detaches all ACLs from the port. Any ACLs attached to the VLAN apply to the port immediately.

When you set a port to VLAN-based using the **set port qos** command with RSVP or COPS enabled on that port, the QoS policy-source is COPS or DSBM-election is enabled. The VLAN-based setting has been 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 to VLAN-based 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

show port qos
set port qos cos
set port qos trust
show qos info

set port qos cos

Use the **set port qos cos** command to set the default value for all packets that have arrived through an untrusted port.

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*	Keyword and variable to specify the CoS value for a port; valid values are from 0 to 7.
cos-ext *cos_value*	Keyword and variable to specify 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 not supported by the NAM.

If the default is enforced when you disable QoS, CoS is enforced when you enable QoS.

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
show port qos
show qos info
set port qos trust
set port qos
show qos info

set port qos trust

Use the **set port qos trust** command to set the trusted state of a port; for example, whether 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	Keyword to specify that packets need to be reclassified from the matching ACE.
trust-cos	Keyword to specify 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	Keyword to specify that although the ToS/CoS bits in the incoming packets are trusted, the ToS is invalid and the ToS is set as IP Precedence.
trust-dscp	Keyword to specify that the ToS/CoS bits in the incoming packets can be accepted as is with no change.

Defaults

The default when you enable QoS 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 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 **show qos info**
show port qos
set port qos
set port qos cos

set port qos trust-ext

Use the **set port qos trust-ext** command to configure the access port on an IP phone connected to the switch port.

set port qos *mod/ports...* **trust-ext** {**trusted** | **untrusted**}

Syntax Description

mod/ports...	Number of the module and the ports on the module.
untrusted	Keyword to specify that all traffic in 802.1Q or 802.1p frames received through the access port is marked with a configured Layer 2 CoS value.
trusted	Keyword to specify that all traffic received through the access port passes through the phone switch unchanged.

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

show qos info
show port qos
set port qos
set port qos cos

set port rsvp dsbm-election

Use the **set port rsvp dsbm-election** command to specify whether or not the switch participates in the DSBM election on that particular segment.

set port rsvp *mod/port* **dsbm-election enable** | **disable** [*dsbm_priority*]

Syntax Description

mod/port	Number of the module and the port.
enable	Keyword to enable participation in the DSBM election.
disable	Keyword to disable 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

Use the **set port security** command set to configure port security on a port or range of ports.

set port security *mod/ports...* [**enable** | **disable**] [*mac_addr*] [**age** {*age_time*}] [**maximum** {*num_ of_mac*}] [**shutdown** {*shutdown_time*}] [**violation** {**shutdown** | **restrict**}]

Syntax Description

mod/ports...	Number of the module and the ports on the module.
enable	(Optional) Keyword to enable port security.
disable	(Optional) Keyword to disable port security.
mac_addr	(Optional) Secure MAC address of the enabled port.
age *age_time*	(Optional) Keyword and variable to specify the duration for which addresses on the port will be secured; valid values are 0 (to disable) and from 10 to 1440 (minutes).
maximum *num_of_mac*	(Optional) Keyword and variable to specify the maximum number of MAC addresses to secure on the port; valid values are from 1 to 1025.
shutdown *shutdown_time*	(Optional) Keyword and variable to specify the duration for which a port will remain disabled in case of a security violation; valid values are 0 (to disable) and from 10 to 1440 (minutes).
violation	(Optional) Keyword to specify the action to be taken in the event of a security violation.
shutdown	Keyword to shut down the port in the event of a security violation.
restrict	Keyword to restrict packets from unsecure hosts.

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.

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. The maximum number is 1024.

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.

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 01-02-03-04-05-06
Port 3/1 port security enabled with 01-02-03-04-05-06 as the secure mac address.
Console> (enable)
```

This example sets 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 sets 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)
```

Related Commands **show port security**
clear port security

set port speed

Use the **set port speed** command to configure the speed of a port interface. You can configure the speed of a Fast Ethernet interface.

set port speed *mod/port* {**10** | **100** | **auto**}

Syntax Description

mod/port	Number of the module and the port on the module.
10 | **100** | **auto**	Keyword to set a port speed to 10 Mbps, 100 Mbps, or autospeed detection mode.

Defaults

The default is **auto**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can configure Fast Ethernet interfaces on the 10/100-Mbps Fast Ethernet switching module to either 10 or 100 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.

This command is not supported by the Gigabit Ethernet switching module or the NAM.

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 trap

Use the **set port trap** command to enable or disable the operation of the standard SNMP link trap (up or down) for a port or range of ports.

set port trap *mod/port* {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to activate the SNMP link trap.
disable	Keyword to deactivate 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

set port disable
set port duplex
set port enable
set port speed
show port

set port voice interface dhcp

Use the **set port voice interface dhcp** command to set the port voice interface for the DHCP, TFTP, and DNS servers.

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	Keyword to activate the SNMP link trap.
vlan *vlan*	(Optional) Keyword and variable to specify a VLAN interface.
disable	Keyword to deactivate the SNMP link trap.
ipaddrspec	IP address and mask; see the "Usage Guidelines" section for format instructions.
tftp *ipaddr*	Keyword and variable to specify the number of the TFTP server IP address or IP alias in dot notation a.b.c.d.
gateway *ipaddr*	(Optional) Keyword and variable to specify the number of the gateway server IP address or IP alias in dot notation a.b.c.d.
dns	(Optional) Keyword to specify 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 setting.

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 4/2-9 123.23.32.1/24
Single port must be used when setting the IP address.
Console> (enable)
```

Related Commands

show port voice interface

set power redundancy

Use the **set power redundancy** command to turn redundancy between the power supplies on or off.

set power redundancy enable | **disable**

Syntax Description

enable	Keyword to activate redundancy between the power supplies.
disable	Keyword to deactivate 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 between the power supplies on or off. In a redundant configuration, the power available to the system is the maximum power capability of the weakest supply.

In a nonredundant configuration, the power available to the system is the sum of the power capability of both supplies.

Examples

This example shows how to activate redundancy between power supplies:

```
Console> (enable) set power redundancy enable
Power supply redundancy enabled.
```

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 system
show environment

set prompt

Use the **set prompt** command to change the prompt for the CLI.

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

Use the **set protocolfilter** command to activate or deactivate protocol filtering on Ethernet VLANs and on nontrunking Ethernet, Fast Ethernet, and Gigabit Ethernet ports.

set protocolfilter {**enable** | **disable**}

Syntax Description

enable	Keyword to activate protocol filtering.
disable	Keyword to deactivate 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.

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

Use the **set pvlan** command to bind the isolated or community VLAN to the primary VLAN and assign the isolated or community ports to the private VLAN.

set pvlan *primary_vlan* {*isolated_vlan* | *community_vlan*} [*mod/port*]

Caution We recommend that you read and understand the "Configuring VLANs" chapter in the *Catalyst 6000 Family 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.
mod/port	(Optional) Module and port numbers of the isolated or community ports.

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* 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 and/or multiple community VLANs associated to it.

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)
```

Related Commands

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

set pvlan mapping

Use the **set pvlan mapping** command to map isolated or community VLANs to the primary VLAN on the promiscuous port.

set pvlan mapping *primary_vlan* {*isolated_vlan* | *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.
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 bound 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

set vlan
show vlan
set pvlan
clear vlan
clear pvlan mapping
show pvlan
show pvlan mapping

set qos

Use the **set qos** command to turn on or turn off QoS functionality on the switch.

set qos enable | **disable**

Syntax Description

enable	Keyword to activate QoS functionality.
disable	Keyword to deactivate QoS functionality.

Defaults

The default is QoS functionality is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Refer to the *Catalyst 6000 Family 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
<...trunking reset messages deleted ...>
QoS is enabled.
Console> (enable)
```

This example shows how to disable QoS:

```
Console> (enable) set qos disable
<...trunking reset messages deleted ...>
QoS is disabled.
Console> (enable)
```

Related Commands

show qos info

set qos acl default-action

Use the **set qos acl default-action** command set to set the ACL default actions.

set qos acl default-action ip {**dscp** {*dscp*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*]

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*]

Syntax Description

ip	Keyword to specify the IP ACL default actions.
dscp *dscp*	Keyword and variable to set the DSCP to be associated with packets matching this stream.
trust-cos	Keyword to specify DSCP is derived from the packet CoS.
trust-ipprec	Keyword to specify DSCP is derived from the packet's IP precedence.
trust-dscp	Keyword to specify DSCP is contained in the packet already.
microflow *microflow_name*	(Optional) Keyword and variable to specify the name of the microflow policing rule to be applied to packets matching the ACE.
aggregate *aggregate_name*	(Optional) Keyword and variable to specify the name of the aggregate policing rule to be applied to packets matching the ACE.
ipx	Keyword to specify the IPX ACL default actions.
mac	Keyword to specify the MAC ACL default actions.

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.

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.

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

show qos acl info
clear qos acl

set qos acl ip

Use the **set qos acl ip** command set to create or add IP access lists.

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*]

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*] **igmp** {*src_ip_spec*} {*dest_ip_spec*} [*igmp_type*] [**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*]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
dscp *dscp*	Keyword and variable to set CoS and DSCP from configured DSCP values.
trust-cos	Keyword to specify DSCP is derived from the packet CoS.
trust-ipprec	Keyword to specify DSCP is derived from the packet's IP precedence.
trust-dscp	Keyword to specify DSCP is contained in the packet already.
microflow *microflow_name*	(Optional) Keyword and variable to specify the name of the microflow policing rule to be applied to packets matching the ACE.
aggregate *aggregate_name*	(Optional) Keyword and variable to specify 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.
before *editbuffer_index*	(Optional) Keyword and variable to insert the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Keyword and variable to replace 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.
precedence *precedence*	(Optional) Keyword and variable to specify the precedence level to compare with in 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) Keyword and variable to specify the DSCP field level to compare with an incoming packet. Valid values are from 0 to 7 or by name; valid names are critical, flash, flash-override, immediate, internet, network, priority, and routine.
icmp	Keyword to specify 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.
igmp	Keyword to specify IGMP.
igmp-type	(Optional) IGMP message type or message name; valid message type numbers are from 0 to 15. See the "Usage Guidelines" section for a list of valid names and numbers.
tcp	Keyword to specify 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—Keyword to specify an established connection.
udp	Keyword to specify UDP.

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 6000 Family Software Configuration Guide* for additional marking rule information.

The optional **microflow** *microflow_name*, **aggregate** *aggregate_name* keywords and variables are used to configure policing in the ACE. Refer to the *Catalyst 6000 Family 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, 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), **igmp** (2), **ip** (0), **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.

Valid names and corresponding numbers for *igmp_message* are dvmrp (3), host-query (1), host-report (2), pim (4), and trace (5).

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 IGMP 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*] **igmp** {*src_ip_spec*}
{*dest_ip_spec*} [*igmp_type*] [**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 microflow 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

show qos acl info
clear qos acl
rollback
commit

set qos acl ipx

Use the **set qos acl ipx** command set to define IPX access lists.

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*	Keyword and variable to set CoS and DSCP from configured DSCP values.
trust-cos	Keyword to specify that the DSCP is derived from the packet CoS.
aggregate *aggregate_name*	(Optional) Keyword and variable to specify 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 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) Keyword and variable to insert the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Keyword and variable to replace 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 6000 Family Software Configuration Guide* for additional marking rule information.

The optional **aggregate** *aggregate_name* keyword and variable are used to configure policing in the ACE. Refer to the *Catalyst 6000 Family 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

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

Use the **show security acl** command to display the list.

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

show qos acl info
clear qos acl
rollback
commit

set qos acl mac

Use the **set qos acl mac** command to define MAC access lists.

set qos acl mac {*acl_name*} {**dscp** *dscp* | **trust-cos**} [**aggregate** *aggregate_name*] {*src_mac_addr_spec*} {*dest_mac_addr_spec*} [*ether-type*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
dscp *dscp*	Keyword and variable to set CoS and DSCP from configured DSCP values.
trust-cos	Keyword to specify that the DSCP is derived from the packet CoS.
aggregate *aggregate_name*	(Optional) Keyword and variable to specify 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	(Optional) Number of the destination MAC address.
ether-type	(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.
before *editbuffer_index*	(Optional) Keyword and variable to insert the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Keyword and variable to replace 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 6000 Family Software Configuration Guide* for additional marking rule information.

The optional **aggregate** *aggregate_name* keyword and variable are used to configure policing in the ACE. Refer to the *Catalyst 6000 Family 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, 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 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.

Examples

This example shows how to create an Ethernet ACE:

```
Console> (enable) set qos acl ip my_MACacl trust-cos microflow my-micro aggregate my-agg
any any
my_IPXacl editbuffer modified. Use `commit' command to apply changes.
Console> (enable)
```

Related Commands

show qos acl info
clear qos acl
rollback
commit

set qos acl map

Use the **set qos acl map** command to attach an ACL to a specified port or VLAN.

set qos acl map *acl_name mod/port* | *vlan*

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.

Defaults

There are no default ACL mappings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Caution Use the **copy** command to save the ACL configuration to Flash memory.

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.
```

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)
```

Related Commands

show qos acl map
clear qos acl
rollback
commit

set qos bridged-microflow-policing

Use the **set qos bridged-microflow-policing** command to enable or disable microflow policing of bridged packets on a per-VLAN basis.

set qos bridged-microflow-policing {**enable** | **disable**} *vlanlist*

Syntax Description

enable	Keyword to activate microflow policing functionality.
disable	Keyword to deactivate microflow policing functionality.
vlanlist	List of VLANs; valid values are from 1 to 1000.

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-packet-policing

set qos cos-dscp-map

Use the **set qos cos-dscp map** command to set the CoS-to-DSCP mapping.

set qos cos-dscp-map *dscp1 dscp2... dscp8*

Syntax Description

dscp#	Number of the DSCP; valid values are from 0 to 63.

Defaults

The default CoS-to-DSCP configuration is listed in Table 2-12.

Table 2-12 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

Use the **set qos drop-threshold** command to program the transmit and receive drop thresholds on all ports in the system.

set qos drop-threshold 2q2t tx queue *q# thr1 thr2*

set qos drop-threshold {**1q4t** | **1p1q4t**} **rx queue** *q# thr1 thr2 thr3 thr4*

Syntax Description

2q2t tx	Keywords to specify the transmit drop threshold.
1q4t | **1p1q4t rx**	Keywords to specify the receive drop threshold.
queue *q#*	Keyword and variable to specify 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 drop thresholds:
  - queue 1—80%, 100%
  - queue 2—80%, 100%
- Receive 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 drop thresholds:
  - queue 1—100%, 100%
  - queue 2—100%, 100%
- Receive 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**, **1q4t**, or **1p1q4t**) determines the number of threshold values the hardware supports. For example, with **2q2t**, 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 **1q4t** and **1p1q4t**, the number of queues specified is four. 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 **1p1q4t** port types determines the threshold in the priority queue.

When you configure the drop threshold for **1q1q4t**, 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 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 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

Use the **set qos dscp-cos-map** command to set the DSCP-to-CoS mapping.

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 2-13.

Table 2-13 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

show qos maps
clear qos map

set qos ipprec-dscp-map

Use the **set qos ipprec-dscp-map** command to set the IP precedence-to-DSCP map. 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 2-14.

Table 2-14 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 **show qos maps**
clear qos ipprec-dscp-map

set qos mac-cos

Use the **set qos mac-cos** command to set the CoS value to the MAC address and VLAN pair.

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 1001.
cos	CoS value; valid values are from 0 to 7, higher numbers represent higher priority.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command has no effect on a switch configured with a PFC because the Layer 3 switching engine's result always overrides the Layer 2 result.

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

Use the **set qos map** command to map a specific CoS value to one of the transmit or receive priority queues and one of the thresholds per available priority queue for all ports.

set qos map *port_type* **tx** | **rx** *q# thr#* **cos** *coslist*

Syntax Description

port_type	Port type; valid values are **2q2t** and **1p2q2t** for transmit and **1p1q4t** for receive. The same mapping is used for both the receive and transmit directions.
tx	Keyword to specify the transmit queue.
rx	Keyword to specify 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*	Keyword and variable to specify 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 2-4 and Table 2-5.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

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.

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

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 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 1p2q2t tx 1 1 cos 1,2,5
Qos tx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

This example shows how to map the CoS value 7 to strict priority transmit queue 3/drop threshold 1:

```
Console> (enable) set qos map 1p2q2t tx 3 1 cos 7

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

Use the **set qos policed-dscp-map** command to set the mapping of policed in-profile DSCPs.

set qos policed-dscp-map *in_profile_dscp***:***policed_dscp*...

Syntax Description

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 a Layer 3 switching engine only.

Examples

This example shows how to set the mapping of policed in-profile DSCPs:

```
Console> (enable) set qos policed-dscp-map 60-63:60 20-40:5
QoS policed-dscp-map set successfully.
Console> (enable)
```

Related Commands

clear qos policed-dscp-map
show qos policer
show qos maps

set qos policer

Use the **set qos policer** command to create a policing rule for ACL.

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**

Syntax Description

microflow *microflow_name*	Keyword and variable to specify the name of the microflow policing rule.
rate *rate*	Keyword and variable to specify the average rate; valid values are from 0 and 32 Kbps to 8 Gbps.
burst *burst*	Keyword and variable to specify the burst size; valid values are from 1 Kb to 32 Mb.
drop	Keyword to specify drop traffic.
policed-dscp	Keyword to specify policed DSCP.
aggregate *aggregate_name*	Keyword and variable to specify the name of the aggregate policing rule.

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 6000 family 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 flowmask is bumped up to full flow.

Before aggregate policing can occur, you must create an aggregate and a policing rule for that aggregate. The Catalyst 6000 family switch supports up to 1023 aggregates and 1023 policing rules.

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 Kbps to 8 Gbps and the range for the burst size is 1 Kb (entered as 1) to 32 Mb (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-Kb minimum value burst size. Due to the nature of the traffic at different customer sites, coupled with the hardware granularity, 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.

Modifying an existing microflow or aggregate rate limit modifies that entry in NVRAM 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-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

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)
```

This example shows 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)
```

Related Commands

clear qos policer
show qos policer

set qos policy-source

Use the **set qos policy-source** command to set the QoS policy source.

set qos policy-source local | **cops**

Syntax Description

local	Keyword to set the policy source to local NVRAM configuration.
cops	Keyword to set 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.

When you set the policy source to COPS, all configuration that is global to the device, such as the DSCP to marked-down DSCP, is taken from policy downloaded to the PEP by the PDP. Configuration of each physical port, however, is taken from COPS 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:

```
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 and no COPS 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

set qos rsvp

Use the **set qos rsvp** command set to turn on or turn off the RSVP+ feature on the switch, set the time in minutes after which the RSVP+ databases get flushed (when the policy server dies), and set the local policy.

set qos rsvp enable | **disable**

set qos rsvp policy-timeout *timeout*

set qos rsvp local-policy forward | **reject**

Syntax Description

enable	Keyword to activate the RSVP+ feature.
disable	Keyword to deactivate the RSVP+ feature.
policy-timeout *timeout*	Keyword and variable to specify the time in minutes after which the RSVP+ databases get flushed; valid values are from 1 to 65535 minutes.
local-policy forward | **reject**	Keywords to specify 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 has been lost
- Old flows 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 txq-ratio

Use the **set qos txq-ratio** command to set the amount of packet buffer memory allocated to high-priority traffic and low-priority traffic.

set qos txq-ratio *port_type queue1_val queue2_val... queueN_val*

Syntax Description

port_type	Port type; valid values are **2q2t** and **1p2q2t**.
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

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. Since high-priority traffic is typically a smaller fraction of the traffic and since 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.

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

clear qos config
show qos info

set qos wred-threshold

Use the **set qos wred-threshold** command to configure the WRED threshold parameters for the specified port type.

set qos wred-threshold 1p2q2t tx queue *q# thr1 thr2*

Syntax Description

1p2q2t	Keyword to specify the port type; only valid value is **1p2q2t**.
tx	Keyword to specify the parameters for output queuing; only valid value is **tx**.
queue *q#*	Keyword and variable to specify the queue to which the arguments apply.
thr1 thr2	Percentage of the buffer size.

Defaults

The defaults are queue type is **tx**, threshold 1 is 80 percent, threshold 2 is 100 percent, and the low threshold is picked automatically by the system.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The queue number is 1 for the low-priority standard transmit queue and 2 for the high-priority standard transmit queue. The strict priority queue is not configurable; it uses threshold 2 as specified for queue 2.

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.

Examples

This example shows how to configure the low-priority transmit queue drop thresholds:

```
Console> (enable) set qos wred-threshold 1p2q2t tx queue 1 50 60
WRED thresholds for queue 1 set to 50%,60% on all WRED-capable 1p2q2t ports.
Console> (enable)
```

Related Commands

clear qos config
show qos info

set qos wrr

Use the **set qos wrr** command to specify the weights that determine how many packets will transmit out of one queue before switching to the other queue.

set qos wrr *port_type queue1_val queue2_val*

Syntax Description

port_type	Port type; valid values are **2q2t** and **1p2q2t**.
queue1_val *queue2_val*	Number of weights for queues 1 and 2; valid values are from 1 to 255.

Defaults

The default WRR 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**, only two queues can be set; the third queue is strict priority.

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)
```

Related Commands **show qos info**
show qos statistics

set radius deadtime

Use the **set radius deadtime** command to set the time to skip RADIUS servers that do not reply to an authentication request.

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 key

Use the **set radius key** command to set the encryption and authentication for all communication between the RADIUS client and the server.

set radius key *key*

Syntax Description

key	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

Use the **set radius retransmit** command to specify the number of times the RADIUS servers are tried before giving up on the server.

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 (three attempts).

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

show radius

set radius server

Use the **set radius server** command to set up the RADIUS server.

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) Keyword and variable to specify a destination UDP port for RADIUS authentication messages.
acct-port *port*	(Optional) Keyword and variable to specify a destination UDP port for RADIUS accounting messages.
primary	(Optional) Keyword to specify 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

Use the **set radius timeout** command to set the time between retransmissions to the RADIUS server.

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

set rcp username

Use the **set rcp username** command to specify your username for rcp file transfers.

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 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.

Examples

This example shows how to set the username for rcp:

```
Console> (enable) set rcp username jdoe
Console> (enable)
```

set rgmp

Use the **set rgmp** command to enable or disable the RGMP feature on the switch.

set rgmp {**enable** | **disable**}

Syntax Description

enable	Keyword to enable RGMP on the switch.
disable	Keyword to disable RGMP on the switch.

Defaults

The default is RGMP is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

RGMP is a global command. 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

show rgmp group
show rgmp statistics
clear rgmp statistics
set igmp

set rspan

Use the **set rspan** command set to create remote SPAN sessions.

set rspan disable source [*rspan_vlan* | **all**]

set rpsan disable destination [*mod/port* | **all**]

set rspan source {*src_mod/src_ports...* | *vlans...* | **sc0**} {*rspan_vlan*} [**rx** | **tx** | **both**] [**multicast** {**enable** | **disable**}] [**filter** *vlans...*] [**create**]

set rspan destination {*mod/port*} {*rspan_vlan*} [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}] [**create**]

Syntax Description

disable source	Keywords to disable remote SPAN source information.
rspan_vlan	(Optional) Remote SPAN VLAN.
all	(Optional) Keyword to disable all remote SPAN source or destination sessions.
disable destination	Keywords to disable 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	Keyword to specify the inband port is a valid source.
rx	(Optional) Keyword to specify that information received at the source (ingress SPAN) is monitored.
tx	(Optional) Keyword to specify that information transmitted from the source (egress SPAN) is monitored.
both	(Optional) Keyword to specify that information both transmitted from the source (ingress SPAN) and received (egress SPAN) at the source are monitored.
multicast enable	(Optional) Keywords to enable monitoring multicast traffic (egress traffic only).
multicast disable	(Optional) Keywords to disable monitoring multicast traffic (egress traffic only).
filter *vlans*	(Optional) Keywords to monitor traffic on selected VLANs on source trunk ports.
create	(Optional) Keyword to create a new remote SPAN session instead of overwriting the previous SPAN session.
inpkts enable	(Optional) Keywords to allow 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) Keywords to disable the receiving of normal inbound traffic on the remote SPAN destination port.
learning enable	(Optional) Keywords to enable learning for the remote SPAN destination port.
learning disable	(Optional) Keywords to disable 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 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.

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 capture-ports

Use the **set security acl capture-ports** command 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.

set security acl capture-ports {*mod/ports...*}

Syntax Description

mod/ports...	Module and port number.

Defaults

This command has no default setting.

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 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 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 ip

Use the **set security acl ip** command set to create a new entry in a standard IP VACL and append the new entry at the end of VACL.

set security acl ip {*acl_name*} {**permit** | **deny**} {*src_ip_spec*} [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** *mod_num/port_num*} {*protocol*} {s*rc_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**ip** | **0**] {s*rc_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**icmp** | **1**] {s*rc_ip_spec*} {*dest_ip_spec*} [*icmp_type*] [*icmp_code*] | [*icmp_message*] [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**igmp** | **2**] {s*rc_ip_spec*} {*dest_ip_spec*} [*igmp_type*] [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**tcp** | **6**] {s*rc_ip_spec*} [*operator port* [*port*]] {*dest_ip_spec*} [*operator port* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**udp** | **17**] {s*rc_ip_spec*} [*operator port* [*port*]] {*dest_ip_spec*} [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Syntax Description

acl_name	Unique name that identifies the lists to which the entry belongs.
permit	Keyword to allow traffic from the source IP address.
deny	Keyword to block 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) Keyword and variable to insert the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Keyword and variable to replace an ACE with the new ACE.
redirect	Keyword to specify to which switched ports the packet is redirected.
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) Keyword and variable to specify 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) Keyword and variable to specify 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.
capture	(Optional) Keyword to specify packets are switched normally and captured; **permit** must also be enabled.
ip | **0**	(Optional) Keyword or number to match any Internet Protocol packets.
icmp | **1**	(Optional) Keyword or number to match 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.
igmp | **2**	(Optional) Keyword or number to match IGMP packets.
igmp-type	(Optional) IGMP message type or message name; valid message type numbers are from 0 to 15. See the "Usage Guidelines" section for a list of valid names and corresponding numbers.
tcp | **6**	(Optional) Keyword or number to match 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) Keyword to specify an established connection; used only for TCP protocol.
udp | **17**	(Optional) Keyword or number to match UDP packets.

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 them in NVRAM and in the hardware.

If you use the **redirect** keyword, the destination must be 255.255.255.255.

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

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.

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), **igmp** (2), **ip** (0), **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.

Valid names and corresponding numbers for *igmp_message* are dvmrp (3), host-query (1), host-report (2), pim (4), and trace (5).

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** | **0**] {*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 IGMP, you can use the following syntax:

set security acl ip {*acl_name*} {**permit** | **deny** | **redirect** {*mod_num/port_num*}} [**igmp** | **2**] {*src_ip_spec*} {*dest_ip_spec*} [*igmp_type*] [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

For TCP, you can use 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 use 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*]

Examples

These examples show different ways to use the **set security acl ip** commands to configure IP security ACL:

```
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.
```

Related Commands

clear security acl
clear security acl capture-ports
clear security acl map
commit
show security acl
show security acl capture-ports
set security acl map
set security acl capture-ports

set security acl ipx

Use **the set security acl ipx** command to create a new entry in a standard IPX VACL and to append the new entry at the end of the VACL.

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	Keyword to allow traffic from the specified source IPX address.
deny	Keyword to block traffic from the specified source IPX address.
redirect	Keyword to redirect 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 amd 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) Keyword to specify packets are switched normally and captured.
before *editbuffer_index*	(Optional) Keyword and variable to insert the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Keyword and variable to replace 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 IP address:

```
Console> (enable) set security acl ipx IPXACL1 deny 1.a
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
show security acl
show security acl capture-ports
set security acl map
set security acl capture-ports

set security acl mac

Use the **set security acl mac** command 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.

set security acl mac {*acl_name*} {**permit** | **deny**} {*src_mac_addr_spec*} {*dest_mac_addr_spec*} [*ether-type*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
permit	Keyword to allow traffic from the specified source MAC address.
deny	Keyword to block 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.
ether-type	(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.
capture	(Optional) Keyword to specify packets are switched normally and captured.
before *editbuffer_index*	(Optional) Keyword and variable to insert the new ACE in front of another ACE.
modify *editbuffer_index*	(Optional) Keyword and variable to replace 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

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 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), and xerox-address-translation (0x0601).

Use the **show security acl** command to display the list.

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
show security acl
show security acl capture-ports
set security acl map
set security acl capture-ports

set security acl map

Use the **set security acl map** command to map an existing VACL to a VLAN.

set security acl map *acl_name vlan*

Syntax Description

acl_name	Unique name that identifies the list to which the entry belongs.
vlan	Number of the VLAN to be mapped to the VACL.

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 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.

Examples

This example shows how to map an existing VACL 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)
```

Related Commands

clear security acl
clear security acl map
commit
show security acl

set snmp access

Use the **set snmp access** command set to define the access rights of an SNMP group with a specific security model in different security levels.

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*}] [**volatile | nonvolatile**]

Syntax Description

-hex	(Optional) Keyword to display the *groupname*, *readview*, *writeview*, and *notifyview* in a hexadecimal format.
groupname	Name of the SNMP group.
security-model v1 | v2c	Keywords to specify security-model v1 or v2c.
read *readview*	(Optional) Keyword and variable to specify the name of the view that allows you to see the MIB objects.
write *writeview*	(Optional) Keyword and variable to specify the name of the view that allows you to configure the contents of the agent.
notify *notifyview*	(Optional) Keyword and variable to specify the name of the view that allows you to send a trap about MIB objects.
v3	Keyword to specify security model v3.
noauthentication	Keyword to specify security model is not set to use authentication protocol.
authentication	Keyword to specify the type of authentication protocol.
privacy	Keyword to specify that the messages sent on behalf of the user are protected from disclosure.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify 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 **nonvolatile**.
- **read** *readview* is Internet OID space.
- **write** *writeview* is NULL OID.
- **notify** *notifyview* is NULL OID.

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).

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

set snmp community

Use the **set snmp community** command to set SNMP communities and associated access types.

set snmp community {**read-only** | **read-write** | **read-write-all**} [*community_string*]

Syntax Description

read-only	Keyword to assign read-only access to the specified SNMP community.
read-write	Keyword to assign read-write access to the specified SNMP community.
read-write-all	Keyword to assign read-write access to the specified SNMP community.
community_string	(Optional) Name of the SNMP community.

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.

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.

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
show snmp

set snmp extendedrmon netflow

Use the **set snmp extendedrmon netflow** command to enable or disable the SNMP extended RMON support for the NAM.

set snmp extendedrmon netflow {**enable** | **disable**} {*mod*}

Syntax Description

enable	Keyword to enable the extended RMON support.
disable	Keyword to disable 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

Use the **set snmp group** command to establish the relationship between an SNMP group and a user with a specific security model.

set snmp group [**-hex**] {*groupname*} **user** [**-hex**] {*username*}
{**security-model** {**v1** | **v2c** | **v3**}} [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Keyword to display 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	Keyword to specify the SNMP group user name.
username	Name of the SNMP user that belongs to the SNMP group; the maximum length is 32 bytes.
security-model v1 | **v2c** | **v3**	Keywords to specify security-model v1, v2c, or v3.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify 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 notify

Use the **set snmp notify** command to set the notifyname entry in the snmpNotifyTable and the notifytag entry in the snmpTargetAddrTable.

set snmp notify [**-hex**] {*notifyname*} **tag** [**-hex**] {*notifytag*}
[**trap** | **inform**] [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Keyword to display the notifyname and notifytag in a hexadecimal format.
notifyname	Identifier to index the snmpNotifyTable.
tag	Keyword to specify the tag name in the taglist.
notifytag	Name of entries in the snmpTargetAddrTable.
trap	(Optional) Keyword to specify all messages that contain snmpv2-Trap PDUs.
inform	(Optional) Keyword to specify all messages that contain InfoRequest PDUs.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify 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**.
- 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

Use the **set snmp rmon** command to enable or disable SNMP RMON support.

set snmp rmon {**enable** | **disable**}

Syntax Description

enable	Keyword to activate SNMP RMON support.
disable	Keyword to deactivate 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 targetaddr

Use the **set snmp targetaddr** command to configure the SNMP target address entries in the snmpTargetAddressTable.

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) Keyword to display *addrname, paramsname, tagvalue*, and *tag* in a hexadecimal format.
addrname	Unique identifier to index the snmpTargetAddrTable; the maximum length is 32 bytes.
param	Keyword to specify 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) Keyword and variable to specify which UDP port of the target host to use.
timeout *value*	(Optional) Keyword and variable to specify the number of timeouts.
retries *value*	(Optional) Keyword and variable to specify the number of retries.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify 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) Keyword and variable to specify a tag name in the taglist.
tag *tagvalue*	(Optional) Keyword and variable to specify 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

Use the **set snmp targetparams** command set to configure the SNMP parameters used in the snmpTargetParamsTable when generating a message to a target.

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) Keyword to display the *paramsname* and *username* in a hexadecimal format.
paramsname	Name of the parameter in the snmpTargetParamsTable; the maximum length is 32 bytes.
user	Keyword to specify 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**	Keywords to specify security-model v1 or v2c.
message-processing v1 | **v2c** | **v3**	Keywords to specify the version number used by the message processing model.
security-model v3	Keyword to specify security-model v3.
message-processing v3	Keywords to specify v3 is used by the message-processing model.
noauthentication	Keyword to specify security model is not set to use authentication protocol.
authentication	Keyword to specify the type of authentication protocol.
privacy	Keyword to specify the messages sent on behalf of the user are protected from disclosure.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify 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

set snmp trap

Use the **set snmp trap** command set to enable or disable the different SNMP traps on the system or to add an entry into the SNMP authentication trap receiver table.

set snmp trap {**enable** | **disable**} [**all** | **auth** | **bridge** | **chassis** | **config** | **entity** | **ippermit** | **module** | **repeater** | **stpx** | **syslog** | **vmps** | **vtp**]

set snmp trap *rcvr_addr rcvr_community*

Syntax Description

enable	Keyword to enable SNMP traps.
disable	Keyword to disable SNMP traps.
all	(Optional) Keyword to specify all trap types and all port traps. See the "Usage Guidelines" section before using this option.
auth	(Optional) Keyword to specify the authenticationFailure trap from RFC 1157.
bridge	(Optional) Keyword to specify the newRoot and topologyChange traps from RFC 1493 (the BRIDGE-MIB).
chassis	(Optional) Keyword to specify the chassisAlarmOn and chassisAlarmOff traps from the CISCO-STACK-MIB.
config	(Optional) Keyword to specify the sysConfigChange trap from the CISCO-STACK-MIB.
entity	(Optional) Keyword to specify the entityMIB trap from the ENTITY-MIB.
ippermit	(Optional) Keyword to specify the IP Permit Denied access from the CISCO-STACK-MIB.
module	(Optional) Keyword to specify the moduleUp and moduleDown traps from the CISCO-STACK-MIB.
repeater	(Optional) Keyword to specify the rptrHealth, rptrGroupChange, and rptrResetEvent traps from RFC 1516 (the SNMP-REPEATER-MIB).
stpx	(Optional) Keyword to specify the STPX trap.
syslog	(Optional) Keyword to specify the syslog notification traps.
vmps	(Optional) Keyword to specify the vmVmpsChange trap from the CISCO-VLAN-MEMBERSHIP-MIB.
vtp	(Optional) Keyword to specify 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.

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.

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 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)
```

Related Commands

show snmp
test snmp trap
clear snmp trap
set port trap

set snmp user

Use the **set snmp user** command to configure a new SNMP user.

set snmp user [**-hex**] {*username*} {**remote** {*engineid*}}
[**authentication** {**md5** | **sha** | *authpassword*}] [**privacy** {*privpassword*}]
[**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Keyword to display *username* in a hexadecimal format.
username	Name of the SNMP user.
remote *engineid*	Keyword and variable to specify the remote SNMP engine ID.
authentication	(Optional) Keyword to specify the authentication protocol.
md5	Keyword to specify HMAC-MD5-96 authentication protocol.
sha	Keyword to specify HMAC-SHA-96 authentication protocol.
authpassword	Password for authentication.
privacy *privpassword*	(Optional) Keyword and variable to enable the host to encrypt the contents of the message sent to or from the agent; the maximum length is 32 bytes.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify 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.

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.

authpassword and *privpassword* 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

set snmp view

Use the **set snmp view** command to configure the SNMP MIB view.

set snmp view [**-hex**]{*viewname*}{*subtree*}[**mask**] [**included** | **excluded**] [**volatile** | **nonvolatile**]

Syntax Description

-hex	(Optional) Keyword to display the *viewname* in a hexadecimal format.
viewname	Name of a MIB view.
subtree	MIB subtree.
mask	(Optional) Keyword to specify 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) Keywords to specify that the MIB subtree is included or excluded.
volatile	(Optional) Keyword to specify that the storage type is defined as temporary memory and the content is deleted if the device is turned off.
nonvolatile	(Optional) Keyword to specify 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 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

set span

Use the **set span** command set to configure and display SPAN.

set span disable [*dest_mod/dest_port* | **all**]

set span {*src_mod/src_ports* | *src_vlans* | **sc0**} {*dest_mod/dest_port*} [**rx** | **tx** | **both**] [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}] [**multicast** {**enable** | **disable**}] [**filter** *vlans*...] [**create**]

Syntax Description

disable	Keyword to disable SPAN.
dest_mod	(Optional) Monitoring module (SPAN destination).
dest_port	(Optional) Monitoring port (SPAN destination).
all	(Optional) Keyword to disable all SPAN sessions.
src_mod	Monitored module (SPAN source).
src_ports	Monitored ports (SPAN source).
src_vlans	Monitored VLANs (SPAN source).
sc0	Keyword to specify the inband port is a valid source.
rx	(Optional) Keyword to specify that information received at the source (ingress SPAN) is monitored.
tx	(Optional) Keyword to specify that information transmitted from the source (egress SPAN) is monitored.
both	(Optional) Keyword to specify that information both transmitted from the source (ingress SPAN) and received (egress SPAN) at the source are monitored.
inpkts enable	(Optional) Keywords to enable the receiving of normal inbound traffic on the SPAN destination port.
inpkts disable	(Optional) Keywords to disable the receiving of normal inbound traffic on the SPAN destination port.
learning enable	(Optional) Keywords to enable learning for the SPAN destination port.
learning disable	(Optional) Keywords to disable learning for the SPAN destination port.
multicast enable	(Optional) Keywords to enable monitoring multicast traffic (egress traffic only).
multicast disable	(Optional) Keywords to disable monitoring multicast traffic (egress traffic only).
filter *vlans*	(Optional) Keyword and variable to monitor traffic on selected VLANs on source trunk ports.
create	(Optional) Keyword to create a SPAN port.

Defaults

The default is SPAN is disabled, no VLAN filtering is enabled, multicast is enabled, input packets are disabled, and learning is enabled.

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.

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 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

Use the **set spantree backbonefast** command to enable or disable the spanning tree Backbone Fast Convergence feature.

set spantree backbonefast {**enable** | **disable**}

Syntax Description

enable	Keyword to enable Backbone Fast Convergence.
disable	Keyword to disable Backbone Fast Convergence.

Defaults

The default is Backbone Fast Convergence is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

For Backbone Fast Convergence to work, you must enable it on all switches in the network.

Examples

This example shows how to enable Backbone Fast Convergence:

```
Console> (enable) set spantree backbonefast enable
Backbonefast enabled for all VLANs.
Console> (enable)
```

Related Commands

show spantree

set spantree disable

Use the **set spantree disable** command to disable the spanning tree algorithm for all VLANs or a specific VLAN.

set spantree disable [*vlan* | **all**]

Syntax Description

vlan	(Optional) Number of the VLAN.
all	(Optional) Keyword to specify all VLANs.

Defaults

The default is spanning tree is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to disable the spanning tree algorithm for VLAN 1:

```
Console> (enable) set spantree disable 1
VLAN 1 bridge spanning tree disabled.
Console> (enable)
```

Related Commands

set spantree enable
show spantree

set spantree enable

Use the **set spantree enable** command to enable the spanning tree algorithm for all VLANs or a specific VLAN.

set spantree enable [*vlan* | **all**]

Syntax Description

vlan	(Optional) Number of the VLAN.
all	(Optional) Keyword to specify all VLANs.

Defaults

The default is spanning tree is enabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Examples

This example shows how to activate the spanning tree algorithm for VLAN 1:

```
Console> (enable) set spantree enable 1
VLAN 1 bridge spanning tree enabled.
Console> (enable)
```

Related Commands

set spantree disable
show spantree

set spantree fwddelay

Use the **set spantree fwddelay** command to set the bridge forward delay for a VLAN.

set spantree fwddelay *delay* [*vlan*]

Syntax Description

delay	Number of seconds for the bridge forward delay; valid values are from 4 to 30 seconds.
vlan	(Optional) Number of the VLAN.

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, VLAN 1 is assumed.

Usage Guidelines

This command is not supported by the NAM.

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)
```

Related Commands

show spantree

set spantree hello

Use the **set spantree hello** command to set the bridge hello time for a VLAN.

set spantree hello *interval* [*vlan*]

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.
vlan	(Optional) Number of the VLAN.

Defaults

The default is 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, VLAN 1 is assumed.

Usage Guidelines

This command is not supported by the NAM.

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)
```

Related Commands

show spantree

set spantree maxage

Use the **set spantree maxage** command to set the bridge maximum aging time for a VLAN.

set spantree maxage *agingtime* [*vlan*]

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.
vlan	(Optional) Number of the VLAN.

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, VLAN 1 is assumed.

Usage Guidelines

This command is not supported by the NAM.

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)
```

Related Commands

show spantree

set spantree portcost

Use the **set spantree portcost** command to set the path cost for a port.

set spantree portcost {*mod/port*} *cost*

Syntax Description

mod/port	Number of the module and the port on the module.
cost	Number of the path cost; valid values are from 0 to 65535, where 0 is low cost and 65535 is high cost.

Defaults

The default is portcost is 4.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

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.

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

show spantree

set spantree portfast

Use the **set spantree portfast** command to allow a port that is connected to a single workstation or PC to start faster when it is connected.

set spantree portfast {*mod/port*} {**enable** | **disable**}

Syntax Description

mod/port	Number of the module and the port on the module.
enable	Keyword to enable the spanning tree port fast-start feature on the port.
disable	Keyword to disable the spanning tree port fast-start feature on the port.

Defaults

The default is the port fast-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. Use this command on ports that are connected to a single workstation or PC only; do not use it on ports that are connected to networking devices such as hubs, routers, switches, bridges, or concentrators.

Examples

This example shows how to enable the spanning tree port fast-start feature on port 2 on module 1:

```
Console> (enable) set spantree portfast 1/2 enable

Warning: Spantree 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 port 1/2 fast start enabled.
Console> (enable)
```

Related Commands

show spantree

set spantree portfast bpdu-guard

Use the **set spantree portfast bpdu-guard** command to enable or disable BPDU guard on the switch.

set spantree portfast bpdu-guard {**enable** | **disable**}

Syntax Description

enable	Keyword to enable the spanning tree PortFast BPDU guard.
disable	Keyword to disable the spanning tree PortFast BPDU guard.

Defaults

The default is PortFast BPDU guard is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

When you enable 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 a PortFast BPDU guard, a PortFast enabled nontrunking port will stay up when it receives BPDUs, which may cause spanning tree loops.

Examples

This example shows how to enable the spanning tree PortFast BPDU guard:

```
Console> (enable) set spantree portfast bpdu-guard enable
Spantree portfast bpdu-guard enabled on this switch.
Console> (enable)
```

This example shows how to disable the spanning tree PortFast BPDU guard:

```
Console> (enable) set spantree portfast bpdu-guard disable
Spantree portfast bpdu-guard disabled on this switch.
Console> (enable)
```

Related Commands

show spantree summary

set spantree portpri

Use the **set spantree portpri** command to set the bridge priority for a spanning tree port or TrCRF.

set spantree portpri {*mod/port*} | **trcrf** [*priority* | *trcrf_priority*]

Syntax Description

mod/port	Number of the module and the port on the module.
trcrf	Keyword to specify the number of the TrCRF for which you are setting the bridge priority.
priority	(Optional) Number that represents the cost of a link in a spanning tree bridge; valid values are from 0 to 63, with 0 indicating high priority and 63, low priority.
trcrf_priority	(Optional) Number that represents the cost of the TrCRF; valid values are from 0 to 7, with 0 indicating high priority and 7, low priority.

Defaults

The default is all ports with bridge priority are set to 32.

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 priority of port 1 on module 4 to 63:

```
Console> (enable) set spantree portpri 4/1 63
Bridge port 4/1 priority set to 63.
Console> (enable)
```

Related Commands

show spantree

set spantree portstate

Use the **set spantree portstate** command to set the state of a TrCRF manually.

set spantree portstate *trcrf* {**block** | **forward** | **auto**} [*trbrf*]

Syntax Description

trcrf	Number of the TrCRF for which you are manually setting the state.
block | **forward** | **auto**	Keywords to set the TrCRF to a blocked state (**block**), forwarding state (**forward**), or to have the Spanning Tree Protocol determine the correct state automatically (**auto**).
trbrf	(Optional) Number of the parent TrBRF.

Defaults

There is no default configuration for this command.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

Use this command only to set the port state when the TrCRF is in SRT mode and the TrBRF is running the IBM Spanning Tree Protocol, or the TrCRF is in SRB mode and the TrBRF is running the IEEE Spanning Tree Protocol.

When you enable Spanning Tree Protocol, every switch in the network goes through the blocking state and the transitory states of listening and learning at power up. If properly configured, the ports then stabilize to the forwarding or blocking state. However, with TrBRFs and TrCRFs, there are two exceptions to this rule that require you to set the state of the logical ports of a TrBRF manually:

- The TrBRF is running the IBM Spanning Tree Protocol, and the TrCRF is in SRT mode.
- The TrBRF is running the IEEE Spanning Tree Protocol, and the TrCRF is in SRB mode.

If either condition exists, use the **set spantree portstate** command to set the state of a TrCRF manually to blocked or forwarding mode or set the Spanning Tree Protocol to determine the correct state automatically.

Examples

This example shows the manual setting of TrCRF 900 to a forwarding state:

```
Console> (enable) set spantree portstate 900 forward
reserve_nvram : requested by block = 0
reserve_nvram : granted to block = 0
release_nvram : releasing block = 0
Console> (enable)
```

Related Commands

show spantree

set spantree portvlancost

Use the **set spantree portvlancost** command to assign a lower path cost to a set of VLANs on a port.

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) Keyword to indicate the path cost. The portvlancost applies only to trunk ports.
vlan_list	(Optional) If you do not list a VLAN explicitly, the VLANs listed in prior invocations of this command are affected. If no cost is listed explicitly, and previous cost values are specified in prior invocations, then the portvlancost is set to 1 less than the current port cost for a port. However, this may not assure load balancing in all cases.

Defaults

The default is portvlancost is 3.

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 in MISTP mode.

Examples

These examples show various ways to use the **set spantree portvlancost** command:

```
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 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 cost:

```
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

show spantree

set spantree portvlanpri

Use the **set spantree portvlanpri** command to set the port priority for a subset of VLANs in the trunk port.

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. The priority level is from 0 to 63, with 0 indicating high priority and 63 indicating low priority.
vlans	(Optional) VLANs that use the specified priority level.

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

This command is not supported by the NAM.

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 portvlancost
show spantree

set spantree priority

Use the **set spantree priority** command to set the bridge priority for a VLAN.

set spantree priority *bridge_priority* [*vlan*]

Syntax Description

bridge_priority	Number representing the priority of the bridge. The priority level is from 0 to 65535, with 0 indicating high priority and 65535, low priority.
vlan	(Optional) Number of the VLAN. If you do not specify a VLAN number, VLAN 1 is used.

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.

This feature is not supported for the MSM.

Examples

This example shows how to set the bridge priority of VLAN 1 to 4096:

```
Console> (enable) set spantree priority 4096
VLAN 1 bridge priority set to 4096.
Console> (enable)
```

Related Commands

show spantree

set spantree root

Use the **set spantree root** command to set the primary or secondary root for specific VLANs or for all VLANs of the switch.

set spantree root [**secondary**] [*vlan_list*] [**dia** *network_diameter*] [**hello** *hello_time*]

Syntax Description

secondary	(Optional) Keyword to designate this switch as a secondary root, should the primary root fail.
vlan_list	(Optional) Number of the VLAN.
dia *network_diameter*	(Optional) Keyword to specify the maximum number of bridges between any two points of attachment of end stations; valid values are from 1 through 7.
hello *hello_time*	(Optional) Keyword to specify in seconds, the duration between the generation of configuration messages by the root switch.

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*, the current value of *hello_time* from the NVRAM is used.

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 secondary command reduces the bridge priority value to 16384.

This command increases path costs to a value greater than 3000.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to use the **set spantree root** command:

```
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)
```

These examples show that setting the bridge priority to 8192 was not sufficient to make this switch the root. So, 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

Use the **set spantree uplinkfast** command to enable fast switchover to alternate ports when the root port fails. 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	Keyword to enable fast switchover.
disable	Keyword to disable fast switchover.
rate	(Optional) Keyword to specify the number of multicast packets transmitted per 100 ms when an alternate port is chosen after the root port goes down.
station_update_rate	(Optional) Number of multicast packets transmitted per 100 ms when an alternate port is chosen after the root port goes down.
all-protocols	(Optional) Keyword to specify whether or not to generate multicast packets for all protocols (IP, IPX, AppleTalk, and Layer 2 packets).
off	(Optional) Keyword to turn off the all-protocols feature.
on	(Optional) Keyword to turn on the all-protocols feature.

Defaults

The default *station_update_rate* is 15 packets per 100 ms.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

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 **set spantree uplinkfast enable** 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 **set spantree uplinkfast disable** on a switch, the UplinkFast feature is disabled but the switch priority and port cost values are not reset to the factory-set defaults. To reset the values to the factory-set defaults, enter the **clear spantree uplinkfast** command.

The default *station_update_rate* value is 15 packets per 100 ms, which is equivalent to a 1 percent load on a 10-Mbps Ethernet. 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 6000 family switches that have both the UplinkFast and protocol filtering features enabled. Use the all-protocols feature only on Catalyst 6000 family 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 ms:

```
Console> (enable) set spantree uplinkfast enable rate 40
VLANs 1-1000 bridge priority set to 49152.
The port cost and portvlancost of all ports increased to above 3000.
Station update rate set to 40 packets/100ms.
uplinkfast turned on 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 already 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)
```

Related Commands

show spantree

set summertime

Use the **set summertime** command to specify whether the system should set the clock ahead one hour during daylight saving time.

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	Keyword to cause the system to set the clock ahead one hour during daylight saving time.
disable	Keyword to prevent the system from setting the clock ahead one hour during daylight saving time.
zone	(Optional) Time zone used by the **set summertime** command.
recurring	Keyword to specify the summertime dates which recur every year.
week	Week of the month (first, second, third, fourth, last, 1...5).
day	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	Day of the month (1 to 31).
year	Number of the year (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

Use the **set system baud** command to set the console port baud rate.

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

set system contact

Use the **set system contact** command to identify a contact person for the system.

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 countrycode

Use the **set system countrycode** command to specify the country where the system is physically located.

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 2-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)
```

set system highavailability

Use the **set system highavailability** command to enable or disable high system availability for the switch.

set system highavailability enable | **disable**

Syntax Description

enable	Keyword to activate system high availability.
disable	Keyword to deactivate system high availability.

Defaults

The default is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

High availability provides Layer 2 to Layer 3 protocol redundancy.

If you enable high availability while the standby 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 standby supervisor engine after switchover.

If you disable high availability from the enabled state, synchronization from the active supervisor engine is stopped. On the standby supervisor engine, current synchronization data is discarded. If you enable high availability from the disabled state, synchronization from the active to standby supervisor engines starts (if you have a standby supervisor engine and the standby supervisor engine image version is compatible).

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

Use the **set system highavailability versioning** command to enable and disable support for supervisor engine image versioning.

set system highavailability versioning enable | **disable**

Syntax Description

enable	Keyword to activate system high availability versioning.
disable	Keyword to deactivate 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 6000 family switch to run different images on the active and standby supervisor engines. When you enable image versioning, Flash image synchronization (from active to the standby supervisor engines) does not occur, allowing active and standby supervisor engines to run different images.

Caution When you disable image versioning, the active and standby 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 standby supervisor engine (the standby supervisor engine should be running the same image as the active supervisor engine). If you want to load a different images, you have to restart the standby supervisor engine.

If you enable the image versioning option from the disabled state, and you have a standby supervisor engine and active supervisor engine running different images, Flash synchronization will copy the active supervisor engine image to the standby supervisor engine image and then restart it.

If you enable the image versioning option on the active supervisor engine, and the standby 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 location

Use the **set system location** command to identify the location of the system.

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 setting.

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

Use the **set system modem** command to enable or disable modem control lines on the console port.

set system modem {**enable** | **disable**}

Syntax Description

enable	Keyword to activate modem control lines on the console port.
disable	Keyword to deactivate 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

set system name

Use the **set system name** command to configure a name for the system.

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

show system
set prompt

set tacacs attempts

Use the **set tacacs attempts** command to configure the maximum number of login attempts allowed to the TACACS+ server.

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

Use the **set tacacs directedrequest** command to enable or disable the TACACS+ directed-request option. 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	Keyword to send the portion of the address before the @ sign (the username) to the host specified after the @ sign.
disable	Keyword to send 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 6000 family 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

Use the **set tacacs key** command to set the key for TACACS+ authentication and encryption.

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.

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

Use the **set tacacs server** command to define a TACACS+ server.

set tacacs server *ip_addr* [**primary**]

Syntax Description

ip_addr	IP address of the server on which the TACACS+ server resides.
primary	(Optional) Keyword to designate the specified server as the primary TACACS+ server.

Defaults

This command has no default setting.

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

Use the **set tacacs timeout** command to set the response timeout interval for the TACACS+ server daemon. 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 diaglevel

Use the **set test diaglevel** command to set the diagnostic level.

set test diaglevel {**complete** | **minimal** | **bypass**}

Syntax Description

complete	Keyword to specify complete diagnostics.
minimal	Keyword to specify minimal diagnostics.
bypass	Keyword to specify bypass diagnostics.

Defaults

The default is minimal diagnostics. 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**.

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

set time

Use the **set time** command to change the time of day on the system clock.

set time [*day_of_week*] [*mm/dd/yy*] [*hh:mm:ss*]

Syntax Description

day_of_week	(Optional) Day of the week.
mm/dd/yy	(Optional) Month, day, and year.
hh:mm:ss	(Optional) Current time in 24-hour format.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to set the system clock to Saturday, October 31, 1998, 7:50 a.m:

```
Console> (enable) set time sat 10/31/98 7:50
Sat Oct 31 1998, 07:50:00
Console> (enable)
```

Related Commands

show time

set timezone

Use the **set timezone** command to set the time zone for the system.

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 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 6000 family 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 trunk

Use the **set trunk** command to configure trunk ports and to add VLANs to the allowed VLAN list for existing trunks.

set trunk *mod/port* {**on** | **off** | **desirable** | **auto** | **nonegotiate**}[*vlans*] [**isl** | **dot1q** | **negotiate**]

Syntax Description

mod/port	Number of the module and the port on the module.
on	Keyword to force 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	Keyword to force 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	Keyword to cause the port to negotiate actively with the neighboring port to become a trunk link.
auto	Keyword to cause the port to become a trunk port if the neighboring port tries to negotiate a trunk link. This is the default mode for EtherChannel ports.
nonegotiate	Keyword to force the port to become a trunk port but prevent it from sending DTP frames to its neighbor.
isl	(Optional) Keyword to specify an ISL trunk on a Fast or Gigabit Ethernet port.
dot1q	(Optional) Keyword to specify an IEEE 802.1Q trunk on a Fast or Gigabit Ethernet port.
negotiate	(Optional) Keyword to specify that the port become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring port.
vlans	(Optional) VLANs to add to the list of allowed VLANs on the trunk; valid values are from 1 to 1000 and 1025 to 4094.

Defaults

The default port mode is 802.1Q-Native.

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 6000 Family Module Installation Guide* to determine the trunking capabilities of your hardware, or enter the **show port capabilities** command.
- The Catalyst 6000 family switches use the DTP to negotiate trunk links automatically on EtherChannel ports. Whether 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 6000 Family 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 6000 family 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.
- 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.
- 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.

The following configuration guidelines and restrictions apply when using 802.1Q trunks impose some limitations on the trunking strategy for a network. Note these restrictions when using 802.1Q trunks:

- When connecting Cisco switches through an 802.1q trunk, make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning tree loops might result.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every VLAN in the network. Make sure your network is free of physical loops before disabling spanning tree.
- When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning-tree BPDUs on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Cisco Shared Spanning Tree (SSTP) multicast MAC address (01-00-0c-cc-cc-cd).
- Non-Cisco 802.1Q switches maintain only a single instance of spanning tree (the Mono Spanning Tree, or MST) that defines the spanning-tree topology for all VLANs. When you connect a Cisco switch to a non-Cisco switch through an 802.1Q trunk, the MST of the non-Cisco switch and the native VLAN spanning-tree of the Cisco switch combine to form a single spanning-tree topology known as the Common Spanning Tree (CST).
- Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on VLANs other than the native VLAN of the trunk, non-Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Other Cisco switches connected to the non-Cisco 802.1q cloud receive these flooded BPDUs. This allows Cisco switches to maintain a

per-VLAN spanning tree topology across a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single broadcast segment between all switches connected to the non-Cisco 802.1q cloud through 802.1q trunks.

- Make certain that the native VLAN is the same on ALL of the 802.1q trunks connecting the Cisco switches to the non-Cisco 802.1q cloud.
- If you are connecting multiple Cisco switches to a non-Cisco 802.1q cloud, all of the connections *must* be through 802.1q trunks. You *cannot* connect Cisco switches to a non-Cisco 802.1q cloud through ISL trunks or through access ports. Doing so will cause the switch to place the ISL trunk port or access port into the spanning tree "port inconsistent" state and no traffic will pass through the port.

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)
```

Related Commands

clear trunk
set vtp
show trunk
show vtp statistics

set udld

Use the **set udld** command to enable or disable the UDLD information display on specified ports or globally on all ports.

set udld enable | **disable** [*mod/port*]

Syntax Description

enable	Keyword to enable the UDLD information display.
disable	Keyword to disable 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 1000BaseTX ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

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

Use the **set udld aggressive-mode** command to enable or disable the UDLD aggressive mode on specified ports or globally on all ports.

set udld aggressive-mode enable | **disable** *mod/port*

Syntax Description

enable	Keyword to enable UDLD aggressive mode.
disable	Keyword to disable 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

set udld interval

Use the **set udld** command to set the UDLD message interval timer.

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

Use the **set vlan** command set to group ports into a VLAN or set the private VLAN type.

set vlan {*vlan_num*}{*mod/ports*}

set vlan {*vlan_num*} [**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*}] [**ring** {*hex_ring_numbe*r}] [**decring** {*decimal_ring_number*}] [**parent** {*vlan_num*}] [**backupcrf** {**off** | **on**}] [**stemaxhop** {*hopcount*}] [**rspan**]

Syntax Description

vlan_num	Number identifying the VLAN.
mod/ports	Number of the module and ports on the module belonging to the VLAN.
name *name*	(Optional) Keyword and variable to define a text string used as the name of the VLAN; valid values are from 1 to 32 characters.
type *type*	(Optional) Keyword and variable to identify the VLAN type.
state *state*	(Optional) Keyword and variable to specify whether the state of the VLAN is active or suspended.
said *said*	(Optional) Keyword and variable to specify the security association identifier; valid values are from 1 to 4294967294.
mtu *mtu*	(Optional) Keyword and variable to specify the maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from 576 to 18190.
bridge *bridge_num*	(Optional) Keyword and variable to specify the identification number of the bridge; valid values are hexadecimal numbers from 0x1 to 0xF.
mode *bridge_mode*	(Optional) Keyword and variable to specify the bridge mode; valid values are **srt** and **srb**.
stp *stp_type*	(Optional) Keyword and variable to specify the STP type; valid values are **ieee**, **ibm**, and **auto**.
translation *vlan_num*	(Optional) Keyword and variable to specify a translational VLAN used to translate FDDI or Token Ring to Ethernet; valid values are from 1 to 1005.
aremaxhop *hopcount*	(Optional) Keyword and variable to specify 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.
ring *hex_ring_number*	(Optional) Keyword to specify the VLAN as the primary VLAN in a private VLAN.
decring *decimal_ring_number*	(Optional) Keyword and variable to specify the decimal ring number; valid values are from 1 to 4095.
parent *vlan_num*	(Optional) Keyword and variable to specify the VLAN number of the parent VLAN; valid values are from 2 to 1005.

backupcrf off | **on**	(Optional) Keywords to specify whether the TrCRF is a backup path for traffic.
stemaxhop *hopcount*	(Optional) Keyword and variable to specify the maximum number of hops for Spanning Tree Explorer frames; valid values are from 1 to 14.
rspan	(Optional) Keyword to create a VLAN for remote SPAN.

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.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

You cannot use the **set vlan** command until the Catalyst 6000 family 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.

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, the VLAN number must be within the range 2 to 1001. When you are modifying a VLAN, the valid range for the VLAN number is from 2 to 1005.

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 6000 family 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:

- **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.
- **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.

Examples

This example shows how to set VLAN 850 to include ports 3 through 7 on module 3:

```
Console> (enable) set vlan 850 3/4-7
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)
```

Related Commands

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

set vlan mapping

Use the **set vlan mapping** command to map 802.1Q VLANs to ISL VLANs.

set vlan mapping dot1q *1q_vlan_num* **isl** *isl_vlan_num*

Syntax Description

dot1q *1q_vlan_num*	Keyword and variable to specify the 802.1Q VLAN; valid values are from 1001 to 4095.
isl *isl_vlan_num*	Keyword to specify the ISL VLAN; valid values are from 1 to 1024.

Defaults

The default is all switched Ethernet ports and Ethernet repeater ports are in VLAN 1.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

IEEE 802.1Q VLAN trunks support VLANs 1 through 4095. ISL VLAN trunks support VLANs 1 through 1024 (1005 to 1024 are reserved). The switch automatically maps 802.1Q VLANs 1000 and lower to ISL VLANs with the same number.

Use this feature to map 802.1Q VLANs above 1000 to ISL VLANs.

You can map up to eight VLANs. 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.

If *vlan_num* 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.

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 **show vlan**
clear vlan mapping

set vtp

Use the **set vtp** command to set the options for VTP.

set vtp [**domain** *domain_name*] [**mode** {**client** | **server** | **transparent**}] [**passwd** *passwd*] [**pruning** {**enable** | **disable**}] [**v2** {**enable** | **disable**}]

Syntax Description

domain *domain_name*	(Optional) Keywords to define the name that identifies the VLAN management domain. The *domain_name* can be from 1 to 32 characters in length.
mode {**client** | **server** | **transparent**}	(Optional) Keywords to specify the VTP mode.
passwd *passwd*	(Optional) Keyword and variable to define the VTP password; the VTP password can be from 8 to 64 characters in length.
pruning {**enable** | **disable**}	(Optional) Keywords to enable or disable VTP pruning for the entire management domain.
v2 {**enable** | **disable**}	(Optional) Keywords to enable or disable version 2 mode.

Defaults

The defaults are as follows: server mode, no password, pruning disabled, and v2 disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

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 VTP domain.

If all switches in a domain are VTP version 2-capable, you only need to enable VTP version 2 on one switch (using the **set vtp v2 enable** command); the version number is then propagated to the other version 2-capable switches in the VTP domain.

If the VTP password has already been defined, entering **passwd 0** (zero) clears the VTP password.

VTP supports three different modes: server, client, and transparent. 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 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.

The **pruning** keyword is used to enable or disable VTP pruning for the 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 pruning** commands to specify which VLANs should or should not be pruned when pruning is enabled for the domain.

To disable VTP, enter the **set vtp mode transparent** command. This command disables VTP from the domain but does not remove the domain from the switch. 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.

Examples

This example shows how to use the **set vtp** command:

```
Console> (enable) set vtp domain Engineering mode client
VTP domain Engineering 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)
```

Related Commands

show vtp domain
set vlan
clear vlan
show vlan
set vtp pruneeligible
clear vtp pruning

set vtp pruneeligible

Use the **set vtp pruneeligible** command to specify which VTP domain VLANs are pruning eligible.

set vtp pruneeligible *vlan_range*

Syntax Description

vlan_range	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 pruning** 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 pruning** 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

show vtp domain
set vlan
clear vtp pruning

show accounting

Use the **show accounting** command to display accounting setup and configuration information on the switch.

show accounting

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privileged.

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 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)
```

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 alias

Use the **show alias** command to display a listing of defined command aliases.

show alias [*name*]

Syntax Description

name	(Optional) Name of the alias to be displayed.

Defaults

This command has no default setting.

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

Use the **show arp** command to display the ARP table.

show arp [*ip_addr* | *hostname*] [**noalias**]

Syntax Description

ip_addr	(Optional) Number of the IP address.
hostname	(Optional) Name of the host.
noalias	(Optional) Keyword to force the display to show only IP addresses, not IP aliases.

Defaults

This command has no default setting.

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

Use the **show authentication** command to display authentication information.

show authentication

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

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

Use the **show authorizaton** command to display authorization setup and configuration information on the switch.

show authorization

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default setting.

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

show boot

Use the **show boot** command to display the contents of the BOOT environment variables and the configuration register setting.

show boot [*mod*]

Syntax Description

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

Defaults

This command has no default setting.

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

Use the **show boot device** command to display the NAM boot string stored in NVRAM.

show boot device *mod*

Syntax Description

mod	Number of the module containing the Flash device.

Defaults

This command has no default setting.

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

Use the **show cam** command set to display CAM table entries.

show cam {**dynamic** | **static** | **permanent** | **system**} *mod/port*

show cam *mac_addr* [*vlan*]

Syntax Description

dynamic	Keyword to display dynamic CAM entries.
static	Keyword to display static CAM entries.
permanent	Keyword to display permanent CAM entries.
system	Keyword to display system CAM entries.
mod/port	Number of the module and the port on the module.
mac_addr	MAC address.
vlan	(Optional) Number of the VLAN.

Defaults

This command has no default setting.

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.

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.

VLAN  Dest MAC/Route Des    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 routers listed as the CAM entries:

```
Console> show cam 00-00-81-01-23-45
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry

Router Watergate with IP address 172.25.55.1 has CAM entries:
VLAN  Dest MAC/Route Des    Destination Ports or VCs
----  ------------------    ---------------------------------------------------
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>
```

Related Commands

clear cam
set cam
show config
show cam agingtime

show cam agingtime

Use the **show cam agingtime** command to display CAM aging time information for all configured VLANs.

show cam agingtime [*vlan*]

Syntax Description

vlan	(Optional) Number of the VLAN or range of VLANs; valid values are from **1** to **1005** and from **1025** to **4094**.

Defaults

This command has no default setting.

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

Use the **show cam** command to display the number of CAM entries only.

show cam count {**dynamic** | **static** | **permanent** | **system**} [*vlan*]

Syntax Description

dynamic	Keyword to display dynamic CAM entries.
static	Keyword to display static CAM entries.
permanent	Keyword to display permanent CAM entries.
system	Keyword to display system CAM entries.
vlan	(Optional) Number of the VLAN.

Defaults

This command has no default setting.

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 msfc

Use the **show cam msfc** command to display the router's MAC-VLAN entries.

show cam msfc {*mod*} [*vlan*]

Syntax Description

mod	Number of the module for which MSFC information is displayed.
vlan	(Optional) Number of the VLAN.

Defaults

This command has no default setting.

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 cdp

Use the **show cdp** command set to display CDP information.

show cdp

show cdp neighbors [*mod*[/*port*]] [**vlan** | **duplex** | **capabilities** | **detail**]

show cdp port [*mod*[/*port*]]

Syntax Description

neighbors	Keyword to show 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) Keyword to show the native VLAN number for the neighboring Cisco products.
duplex	(Optional) Keyword to show the duplex type of the neighboring Cisco products.
capabilities	(Optional) Keyword to show 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) Keyword to show detailed information about neighboring Cisco products.
port	Keyword to show CDP port settings.

Defaults

This command has no default setting.

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.

If you do not specify a module number, CDP information for the entire switch is displayed.

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> show cdp neighbors capabilities
* - indicates vlan mismatch.
# - indicates duplex mismatch.

Port     Device-ID                      Port-ID                  Capabilities
-------- ------------------------------ ------------------------ ------------
3/5      002267619                      3/6 *                    T S
3/6      002267619                      3/5                      T S
4/1      002267619                      4/2                      T S
4/2      002267619                      4/1 #                    T S
4/20     069000057                      8/5                      T B S
5/1      005763872                      2/1                      T B S
5/1      066506245                      2/1                      T B S
5/1      066508595                      5/12 *#                  T B S
5/1      066508596                      5/1                      T B S
Console>
```

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

Use the **show channel** command to display EtherChannel information for a channel.

show channel [*channel_id*] [**info** | **statistics** | **mac**]

show channel [*channel_id*] [**info** [**spantree** | **trunk** | **protcol** | **gmrp** | **gvrp** | **qos**]]

Syntax Description

channel_id	(Optional) Number of the channel.
info	(Optional) Keyword to display channel information.
statistics	(Optional) Keyword to display statistics about the port (PAgP packets sent and received).
mac	(Optional) Keyword to display MAC information about the channel.
spantree | **trunk** | **protocol** | **gmrp** | **gvrp** | **qos**	(Optional) Keyword to display feature-related parameters.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify *channel_id*, 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** keyword with any of the options (**spantree** | **trunk** | **protcol** | **gmrp** | **gvrp** | **qos**), the specified feature-related parameters are displayed in the output.

Examples

This example shows how to display channel information for a specific channel:

```
Console> show channel 768
Channel Ports                                            Status    Channel
id                                                                 Mode
------- ------------------------------------------------ --------- --------
768     2/1-2                                          connected on
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 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 -

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

Chan Port  Device-ID                      Port-ID                  Platform
id
---- ----- ------------------------------ ------------------------ ----------
769  1/1
769  1/2

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

Chan Port  Portvlancost-vlans
id
---- ----- ---------------------------------------------------------------------
769  1/1
769  1/2

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

Chan Port  Portvlancost-vlans
id
---- ----- ------------------------------------------------------------------
 769  1/1
 769  1/2
```

```
 865  4/1
 865  4/2

Chan Port  Port     Portfast Port    Port
id         priority          vlanpri vlanpri-vlans
---- ----- -------- -------- ------- ----------------------------------------
 769  1/1        32 disabled       0
 769  1/2        32 disabled       0
 865  4/1        32 disabled       0
 865  4/2        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
 865  4/1  on       auto-on  auto-on
 865  4/2  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
 865  4/1  enabled  normal       disabled
 865  4/2  enabled  normal       disabled

Chan Port  GVRP     GVRP          GVRP
id         status   registeration applicant
---- ----- -------- ------------- ---------
 769  1/1  disabled normal        normal
 769  1/2  disabled normal        normal
 865  4/1  disabled normal        normal
 865  4/2  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
 865  4/1  2q2t   1q4t   untrusted             0 false
 865  4/2  2q2t   1q4t   untrusted             0 false

Chan Port  ACL name                         Protocol
id
---- ----- -------------------------------- --------
 769  1/1                                   IP
                                            IPX
                                            MAC
 769  1/2                                   IP
                                            IPX
                                            MAC
 865  4/1                                   IP
                                            IPX
                                            MAC
 865  4/2                                   IP
                                            IPX
                                            MAC
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        92         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 port channel**
show channel group

show channel group

Use the **show channel group** command set to display EtherChannel group status information.

show channel group [*admin_group*] [**info** | **statistics**]

show channel group [*admin_group*] [**info** [**spantree** | **trunk** | **protcol** | **gmrp** | **gvrp** | **qos**]]

Syntax Description

admin_group	(Optional) Number of the administrative group; valid values are from 1 to 1024.
info	(Optional) Keyword to display group information.
statistics	(Optional) Keyword to display statistics about the group.
spantree | **trunk** | **protcol** | **gmrp** | **gvrp** | **qos**	(Optional) Keyword to display feature-related parameters.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Normal.

Usage Guidelines

If you do not specify *admin_group*, EtherChannel information is shown for all admin groups.

If you enter the optional **info** keyword with any of the options (**spantree** | **trunk** | **protcol** | **gmrp** | **gvrp** | **qos**), the specified feature-related parameters are displayed in the output.

Examples

This example shows how to display Ethernet channeling information for all admin 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 port channel**
show channel

show config

Use the **show config** command to display the nondefault system or module configuration.

show config {**system** | *mod*} [**all**]

Syntax Description

system	Keyword to display system configuration.
mod	Keyword to display module configuration.
all	(Optional) Keyword to specify all module and system configuration

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Normal.

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
!
```