Catalyst 2360 Switch Command Reference

Cisco IOS 12.2(53)EY
June 2010

Americas 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: 408 527-0883

Text Part Number: OL-19818-01

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/web/siteassets/legal/trademark.html. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Catalyst 2360 Switch Command Reference
© 2010 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface xiii

Audience xiii

Purpose xiii

Conventions xiii

Related Publications xiv

Obtaining Documentation and Submitting a Service Request xv

CHAPTER 1 **Using the Command-Line Interface** 1-1

CLI Command Modes 1-1

User EXEC Mode 1-2

Privileged EXEC Mode 1-3

Global Configuration Mode 1-3

Interface Configuration Mode 1-4

config-vlan Mode 1-4

Line Configuration Mode 1-4

CHAPTER 2 **Catalyst Switch Cisco IOS Commands** 2-1

aaa authorization network 2-1

archive download-sw 2-3

archive tar 2-6

archive upload-sw 2-9

boot config-file 2-11

boot enable-break 2-12

boot helper 2-13

boot helper-config-file 2-14

boot manual 2-15

boot private-config-file 2-16

boot system 2-17

channel-group 2-18

channel-protocol 2-21

class-map 2-22

clear eap 2-24

clear errdisable interface 2-25
clear lacp 2-26
clear logging onboard 2-27
clear mac address-table 2-28
clear pagp 2-29
clear spanning-tree counters 2-30
clear spanning-tree detected-protocols 2-31
clear vtp counters 2-32
cluster commander-address 2-33
cluster discovery hop-count 2-35
cluster enable 2-36
cluster holdtime 2-38
cluster member 2-39
cluster outside-interface 2-41
cluster run 2-42
cluster timer 2-43
copy logging onboard 2-44
define interface-range 2-46
delete 2-48
diagnostic monitor 2-49
diagnostic schedule 2-51
diagnostic start 2-53
duplex 2-55
errdisable detect cause 2-57
errdisable detect cause small-frame 2-59
errdisable recovery 2-60
errdisable recovery cause small-frame 2-62
exception crashinfo 2-63
flowcontrol 2-64
hw-module 2-66
interface port-channel 2-67
interface range 2-69
interface vlan 2-72
ip access-group 2-74
ip address 2-76

ip admission **2-78**
ip admission name proxy http **2-79**
ip igmp filter **2-80**
ip igmp max-groups **2-81**
ip igmp profile **2-83**
ip igmp snooping **2-85**
ip igmp snooping last-member-query-interval **2-87**
ip igmp snooping querier **2-89**
ip igmp snooping report-suppression **2-91**
ip igmp snooping tcn **2-93**
ip igmp snooping tcn flood **2-95**
ip igmp snooping vlan immediate-leave **2-96**
ip igmp snooping vlan static **2-97**
ip ssh **2-99**
ipv6 mld snooping **2-101**
ipv6 mld snooping last-listener-query-count **2-103**
ipv6 mld snooping last-listener-query-interval **2-105**
ipv6 mld snooping listener-message-suppression **2-107**
ipv6 mld snooping robustness-variable **2-109**
ipv6 mld snooping tcn **2-111**
ipv6 mld snooping vlan **2-113**
lacp port-priority **2-115**
lacp system-priority **2-117**
link state group **2-119**
link state track **2-121**
location (global configuration) **2-122**
location (interface configuration) **2-124**
logging file **2-126**
mac address-table aging-time **2-128**
mac address-table static **2-129**
mac address-table static drop **2-130**
match (class-map configuration) **2-132**
mdix auto **2-135**
media-type rj45 **2-137**
mls qos **2-138**

mls qos cos 2-140
mls qos queue-set output buffers 2-142
mls qos queue-set output threshold 2-144
mls qos srr-queue output cos-map 2-146
mls qos trust 2-148
monitor session 2-149
pagp learn-method 2-153
pagp port-priority 2-155
port-channel load-balance 2-157
priority-queue 2-159
radius-server dead-criteria 2-161
radius-server host 2-163
rcommand 2-165
reload 2-167
rmon collection stats 2-169
service password-recovery 2-170
setup 2-172
setup express 2-175
show access-lists 2-177
show archive status 2-180
show boot 2-181
show class-map 2-184
show cluster 2-185
show cluster candidates 2-187
show cluster members 2-189
show controllers cpu-interface 2-191
show controllers ethernet-controller 2-193
show controllers ethernet-controller fastethernet 2-201
show controllers tcam 2-203
show controllers utilization 2-205
show diagnostic 2-207
show dtp 2-211
show eap 2-213
show env 2-216
show errdisable detect 2-218

show errdisable flap-values 2-220
show errdisable recovery 2-221
show etherchannel 2-223
show fallback profile 2-226
show flowcontrol 2-228
show idprom 2-230
show interfaces 2-232
show interfaces counters 2-241
show interfaces transceivers 2-243
show inventory 2-247
show ip igmp profile 2-248
show ip igmp snooping 2-249
show ip igmp snooping groups 2-252
show ip igmp snooping mrouter 2-254
show ip igmp snooping querier 2-256
show ipv6 mld snooping 2-258
show ipv6 mld snooping address 2-260
show ipv6 mld snooping mrouter 2-262
show ipv6 mld snooping querier 2-264
show lacp 2-266
show link state group 2-270
show location 2-272
show mac address-table 2-275
show mac address-table address 2-277
show mac address-table aging-time 2-279
show mac address-table count 2-281
show mac address-table dynamic 2-283
show mac address-table interface 2-285
show mac address-table static 2-287
show mac address-table vlan 2-289
show mls qos 2-291
show mls qos interface 2-292
show mls qos maps 2-294
show mls qos queue-set 2-297
show monitor 2-299

show pagp 2-301
show setup express 2-303
show spanning-tree 2-304
show system mtu 2-310
show udld 2-311
show version 2-314
show vlan 2-316
show vtp 2-320
shutdown 2-325
shutdown vlan 2-326
small-frame violation rate 2-327
snmp-server enable traps 2-329
snmp-server host 2-332
snmp trap mac-notification 2-336
spanning-tree backbonefast 2-338
spanning-tree bpdufilter 2-339
spanning-tree bpduguard 2-341
spanning-tree cost 2-343
spanning-tree etherchannel guard misconfig 2-345
spanning-tree extend system-id 2-347
spanning-tree guard 2-349
spanning-tree link-type 2-351
spanning-tree loopguard default 2-353
spanning-tree mode 2-355
spanning-tree mst configuration 2-357
spanning-tree mst cost 2-359
spanning-tree mst forward-time 2-361
spanning-tree mst hello-time 2-362
spanning-tree mst max-age 2-363
spanning-tree mst max-hops 2-364
spanning-tree mst port-priority 2-365
spanning-tree mst pre-standard 2-367
spanning-tree mst priority 2-368
spanning-tree mst root 2-369
spanning-tree port-priority 2-371

spanning-tree portfast (global configuration) 2-373
spanning-tree portfast (interface configuration) 2-376
spanning-tree transmit hold-count 2-378
spanning-tree uplinkfast 2-379
spanning-tree vlan 2-381
speed 2-384
srr-queue bandwidth limit 2-386
srr-queue bandwidth shape 2-388
srr-queue bandwidth share 2-390
switchport access 2-392
switchport autostate exclude 2-393
switchport host 2-395
switchport mode 2-396
switchport nonegotiate 2-398
switchport trunk 2-400
system env temperature threshold yellow 2-403
system mtu 2-404
traceroute mac 2-406
traceroute mac ip 2-409
udld 2-411
udld port 2-413
udld reset 2-415
usb-inactivity-timeout 2-416
vlan (global configuration) 2-417
vtp (global configuration) 2-422
vtp (VLAN configuration) 2-426

APPENDIX A **Catalyst 2360 Switch Boot Loader Commands** A-1

arp A-2
boot A-3
cat A-5
copy A-6
delete A-7
dir A-8
flash_init A-10
format A-11

fsck A-12
help A-13
memory A-14
mgmt_clr A-16
mgmt_init A-17
mgmt_show A-18
mkdir A-19
more A-20
rename A-21
reset A-22
rmdir A-23
set A-24
type A-27
unset A-28
version A-30

APPENDIX B **Debug Commands** B-1
debug cluster B-2
debug dtp B-4
debug eap B-5
debug etherchannel B-6
debug fastethernet B-7
debug interface B-8
debug ip igmp filter B-9
debug ip igmp max-groups B-10
debug ip igmp snooping B-11
debug lacp B-12
debug matm B-13
debug matm move update B-14
debug monitor B-15
debug nvram B-16
debug pagp B-17
debug platform acl B-18
debug platform cpu-queues B-20
debug platform etherchannel B-22
debug platform frontend-controller B-23

debug platform ip igmp snooping B-24
debug platform led B-26
debug platform matm B-27
debug platform messaging application B-28
debug platform phy B-29
debug platform pm B-31
debug platform port-asic B-33
debug platform qos-acl-tcam B-34
debug platform resource-manager B-35
debug platform snmp B-36
debug platform span B-37
debug platform supervisor-asic B-38
debug platform sw-bridge B-39
debug platform tcam-driver B-40
debug platform udld B-42
debug platform vlan B-43
debug pm B-44
debug qos B-46
debug spanning-tree B-47
debug spanning-tree backbonefast B-49
debug spanning-tree bpdu B-50
debug spanning-tree bpdu-opt B-51
debug spanning-tree mstp B-52
debug spanning-tree switch B-54
debug spanning-tree uplinkfast B-56
debug sw-vlan B-57
debug sw-vlan ifs B-59
debug sw-vlan notification B-60
debug sw-vlan vtp B-62
debug udld B-64
debug vqpc B-66

APPENDIX C **Show Platform Commands** C-1

show platform acl C-2
show platform dl C-3
show platform etherchannel C-4

show platform forward C-5
show platform frontend-controller C-7
show platform ip igmp snooping C-8
show platform layer4op C-10
show platform mac-address-table C-11
show platform messaging C-12
show platform monitor C-13
show platform pm C-14
show platform port-asic C-15
show platform qos C-20
show platform resource-manager C-21
show platform snmp counters C-23
show platform spanning-tree synchronization C-24
show platform stp-instance C-25
show platform tcam C-26
show platform vlan C-28

APPENDIX D **Acknowledgments for Open-Source Software** D-1

INDEX

Preface

Audience

This guide is for the networking professional using the Cisco IOS command-line interface (CLI) to manage the Catalyst 2360 switch, referred to as *the switch*. Before using this guide, you should have experience working with the Cisco IOS commands and the switch software features. Before using this guide, you should have experience working with the concepts and terminology of Ethernet and local area networking.

Purpose

This guide provides the information that you need about the Layer 2 commands that have been created or changed for use with the Catalyst 2360 switch. For information about the standard Cisco IOS Release 12.2 commands, see the Cisco IOS documentation set available from the Cisco.com home page by selecting **Technical Support & Documentation > Documentation > Cisco IOS Software**.

This guide does not provide procedures for configuring your switch. For detailed configuration procedures, see the software configuration guide for this release.

This guide does not describe system messages you might encounter. For more information, see the system message guide for this release.

For documentation updates, see the release notes for this release.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) means optional elements.
- Braces ({}) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and warnings use these conventions and symbols:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

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

Related Publications

These documents provide complete information about the switch and are available from these Cisco.com sites:

http://www.cisco.com/en/US/products/ps10920/tsd_products_support_series_home.html

Note Before installing, configuring, or upgrading the switch, see these documents:

- For initial configuration information, see the "Using Express Setup" section in the getting started guide or the "Configuring the Switch with the CLI-Based Setup Program" appendix in the hardware installation guide.
- For device manager requirements, see the "System Requirements" section in the release notes .
- For Network Assistant requirements, see the *Getting Started with Cisco Network Assistant* .
- For cluster requirements, see the *Release Notes for Cisco Network Assistant* ..
- For upgrade information, see the "Downloading Software" section in the release notes.

For more information, see these documents on Cisco.com.

- *Release Notes for the Catalyst 2360 Switches*
- *Catalyst 2360 Switch Software Configuration Guide*
- *Catalyst 2360 Switch Command Reference*
- *Catalyst 2360 Switch System Message Guide*
- *Catalyst 2360 Switch Hardware Installation Guide*
- *Getting Started Guide for the Catalyst 2360 Switch*
- *Getting Started Guide for the Catalyst 3560-E Switch*
- *Regulatory Compliance and Safety Information for the Catalyst 2360 Switches*
- *Getting Started with Cisco Network Assistant*
- *Release Notes for Cisco Network Assistant*

- *Installation Notes for the Power Supply Modules for the Catalyst 2360 Switch*
- *Installation Notes for the Fan Modules for the Catalyst 2360 Switch*
- *Product Documentation and Compliance for the Catalyst 2360 Switch*

For more information about the Network Admission Control (NAC) features, see the *Network Admission Control Software Configuration Guide.*

- Information about Cisco SFP, SFP+, and GBIC modules is available from this Cisco.com site:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

  SFP compatibility matrix documents are available from this Cisco.com site:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Using the Command-Line Interface

The Catalyst 2360 switch is supported by Cisco IOS software. This chapter describes how to use the switch command-line interface (CLI) to configure software features. You can connect to the switch through the console port or Ethernet management port.

For a complete description of the commands that support these features, see Chapter 2, "Catalyst Switch Cisco IOS Commands." For information on the boot loader commands, see Appendix A, "Catalyst 2360 Switch Boot Loader Commands." For information on the **debug** commands, see Appendix B, "Debug Commands." For information on the **show platform** commands, see Appendix C, "Show Platform Commands." For more information on Cisco IOS Release 12.2, see the *Cisco IOS Release 12.2 Command Summary.*

For task-oriented configuration steps, see the software configuration guide for this release.

In this document, IP refers to IP version 4 (IPv4) unless there is a specific reference to IP version 6 (IPv6).

CLI Command Modes

This section describes the CLI command mode structure. Command modes support specific Cisco IOS commands. For example, the **interface** *interface-id* command only works when entered in global configuration mode.

These are the main command modes for the switch:

- User EXEC
- Privileged EXEC
- Global configuration
- Interface configuration
- Config-vlan
- VLAN configuration
- Line configuration

Table 1 lists the main command modes, how to access each mode, the prompt you see in that mode, and how to exit that mode. The prompts listed use the default name *Switch*.

Table 1 Command Modes Summary

Command Mode	Access Method	Prompt	Exit or Access Next Mode
User EXEC	This is the first level of access. (For the switch) Change terminal settings, perform basic tasks, and list system information.	`Switch>`	Enter the **logout** command. To enter privileged EXEC mode, enter the **enable** command.
Privileged EXEC	From user EXEC mode, enter the **enable** command.	`Switch#`	To exit to user EXEC mode, enter the **disable** command. To enter global configuration mode, enter the **configure** command.
Global configuration	From privileged EXEC mode, enter the **configure** command.	`Switch(config)#`	To exit to privileged EXEC mode, enter the **exit** or **end** command, or press **Ctrl-Z**. To enter interface configuration mode, enter the **interface** configuration command.
Interface configuration	From global configuration mode, specify an interface by entering the **interface** command followed by an interface identification.	`Switch(config-if)#`	To exit to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**. To exit to global configuration mode, enter the **exit** command.
Config-vlan	In global configuration mode, enter the **vlan** *vlan-id* command.	`Switch(config-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.
Line configuration	From global configuration mode, specify a line by entering the **line** command.	`Switch(config-line)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

User EXEC Mode

After you access the device, you are automatically in user EXEC command mode. The EXEC commands available at the user level are a subset of those available at the privileged level. In general, use the user EXEC commands to temporarily change terminal settings, perform basic tests, and list system information.

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch> ?
```

Privileged EXEC Mode

Because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** privileged EXEC command through which you access the remaining command modes.

If your system administrator has set a password, you are prompted to enter it before being granted access to privileged EXEC mode. The password does not appear on the screen and is case sensitive.

The privileged EXEC mode prompt is the device name followed by the pound sign (#).

```
Switch#
```

Enter the **enable** command to access privileged EXEC mode:

```
Switch> enable
Switch#
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch# ?
```

To return to user EXEC mode, enter the **disable** privileged EXEC command.

Global Configuration Mode

Global configuration commands apply to features that affect the device as a whole. Use the **configure** privileged EXEC command to enter global configuration mode. The default is to enter commands from the management console.

When you enter the **configure** command, a message prompts you for the source of the configuration commands:

```
Switch# configure
Configuring from terminal, memory, or network [terminal]?
```

You can specify either the terminal or NVRAM as the source of configuration commands.

This example shows you how to access global configuration mode:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch(config)# ?
```

To exit global configuration command mode and to return to privileged EXEC mode, enter the **end** or **exit** command, or press **Ctrl-Z**.

Interface Configuration Mode

Interface configuration commands modify the operation of the interface. Interface configuration commands always follow a global configuration command, which defines the interface type.

Use the **interface** *interface-id* command to access interface configuration mode. The new prompt means interface configuration mode.

```
Switch(config-if)#
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch(config-if)# ?
```

To exit interface configuration mode and to return to global configuration mode, enter the **exit** command. To exit interface configuration mode and to return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

config-vlan Mode

Use this mode to configure normal-range VLANs (VLAN IDs 1 to 1005) or, when VTP mode is transparent, to configure extended-range VLANs (VLAN IDs 1006 to 4094). When VTP mode is transparent, the VLAN and VTP configuration is saved in the running configuration file, and you can save it to the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command. The configurations of VLAN IDs 1 to 1005 are saved in the VLAN database if VTP is in transparent or server mode. The extended-range VLAN configurations are not saved in the VLAN database.

Enter the **vlan** *vlan-id* global configuration command to access config-vlan mode:

```
Switch(config)# vlan 2000
Switch(config-vlan)#
```

The supported keywords can vary but are similar to the commands available in VLAN configuration mode. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch(config-vlan)# ?
```

For extended-range VLANs, all characteristics except the MTU size must remain at the default setting.

To return to global configuration mode, enter **exit**; to return to privileged EXEC mode, enter **end**. All the commands except **shutdown** take effect when you exit config-vlan mode.

Line Configuration Mode

Line configuration commands modify the operation of a terminal line. Line configuration commands always follow a line command, which defines a line number. Use these commands to change terminal parameter settings line-by-line or for a range of lines.

Use the **line vty** *line_number* [*ending_line_number*] command to enter line configuration mode. The new prompt means line configuration mode. The following example shows how to enter line configuration mode for virtual terminal line 7:

```
Switch(config)# line vty 0 7
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch(config-line)# ?
```

To exit line configuration mode and to return to global configuration mode, use the **exit** command. To exit line configuration mode and to return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

CHAPTER 2

Catalyst Switch Cisco IOS Commands

aaa authorization network

Use the **aaa authorization network** global configuration command to the configure the switch to use user-RADIUS authorization for all network-related service requests, such as VLAN assignment. Use the **no** form of this command to disable RADIUS user authorization.

aaa authorization network default group radius

no aaa authorization network default

Syntax Description

default group radius	Use the list of all RADIUS hosts in the server group as the default authorization list.

Defaults

Authorization is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **aaa authorization network default group radius** global configuration command to allow the switch to download authorization parameters from the RADIUS servers in the default authorization list. The authorization parameters are used by features such as VLAN assignment to get parameters from the RADIUS servers.

Use the **show running-config** privileged EXEC command to display the configured lists of authorization methods.

Examples

This example shows how to configure the switch for user RADIUS authorization for all network-related service requests:

```
Switch(config)# aaa authorization network default group radius
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.

archive download-sw

Use the **archive download-sw** privileged EXEC command to download a new image from a TFTP server to the switch and to overwrite or keep the existing image.

archive download-sw [**/allow-feature-upgrade** | **/directory** | **/force-reload** | **/imageonly** | **/leave-old-sw** | **/no-set-boot** | **/no-version-check** | **/only-system-type** *system-type* | **/overwrite** | **/reload** | **/safe**] *source-url1* [*source-url2 source-url3 source-url4*]

archive download-sw [**/allow-feature-upgrade** | **/directory** | **/force-reload** | **/imageonly** | **/leave-old-sw** | **/no-set-boot** | **/overwrite** | **/reload** | **/safe**] **/directory** *source-url1* [*source-url2 source-url3 source-url4*]

Syntax Description

/allow-feature-upgrade	Allow installation of software images with different feature sets (for example, upgrade from the IP base feature set to the IP services features set).
/directory	Specify a directory for all of the images.
/force-reload	Unconditionally force a system reload after successfully downloading the software image.
/imageonly	Download only the software image but not the HTML files associated with the embedded device manager. The HTML files for the existing version are deleted only if the existing version is being overwritten or removed.
/leave-old-sw	Keep the old software version after a successful download.
/no-set-boot	Do not alter the setting of the BOOT environment variable to point to the new software image after it is successfully downloaded.
/overwrite	Overwrite the software image in flash memory with the downloaded one.
/reload	Reload the system after successfully downloading the image unless the configuration has been changed and not been saved.
/safe	Keep the current software image; do not delete it to make room for the new software image before the new image is downloaded. The current image is deleted after the download.

source-url1 [*sourceurl2 sourceurl3 sourceurl4*]	The source URLs for the software images. Enter one source URL for the software image that the switch supports. The *image-name*.**tar** is the software image to download and install on the switch. These options are supported: • Local flash file system syntax: **flash:** • FTP syntax: **ftp:**[[**//***username*[**:***password*]@*location*]/*directory*]/*image-name*.**tar** • HTTP server syntax: **http://**[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name*.**tar** • Secure HTTP server syntax: **https://**[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name*.**tar** • Remote Copy Protocol (RCP) syntax: **rcp:**[[**//***username*@*location*]/*directory*]/*image-name*.**tar** • Secure Copy Protocol (SCP) syntax for the: **scp:**[[**//***username*@*location*]/*directory*]/*image-name*.**tar** • The syntax for the TFTP: **tftp:**[[**//***location*]/*directory*]/*image-name*.**tar**

Defaults

The current software image is not overwritten with the downloaded image.

Both the software image and HTML files are downloaded.

The new image is downloaded to the flash: file system.

The BOOT environment variable is changed to point to the new software image on the flash: file system.

Image names are case sensitive; the image file is provided in tar format.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **/allow-feature-upgrade** option to allow installation of an image with a different feature set, for example, upgrading from the IP base feature set to the IP services feature.

You can use the **archive download-sw /directory** command to specify a directory only once, followed by a tar file or list of tar files to be downloaded, instead of specifying complete paths with each tar file.

The **/imageonly** option removes the HTML files for the existing image if the existing image is being removed or replaced. Only the Cisco IOS image (without the HTML files) is downloaded.

Using the **/safe** or **/leave-old-sw** option can cause the new image download to fail if there is insufficient flash memory. If leaving the software in place prevents the new image from fitting in flash memory due to space constraints, an error results.

If you used the **/leave-old-sw** option and did not overwrite the old image when you downloaded the new one, you can remove the old image by using the **delete** privileged EXEC command. For more information, see the "delete" section on page 2-48.

Use the **/overwrite** option to overwrite the image on the flash device with the downloaded one.

If you specify the command *without* the **/overwrite** option, the download algorithm verifies that the new image is not the same as the one on the switch flash device. If the images are the same, the download does not occur. If the images are different, the old image is deleted, and the new one is downloaded.

After downloading a new image, enter the **reload** privileged EXEC command to begin using the new image, or specify the **/reload** or **/force-reload** option in the **archive download-sw** command.

Use the **/directory** option to specify a directory for the images.

Examples

This example shows how to download a new image from a TFTP server at 172.20.129.10 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://172.20.129.10/test-image.tar
```

This example shows how to download only the software image from a TFTP server at 172.20.129.10 to the switch:

```
Switch# archive download-sw /imageonly tftp://172.20.129.10/test-image.tar
```

This example shows how to keep the old software version after a successful download:

```
Switch# archive download-sw /leave-old-sw tftp://172.20.129.10/test-image.tar
```

This example specifies the location of two tar images without having to specify the path each time:

```
Switch# archive download-sw tftp://10.1.1.10/
c2360-universsalk9.tar c2360-universalk9_2.tar
```

Related Commands

Command	Description
archive tar	Creates a tar file, lists the files in a tar file, or extracts the files from a tar file.
archive upload-sw	Uploads an existing image on the switch to a server.
delete	Deletes a file or directory on the flash memory device.

archive tar

Use the **archive tar** privileged EXEC command to create a tar file, list files in a tar file, or extract the files from a tar file.

archive tar {**/create** *destination-url* **flash:/***file-url*} | {**/table** *source-url*} | {**/xtract** *source-url* **flash:/***file-url* [*dir/file...*]}

Syntax Description

/create *destination-url* **flash:/***file-url*	Create a new tar file on the local or network file system. For *destination-url,* specify *t*he destination URL alias for the local or network file system and the name of the tar file to create. These options are supported: • The syntax for the local flash filesystem: **flash:** • The syntax for the FTP: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar** • The syntax for an HTTP server: **http://**[[*username***:***password*]**@**]{*hostname* | *host-ip*}[**/***directory*]**/***image-name***.tar** • The syntax for a secure HTTP server: **https://**[[*username***:***password*]**@**]{*hostname* | *host-ip*}[**/***directory*]**/***image-name***.tar** • The syntax for the Remote Copy Protocol (RCP): **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar** • The syntax for the TFTP: **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar** The *tar-filename***.tar** is the tar file to be created. For **flash:/***file-url, specify t*he location on the local flash file system from which the new tar file is created. An optional list of files or directories within the source directory can be specified to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file.

/table *source-url*	Display the contents of an existing tar file to the screen. For *source-url*, specify the source URL alias for the local or network file system. These options are supported: • The syntax for the local flash file system: **flash:** • The syntax for the FTP: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar** • The syntax for an HTTP server: **http://**[[*username***:***password*]**@**]{*hostname* | *host-ip*}[**/***directory*]**/***image-name***.tar** • The syntax for a secure HTTP server: **https://**[[*username***:***password*]**@**]{*hostname* | *host-ip*}[**/***directory*]**/***image-name***.tar** • The syntax for the RCP: **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar** • The syntax for the TFTP: **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar** The *tar-filename***.tar** is the tar file to display.
/xtract *source-url* **flash:/***file-url* [*dir/file...*]	Extract files from a tar file to the local file system. For *source-url*, specify *t*he source URL alias for the local file system. These options are supported: • The syntax for the local flash file system: **flash:** • The syntax for the FTP: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar** • The syntax for an HTTP server: **http://**[[*username***:***password*]**@**]{*hostname* | *host-ip*}[**/***directory*]**/***image-name***.tar** • The syntax for a secure HTTP server: **https://**[[*username***:***password*]**@**]{*hostname* | *host-ip*}[**/***directory*]**/***image-name***.tar** • The syntax for the RCP: **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar** • The syntax for the TFTP: **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar** The *tar-filename***.tar** is the tar file from which to extract. For **flash:/***file-url* [*dir/file...*], specify *t*he location on the local flash file system into which the tar file is extracted. Use the *dir/file...* option to specify an optional list of files or directories within the tar file to be extracted. If none are specified, all files and directories are extracted.

Defaults

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Image names are case sensitive.

Examples

This example shows how to create a tar file. The command writes the contents of the *new-configs* directory on the local flash device to a file named *saved.tar* on the TFTP server at 172.20.10.30:

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

This example shows how to display the contents of the *c2360-universalk9.tar* file that is in flash memory. The contents of the tar file appear on the screen:

```
Switch# archive tar /table flash:c2360-universalk9.tar
info (219 bytes)

c2360-universalk9.tar/ (directory)
c2360-universalk9.tar(610856 bytes)
c2360-universalk9.tar/info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the *c2360-universalk9.tar /html* directory and its contents:

```
Switch# archive tar /table flash:c2360-universalk9.tar/html
c2360-universalk9.tar/html/ (directory)
c2360-universalk9.tar/html/const.htm (556 bytes)
c2360-universalk9.tar/html/xhome.htm (9373 bytes)
c2360-universalk9.tar/html/menu.css (1654 bytes)
<output truncated>
```

This example shows how to extract the contents of a tar file on the TFTP server at 172.20.10.30. This command extracts just the *new-configs* directory into the root directory on the local flash file system. The remaining files in the *saved.tar* file are ignored.

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/ new-configs
```

Related Commands

Command	Description
archive download-sw	Downloads a new image from a TFTP server to the switch.
archive upload-sw	Uploads an existing image on the switch to a server.

archive upload-sw

Use the **archive upload-sw** privileged EXEC command to upload an existing switch image to a server.

archive upload-sw [**/version** *version_string*] *destination-url*

Syntax Description

/version *version_string*	(Optional) Specify the specific version string of the image to be uploaded.
destination-url	The destination URL alias for a local or network file system. The *image-name***.tar** is the name of software image to be stored on the server. These options are supported: • Local flash file system syntax: **flash:** • FTP syntax: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***image-name***.tar** • HTTP server syntax: **http://**[[*username***:***password*]**@**]{*hostname* | *host-ip*}[**/***directory*]**/***image-name***.tar** • Secure HTTP server syntax: **https://**[[*username***:***password*]**@**]{*hostname* | *host-ip*}[**/***directory*]**/***image-name***.tar** • Remote Copy Protocol (RCP) syntax: **rcp:**[[**//***username***@***location*]**/***directory*]**/***image-name***.tar** • TFTP syntax: **tftp:**[[**//***location*]**/***directory*]**/***image-name***.tar**

Defaults

Uploads the currently running image from the flash: file system.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the upload feature only if the HTML files associated with the embedded device manager have been installed with the existing image.

The files are uploaded in this sequence: the Cisco IOS image, the HTML files, and info. After these files are uploaded, the software creates the tar file.

Image names are case sensitive.

Examples

This example shows how to upload the currently running image to a TFTP server at 172.20.140.2:

```
Switch# archive upload-sw tftp://172.20.140.2/test-image.tar
```

Related Commands

Command	Description
archive download-sw	Downloads a new image to the switch.
archive tar	Creates a tar file, lists the files in a tar file, or extracts the files from a tar file.

boot config-file

Use the **boot config-file** global configuration command on a standalone switch to specify the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. Use the **no** form of this command to return to the default setting.

boot config-file flash:*/file-url*

no boot config-file

Syntax Description

flash:*/file-url*	The path (directory) and name of the configuration file.

Defaults

The default configuration file is flash:config.text.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

This command changes the setting of the CONFIG_FILE environment variable. For more information, see Appendix A, "Catalyst 2360 Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

boot enable-break

Use the **boot enable-break** global configuration command on a standalone switch to enable interrupting the automatic boot process. Use the **no** form of this command to return to the default setting.

boot enable-break

no boot enable-break

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled. The automatic boot process cannot be interrupted by pressing the Break key on the console.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When you enter this command, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system is initialized.

Note Despite the setting of this command, you can interrupt the automatic boot process at any time by pressing the MODE button on the switch front panel.

This command changes the setting of the ENABLE_BREAK environment variable. For more information, see Appendix A, "Catalyst 2360 Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

boot helper

Use the **boot helper** global configuration command to dynamically load files during boot loader initialization to extend or patch the functionality of the boot loader. Use the **no** form of this command to return to the default.

boot helper *filesystem***:/***file-url* ...

no boot helper

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*file-url*	The path (directory) and a list of loadable files to dynamically load during loader initialization. Separate each image name with a semicolon.

Defaults

No helper files are loaded.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This variable is used only for internal development and testing.

Filenames and directory names are case sensitive.

This command changes the setting of the HELPER environment variable. For more information, see Appendix A, "Catalyst 2360 Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

boot helper-config-file

Use the **boot helper-config-file** global configuration command to specify the name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of Cisco IOS that are loaded. Use the **no** form of this command to return to the default setting.

boot helper-config-file *filesystem***:/***file-url*

no boot helper-config file

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	The path (directory) and helper configuration file to load.

Defaults

No helper configuration file is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This variable is used only for internal development and testing.

Filenames and directory names are case sensitive.

This command changes the setting of the HELPER_CONFIG_FILE environment variable. For more information, see Appendix A, "Catalyst 2360 Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

boot manual

Use the **boot manual** global configuration command on a standalone switch to enable manually booting the switch during the next boot cycle. Use the **no** form of this command to return to the default setting.

boot manual

no boot manual

Syntax Description

This command has no arguments or keywords.

Defaults

Manual booting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The next time you reboot the system, the switch is in boot loader mode, which is shown by the *switch:* prompt. To boot up the system, use the **boot** boot loader command, and specify the name of the bootable image.

This command changes the setting of the MANUAL_BOOT environment variable. For more information, see Appendix A, "Catalyst 2360 Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

boot private-config-file

Use the **boot private-config-file** global configuration command on a standalone switch to specify the filename that Cisco IOS uses to read and write a nonvolatile copy of the private configuration. Use the **no** form of this command to return to the default setting.

boot private-config-file *filename*

no boot private-config-file

Syntax Description

filename	The name of the private configuration file.

Defaults

The default configuration file is *private-config*.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Filenames are case sensitive.

Examples

This example shows how to specify the name of the private configuration file to be *pconfig*:

```
Switch(config)# boot private-config-file pconfig
```

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

boot system

Use the **boot system** global configuration command to specify the Cisco IOS image to load during the next boot cycle. Use the **no** form of this command to return to the default setting.

boot system {*filesystem*:/*file-url* ...}

no boot system

no boot system switch {*number* | **all**}

Syntax Description

filesystem:	Alias for a flash file system. Use **flash:** for the system board flash device.
/*file-url*	The path (directory) and name of a bootable image. Separate image names with a semicolon.

Defaults

The switch attempts to automatically boot up the system by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you enter the **boot system** f*ilesystem:/file-url* command the specified software image is loaded during the next boot cycle.

If you are using the **archive download-sw** privileged EXEC command to maintain system images, you never need to use the **boot system** command. The **boot system** command is automatically manipulated to load the downloaded image.

This command changes the setting of the BOOT environment variable. For more information, see Appendix A, “Catalyst 2360 Switch Boot Loader Commands.”

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

channel-group

Use the **channel-group** interface configuration command to assign an Ethernet port to an EtherChannel group, to enable an EtherChannel mode, or both. Use the **no** form of this command to remove an Ethernet port from an EtherChannel group.

channel-group *channel-group-number* **mode** {**active** | {**auto** [**non-silent**]} | {**desirable** [**non-silent**]} | **on** | **passive**}

no channel-group

PAgP modes:
channel-group *channel-group-number* **mode** {{**auto** [**non-silent**]} | {**desirable** [**non-silent**}}

On mode:
channel-group *channel-group-number* **mode on**

Syntax Description

channel-group-number	Specify the channel group number. The range is 1 to 48.
mode	Specify the EtherChannel mode.
active	Active mode places a port into a negotiating state in which the port initiates negotiations with other ports by sending LACP packets. A channel is formed with another port group in either the active or passive mode.
auto	Enable the Port Aggregation Protocol (PAgP) only if a PAgP device is detected. Auto mode places a port into a passive negotiating state in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. A channel is formed only with another port group in desirable mode. When **auto** is enabled, silent operation is the default.
desirable	Unconditionally enable PAgP. Desirable mode places a port into an active negotiating state in which the port starts negotiations with other ports by sending PAgP packets. An EtherChannel is formed with another port group that is in the desirable or auto mode. When **desirable** is enabled, silent operation is the default.
non-silent	(Optional) Use in PAgP mode with the **auto** or **desirable** keyword when traffic is expected from the other device.
on	Enable **on** mode. In **on** mode, a usable EtherChannel exists only when both connected port groups are in the **on** mode.
passive	Passive mode places a port into a negotiating state in which the port responds to received LACP packets but does not initiate LACP packet negotiation. A channel is formed only with another port group in active mode.

Defaults

No channel groups are assigned.

No mode is configured.

Command Modes Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface first by using the **interface port-channel** global configuration command before assigning a physical port to a channel group. Instead, you can use the **channel-group** interface configuration command. It automatically creates the port-channel interface when the channel group gets its first physical port if the logical interface is not already created. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number,* or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

You do not have to disable the IP address that is assigned to a physical port that is part of a channel group, but we strongly recommend that you do so.

After you configure an EtherChannel, configuration changes that you make on the port-channel interface apply to all the physical ports assigned to the port-channel interface. Configuration changes applied to the physical port affect only the port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply configuration commands to the port-channel interface, for example, spanning-tree commands or commands to configure a Layer 2 EtherChannel as a trunk.

If you do not specify **non-silent** with the **auto** or **desirable** mode, silent is assumed. The silent mode is used when the switch is connected to a device that is not PAgP-capable and seldom, if ever, sends packets. A example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port prevents that port from ever becoming operational. However, it allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. Both ends of the link cannot be set to silent.

In the **on** mode, an EtherChannel exists only when a port group in the **on** mode is connected to another port group in the **on** mode.

Caution You should use care when using the **on** mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same switch. Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.

If you set the protocol by using the **channel-protocol** interface configuration command, the setting is not overridden by the **channel-group** interface configuration command.

For a complete list of configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

Examples

This example shows how to configure an EtherChannel that assigns two static-access ports in VLAN 10 to channel 5 with the PAgP mode **desirable**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end
```

This example shows how to configure an EtherChannel that assigns two static-access ports in VLAN 10 to channel 5 with the LACP mode **active**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
channel-protocol	Restricts the protocol used on a port to manage channeling.
interface port-channel	Accesses or creates the port channel.
show etherchannel	Displays EtherChannel information for a channel.
show lacp	Displays LACP channel-group information.
show pagp	Displays PAgP channel-group information.
show running-config	Displays the operating configuration.

channel-protocol

Use the **channel-protocol** interface configuration command to restrict the protocol used on a port to manage channeling. Use the **no** form of this command to return to the default setting.

channel-protocol {**lacp** | **pagp**}

no channel-protocol

Syntax Description

lacp	Configure an EtherChannel with the Link Aggregation Control Protocol (LACP).
pagp	Configure an EtherChannel with the Port Aggregation Protocol (PAgP).

Defaults

No protocol is assigned to the EtherChannel.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **channel-protocol** command only to restrict a channel to LACP or PAgP. If you set the protocol by using the **channel-protocol** command, the setting is not overridden by the **channel-group** interface configuration command.

You must use the **channel-group** interface configuration command to configure the EtherChannel parameters. The **channel-group** command also can set the mode for the EtherChannel.

You cannot enable both the PAgP and LACP modes on an EtherChannel group.

PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

Examples

This example shows how to specify LACP as the protocol that manages the EtherChannel:

```
Switch(config-if)# channel-protocol lacp
```

You can verify your settings by entering the **show etherchannel** [*channel-group-number*] **protocol** privileged EXEC command.

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
show etherchannel protocol	Displays protocol information the EtherChannel.

class-map

Use the **class-map** global configuration command to create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode. Use the **no** form of this command to delete an existing class map and to return to global configuration mode.

class-map [**match-all** | **match-any**] *class-map-name*

no class-map [**match-all** | **match-any**] *class-map-name*

Syntax Description

match-all	(Optional) Perform a logical-AND of all matching statements under this class map. All criteria in the class map must be matched.
match-any	(Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria must be matched.
class-map-name	Name of the class map.

Defaults

No class maps are defined.

If neither the **match-all** or **match-any** keyword is specified, the default is **match-all**.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.

After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **description**: describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class-map.
- **exit**: exits from QoS class-map configuration mode.
- **match**: configures classification criteria. For more information, see the **match (class-map configuration)** command.
- **no**: removes a match statement from a class map.
- **rename**: renames the current class map. If you rename a class map with a name that is already used, the message `A class-map with this name already exists` appears.

If you enter the **match-all** or **match-any** keyword, you can only use it to specify an extended named access control list (ACL) with the **match access-group** *acl-index-or-name* class-map configuration command.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-all** and **match-any** keywords are equivalent.

Only one ACL can be configured in a class map. The ACL can have multiple access control entries (ACEs).

Examples

This example shows how to configure the class map called *class1* with one match criterion, which is an access list called *103*:

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

This example shows how to delete the class map ***class1***:

```
Switch(config)# no class-map class1
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

Related Commands

Command	Description
class-map	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name.
match (class-map configuration)	Defines the match criteria to classify traffic.
port-channel load-balance	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show class-map	Displays QoS class maps.

clear eap

Use the **clear eap** privileged EXEC command to clear Extensible Authentication Protocol (EAP) session information for the switch or for the specified port.

clear eap sessions [**credentials** *name* [**interface** *interface-id*] | **interface** *interface-id* | **method** *name* | **transport** *name*] [**credentials** *name* | **interface** *interface-id* | **transport** *name*] ...

Syntax Description

credentials name	Clear EAP credential information for the specified profile.
interface *interface-id*	Clear EAP information for the specified interface.
method name	Clear EAP information for the specified method.
transport name	Clear EAP transport information for the specified lower level.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can clear all counters by using the **clear eap** command, or you can clear only the specific information by using the keywords.

Examples

This example shows how to clear all EAP information:

```
Switch# clear eap
```

This example shows how to clear EAP-session credential information for the specified profile:

```
Switch# clear eap sessions credential type1
```

Related Commands

Command	Description
show eap	Displays EAP registration and session information for the switch or for the specified port

clear errdisable interface

Use the **clear errdisable interface** privileged EXEC command to re-enable a VLAN that was error disabled.

clear errdisable interface ***interface-id*** vlan [vlan-list]

Syntax Description

vlan list	(Optional) Specify a list of VLANs to be re-enabled. If a vlan-list is not specified, then all VLANs are re-enabled.

Command Default

No default is defined

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can re-enable a port by using the **shutdown** and **no shutdown** interface configuration commands, or you can clear error disable for VLANs by using the **clear errdisable interface** command.

Examples

This example shows how to re-enable all VLANs that were error-disabled on Gigabit Ethernet port 0/2.

```
Switch# clear errdisable interface gigabitethernet0/2 vlan
```

Related Commands

Command	Description
errdisable detect cause	Enables error-disabled detection for a specific cause or all causes.
errdisable recovery	Configures the recovery mechanism variables.
show errdisable detect	Displays error-disabled detection status.
show errdisable recovery	Display error-disabled recovery timer information.
show interfaces status err-disabled	Displays interface status of a list of interfaces in error-disabled state.

clear lacp

Use the **clear lacp** privileged EXEC command to clear Link Aggregation Control Protocol (LACP) channel-group counters.

clear lacp {*channel-group-number* **counters** | **counters**}

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 48.
counters	Clear traffic counters.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can clear all counters by using the **clear lacp counters** command, or you can clear only the counters for the specified channel group by using the **clear lacp** *channel-group-number* **counters** command.

Examples

This example shows how to clear all channel-group information:

```
Switch# clear lacp counters
```

This example shows how to clear LACP traffic counters for group 4:

```
Switch# clear lacp 4 counters
```

You can verify that the information was deleted by entering the **show lacp counters** or the **show lacp 4 counters** privileged EXEC command.

Related Commands

Command	Description
show lacp	Displays LACP channel-group information.

clear logging onboard

Use the **clear logging onboard** privileged EXEC command to clear all of the on-board failure logging (OBFL) data except for the uptime and CLI-command information stored in the flash memory.

clear logging onboard

Syntax Description

This command has no arguments or keywords.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

We recommend that you keep OBFL enabled and do not erase the data stored in the flash memory.

Examples

This example shows how to clear all the OBFL information except for the uptime and CLI-command information:

```
Switch# clear logging onboard
Clear logging onboard buffer [confirm]
```

You can verify that the information was deleted by entering the **onboard** privileged EXEC command.

Related Commands

Command	Description
hw-module module [*switch-number*] logging onboard	Enables OBFL.
onboard	Displays OBFL information.

clear mac address-table

Use the **clear mac address-table** privileged EXEC command to delete from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN. This command also clears the MAC address notification global counters.

clear mac address-table {**dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*] | **notification**}

Syntax Description

dynamic	Delete all dynamic MAC addresses.
dynamic address *mac-addr*	(Optional) Delete the specified dynamic MAC address.
dynamic interface *interface-id*	(Optional) Delete all dynamic MAC addresses on the specified physical port or port channel.
dynamic vlan *vlan-id*	(Optional) Delete all dynamic MAC addresses for the specified VLAN. The range is 1 to 4094.
notification	Clear the notifications in the history table and reset the counters.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Examples

This example shows how to remove a specific MAC address from the dynamic address table:

```
Switch# clear mac address-table dynamic address 0008.0070.0007
```

You can verify that the information was deleted by entering the **show mac address-table** privileged EXEC command.

Related Commands

Command	Description
show mac address-table	Displays the MAC address table static and dynamic entries.
snmp trap mac-notification	Enables the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific interface.

clear pagp

Use the **clear pagp** privileged EXEC command to clear Port Aggregation Protocol (PAgP) channel-group information.

clear pagp {*channel-group-number* **counters** | **counters**}

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 48.
counters	Clear traffic counters.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can clear all counters by using the **clear pagp counters** command, or you can clear only the counters for the specified channel group by using the **clear pagp** *channel-group-number* **counters** command.

Examples

This example shows how to clear all channel-group information:

```
Switch# clear pagp counters
```

This example shows how to clear PAgP traffic counters for group 10:

```
Switch# clear pagp 10 counters
```

You can verify that information was deleted by entering the **show pagp** privileged EXEC command.

Related Commands

Command	Description
show pagp	Displays PAgP channel-group information.

clear spanning-tree counters

Use the **clear spanning-tree counters** privileged EXEC command to clear the spanning-tree counters.

clear spanning-tree counters [**interface** *interface-id*]

Syntax Description

interface *interface-id*	(Optional) Clear all spanning-tree counters on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If the *interface-id* is not specified, spanning-tree counters are cleared for all interfaces.

Examples

This example shows how to clear spanning-tree counters for all interfaces:

```
Switch# clear spanning-tree counters
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree state information.

clear spanning-tree detected-protocols

Use the **clear spanning-tree detected-protocols** privileged EXEC command to restart the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.

clear spanning-tree detected-protocols [**interface** *interface-id*]

Syntax Description

interface *interface-id*	(Optional) Restart the protocol migration process on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

A switch running the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol or the Multiple Spanning Tree Protocol (MSTP) supports a built-in protocol migration mechanism that enables it to interoperate with legacy IEEE 802.1D switches. If a rapid-PVST+ switch or an MSTP switch receives a legacy IEEE 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, it sends only IEEE 802.1D BPDUs on that port. A multiple spanning-tree (MST) switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) associated with a different region, or a rapid spanning-tree (RST) BPDU (Version 2).

However, the switch does not automatically revert to the rapid-PVST+ or the MSTP mode if it no longer receives IEEE 802.1D BPDUs because it cannot learn whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Use the **clear spanning-tree detected-protocols** command in this situation.

Examples

This example shows how to restart the protocol migration process on a port:

```
Switch# clear spanning-tree detected-protocols interface gigabitethernet0/1
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree state information.
spanning-tree link-type	Overrides the default link-type setting and enables rapid spanning-tree changes to the forwarding state.

clear vtp counters

Use the **clear vtp counters** privileged EXEC command to clear the VLAN Trunking Protocol (VTP) and pruning counters.

clear vtp counters

Syntax Description

This command has no arguments or keywords.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Examples

This example shows how to clear the VTP counters:

```
Switch# clear vtp counters
```

You can verify that information was deleted by entering the **show vtp counters** privileged EXEC command.

Related Commands

Command	Description
show vtp	Displays general information about the VTP management domain, status, and counters.

cluster commander-address

You do not need to enter this command from a standalone cluster member switch. The cluster command switch automatically provides its MAC address to cluster member switches when these switches join the cluster. The cluster member switch adds this information and other cluster information to its running configuration file. Use the **no** form of this global configuration command from the cluster member switch console port or Ethernet management port to remove the switch from a cluster only during debugging or recovery procedures.

cluster commander-address *mac-address* [**member** *number* **name** *name*]

no cluster commander-address

Syntax Description

mac-address	MAC address of the cluster command switch.
member *number*	(Optional) Number of a configured cluster member switch. The range is 0 to 15.
name *name*	(Optional) Name of the configured cluster up to 31 characters.

Defaults

The switch is not a member of any cluster.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This command is available only on the cluster command switch.

A cluster member can have only one cluster command switch.

The cluster member switch retains the identity of the cluster command switch during a system reload by using the *mac-address* parameter.

You can enter the **no** form on a cluster member switch to remove it from the cluster during debugging or recovery procedures. You would normally use this command from the cluster member switch console port or Ethernet management port only when the member has lost communication with the cluster command switch. With normal switch configuration, we recommend that you remove cluster member switches only by entering the **no cluster member** *n* global configuration command on the cluster command switch.

When a standby cluster command switch becomes active (becomes the cluster command switch), it removes the cluster commander address line from its configuration.

Examples

This is partial sample output from the running configuration of a cluster member.

```
Switch(config)# show running-configuration

<output truncated>

cluster commander-address 00e0.9bc0.a500 member 4 name my_cluster

<output truncated>
```

This example shows how to remove a member from the cluster by using the cluster member console.

```
Switch # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no cluster commander-address
```

You can verify your settings by entering the **show cluster** privileged EXEC command.

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.

cluster discovery hop-count

Use the **cluster discovery hop-count** global configuration command on the cluster command switch to set the hop-count limit for extended discovery of candidate switches. Use the **no** form of this command to return to the default setting.

cluster discovery hop-count *number*

no cluster discovery hop-count

Syntax Description

number	Number of hops from the cluster edge that the cluster command switch limits the discovery of candidates. The range is 1 to 7.

Defaults

The hop count is set to 3.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This command is available only on the cluster command switch. This command does not operate on cluster member switches.

If the hop count is set to 1, it disables extended discovery. The cluster command switch discovers only candidates that are one hop from the edge of the cluster. The edge of the cluster is the point between the last discovered cluster member switch and the first discovered candidate switch.

Examples

This example shows how to set hop count limit to 4. This command is executed on the cluster command switch.

```
Switch(config)# cluster discovery hop-count 4
```

You can verify your setting by entering the **show cluster** privileged EXEC command.

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show cluster candidates	Displays a list of candidate switches.

cluster enable

Use the **cluster enable** global configuration command on a command-capable switch to enable it as the cluster command switch, assign a cluster name, and to optionally assign a member number to it. Use the **no** form of the command to remove all members and to make the cluster command switch a candidate switch.

cluster enable *name* [*command-switch-member-number*]

no cluster enable

Syntax Description

name	Name of the cluster up to 31 characters. Valid characters include only alphanumerics, dashes, and underscores.
command-switch-member-number	(Optional) Assign a member number to the cluster command switch of the cluster. The range is 0 to 15.

Defaults

The switch is not a cluster command switch.

No cluster name is defined.

The member number is 0 when the switch is the cluster command switch.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Enter this command on any command-capable switch that is not part of any cluster. This command fails if a device is already configured as a member of the cluster.

You must name the cluster when you enable the cluster command switch. If the switch is already configured as the cluster command switch, this command changes the cluster name if it is different from the previous cluster name.

Examples

This example shows how to enable the cluster command switch, name the cluster, and set the cluster command switch member number to 4.

```
Switch(config)# cluster enable Engineering-IDF4 4
```

You can verify your setting by entering the **show cluster** privileged EXEC command on the cluster command switch.

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.

cluster holdtime

Use the **cluster holdtime** global configuration command on the cluster command switch to set the duration in seconds before a switch (either the command or cluster member switch) declares the other switch down after not receiving heartbeat messages. Use the **no** form of this command to set the duration to the default value.

cluster holdtime *holdtime-in-secs*

no cluster holdtime

Syntax Description

holdtime-in-secs	Duration in seconds before a switch (either a command or cluster member switch) declares the other switch down. The range is 1 to 300 seconds.

Defaults

The default holdtime is 80 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Enter this command with the **cluster timer** global configuration command only on the cluster command switch. The cluster command switch propagates the values to all its cluster members so that the setting is consistent among all switches in the cluster.

The holdtime is typically set as a multiple of the interval timer (**cluster timer**). For example, it takes (holdtime-in-secs divided by the interval-in-secs) number of heartbeat messages to be missed in a row to declare a switch down.

Examples

This example shows how to change the interval timer and the duration on the cluster command switch.

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

You can verify your settings by entering the **show cluster** privileged EXEC command.

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.

cluster member

Use the **cluster member** global configuration command on the cluster command switch to add candidates to a cluster. Use the **no** form of the command to remove members from the cluster.

cluster member [*n*] **mac-address** *H.H.H*

no cluster member *n*

Syntax Description

n	The number that identifies a cluster member. The range is 0 to 15.
mac-address *H.H.H*	MAC address of the cluster member switch in hexadecimal format.

Defaults

A newly enabled cluster command switch has no associated cluster members.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Enter this command only on the cluster command switch to add a candidate to or remove a member from the cluster. If you enter this command on a switch other than the cluster command switch, the switch rejects the command and displays an error message.

You must enter a member number to remove a switch from the cluster. However, you do not need to enter a member number to add a switch to the cluster. The cluster command switch selects the next available member number and assigns it to the switch that is joining the cluster.

You must enter the enable password of the candidate switch for authentication when it joins the cluster. The password is not saved in the running or startup configuration. After a candidate switch becomes a member of the cluster, its password becomes the same as the cluster command-switch password.

If a switch does not have a configured hostname, the cluster command switch appends a member number to the cluster command-switch hostname and assigns it to the cluster member switch.

If you do not specify a VLAN ID, the cluster command switch automatically chooses a VLAN and adds the candidate to the cluster.

Examples

This example shows how to add a switch as member 2 with MAC address 00E0.1E00.2222 and the password *key* to a cluster. The cluster command switch adds the candidate to the cluster through VLAN 3.

```
Switch(config)# cluster member 2 mac-address 00E0.1E00.2222 password key vlan 3
```

This example shows how to add a switch with MAC address 00E0.1E00.3333 to the cluster. This switch does not have a password. The cluster command switch selects the next available member number and assigns it to the switch that is joining the cluster.

```
Switch(config)# cluster member mac-address 00E0.1E00.3333
```

You can verify your settings by entering the **show cluster members** privileged EXEC command on the cluster command switch.

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show cluster candidates	Displays a list of candidate switches.
show cluster members	Displays information about the cluster members.

cluster outside-interface

Use the **cluster outside-interface** global configuration command on the a cluster command switch to configure the outside interface for cluster Network Address Translation (NAT) so that a member without an IP address can communicate with devices outside the cluster. Use the **no** form of this command to return to the default setting.

cluster outside-interface *interface-id*

no cluster outside-interface

Syntax Description

interface-id	Interface to serve as the outside interface. Valid interfaces include physical interfaces, port-channels, or VLANs. The port-channel range is 1 to 48. The VLAN range is 1 to 4094.

Defaults

The default outside interface is automatically selected by the cluster command switch.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Enter this command only on the cluster command switch. If you enter this command on a cluster member switch, an error message appears.

Examples

This example shows how to set the outside interface to VLAN 1:

```
Switch(config)# cluster outside-interface vlan 1
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.

cluster run

Use the **cluster run** global configuration command to enable clustering on a switch. Use the **no** form of this command to disable clustering on a switch.

cluster run

no cluster run

Syntax Description

This command has no arguments or keywords.

Defaults

Clustering is enabled on all switches.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When you enter the **no cluster run** command on a cluster command switch, the cluster command switch is disabled. Clustering is disabled, and the switch cannot become a candidate switch.

When you enter the **no cluster run** command on a cluster member switch, it is removed from the cluster. Clustering is disabled, and the switch cannot become a candidate switch.

When you enter the **no cluster run** command on a switch that is not part of a cluster, clustering is disabled on this switch. This switch cannot then become a candidate switch.

Examples

This example shows how to disable clustering on the cluster command switch:

```
Switch(config)# no cluster run
```

You can verify your setting by entering the **show cluster** privileged EXEC command.

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.

cluster timer

Use the **cluster timer** global configuration command on the a cluster command switch to set the interval in seconds between heartbeat messages. Use the **no** form of this command to set the interval to the default value.

cluster timer *interval-in-secs*

no cluster timer

Syntax Description

interval-in-secs	Interval in seconds between heartbeat messages. The range is 1 to 300 seconds.

Defaults

The interval is 8 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(46)EY	This command was introduced.

Usage Guidelines

Enter this command with the **cluster holdtime** global configuration command only on the cluster command switch. The cluster command switch propagates the values to all its cluster members so that the setting is consistent among all switches in the cluster.

The holdtime is typically set as a multiple of the heartbeat interval timer (**cluster timer**). For example, it takes (holdtime-in-secs divided by the interval-in-secs) number of heartbeat messages to be missed in a row to declare a switch down.

Examples

This example shows how to change the heartbeat interval timer and the duration on the cluster command switch:

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

You can verify your settings by entering the **show cluster** privileged EXEC command.

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.

copy logging onboard

Use the **copy logging onboard** privileged EXEC command to copy on-board failure logging (OBFL) data to the local network or a specific file system.

copy logging onboard *destination*

Syntax Description

destination	Specify the location on the local network or file system to which the system messages are copied. For *destination,* specify *t*he destination on the local or network file system and the filename. These options are supported: • The syntax for the local flash file system: **flash**[*number*]**:/***filename* • The syntax for the FTP: **ftp://***username***:***password***@***host***/***filename* • The syntax for an HTTP server: **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[*/directory*]*/filename* • The syntax for the NVRAM: **nvram:/***filename* • The syntax for the null file system: **null:/***filename* • The syntax for the Remote Copy Protocol (RCP): **rcp://***username***@***host***/***filename* • The syntax for the switch file system: **system:***filename* • The syntax for the temporary file system: **tmpsys:/***filename* • The syntax for the TFTP: **tftp:**[[*//location*]*/directory*]*/filename*

Defaults

This command has no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

For information about OBFL, see the **hw-module** command.

Examples

This example shows how to copy the OBFL data messages to the *obfl_file* file on the flash file system:

```
Switch# copy logging onboard flash:obfl_file
OBFL copy successful
Switch#
```

Related Commands

Command	Description
hw-module module [*switch-number*] **logging onboard**	Enables OBFL.
onboard	Displays OBFL information.

define interface-range

Use the **define interface-range** global configuration command to create an interface-range macro. Use the **no** form of this command to delete the defined macro.

define interface-range *macro-name interface-range*

no define interface-range *macro-name interface-range*

Syntax Description

macro-name	Name of the interface-range macro; up to 32 characters.
interface-range	Interface range; for valid values for interface ranges, see "Usage Guidelines."

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The macro name is a 32-character maximum character string.

A macro can contain up to five ranges.

All interfaces in a range must be the same type; that is, all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs, but you can combine multiple interface types in a macro.

When entering the *interface-range*, use this format:

- *type* {*first-interface*} - {*last-interface*}
- You must add a space between the first interface number and the hyphen when entering an *interface-range*. For example, **gigabitethernet 0/1 - 2** is a valid range; **gigabitethernet0/1-2** is not a valid range

Valid values for *type* and *interface*:

- **vlan** *vlan-id - vlan-ID*, where the VLAN ID is 1 to 4094

  VLAN interfaces must have been configured with the **interface vlan** command (the **show running-config** privileged EXEC command displays the configured VLAN interfaces). VLAN interfaces not displayed by the **show running-config** command cannot be used in *interface-ranges.*
- **port-channel** *port-channel-number*, where *port-channel-number* is from 1 to 48
- **gigabitethernet** module/{*first port*} - {*last port*}
- **tengigabitethernet** module/{*first port*} - {*last port*}

For physical interfaces:

- module is always 0.
- the range is *type* **0**/*number* - *number* (for example, **gigabitethernet 0/1 - 2**).

When you define a range, you must enter a space before the hyphen (-), for example:

gigabitethernet0/1 - 2

You can also enter multiple ranges. When you define multiple ranges, you must enter a space after the first entry before the comma (,). The space after the comma is optional, for example:

gigabitethernet0/3, gigabitethernet0/1 - 2

gigabitethernet0/3 -4, tengigabitethernet0/1 - 2

Examples

This example shows how to create a multiple-interface macro:

```
Switch(config)# define interface-range macro1 gigabitethernet0/1 - 2,
gigabitethernet0/5 - 7, tengigabitethernet0/1 - 2
```

Related Commands

Command	Description
interface range	Executes a command on multiple ports at the same time.
show running-config	Displays the operating configuration.

delete

Use the **delete** privileged EXEC command to delete a file or directory on the flash memory device.

delete [**/force**] [**/recursive**] *filesystem***:***/file-url*

Syntax Description

/force	(Optional) Suppress the prompt that confirms the deletion.
/recursive	(Optional) Delete the named directory and all subdirectories and the files contained in it.
*filesystem***:**	Alias for a flash file system. The syntax for the local flash file system: **flash:**
/file-url	The path (directory) and filename to delete.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If you use the **/force** keyword, you are prompted once at the beginning of the deletion process to confirm the deletion.

If you use the **/recursive** keyword without the **/force** keyword, you are prompted to confirm the deletion of every file.

The prompting behavior depends on the setting of the **file prompt** global configuration command. By default, the switch prompts for confirmation on destructive file operations. For more information about this command, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*.

Examples

This example shows how to remove the directory that contains the old software image after a successful download of a new image:

```
Switch# delete /force /recursive flash:/old-image
```

You can verify that the directory was removed by entering the **dir** *filesystem***:** privileged EXEC command.

Related Commands

Command	Description
archive download-sw	Downloads a new image to the switch and overwrites or keeps the existing image.

diagnostic monitor

Use the **diagnostic monitor** global configuration command to configure health-monitoring diagnostic testing. Use the **no** form of this command to disable testing and to return to the default settings.

diagnostic monitor interval test {*name* | *test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds day*

diagnostic monitor test {*name* | *test-id* | *test-id-range* | **all**}

diagnostic monitor syslog

diagnostic monitor threshold test {*name* | *test-id* | *test-id-range* | **all**} **failure count** *count*

no diagnostic monitor interval test {*name* | *test-id* | *test-id-range* | **all**}

no diagnostic monitor test {*name* | *test-id* | *test-id-range* | **all**}

no diagnostic monitor syslog

no diagnostic monitor threshold test {*name* | *test-id* | *test-id-range* | **all**} **failure count** *count*

Syntax Description

interval	Configure the interval between tests.
test	Specify the tests to be run.
name	Specify the name of the test. For more information, see the “Usage Guidelines” section.
test-id	Specify the ID number of the test. The range is from 1 to 7. For more information, see the “Usage Guidelines” section.
test-id-range	Specify more than one test with the range of test ID numbers. For more information, see the “Usage Guidelines” section.
all	Specify all of the diagnostic tests.
hh:mm:ss	Configure the monitoring interval in hours, minutes, and seconds. For formatting information, see the “Usage Guidelines” section.
milliseconds	Configure the monitoring interval in milliseconds (ms). The range is from 0 to 999 ms.
day	Configure the monitoring interval in the number of days. The range is from 0 to 20 days. For formatting information, see the “Usage Guidelines” section.
syslog	Enable the generation of a syslog message when a health-monitoring test fails.
threshold	Configure the failure threshold.
failure **count** *count*	Set the failure threshold count. The range for *count* is from 0 to 99.

Defaults

Monitoring is disabled, and a failure threshold value is not set.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Follow these guidelines when configuring health-monitoring diagnostic testing:

- *name*—Enter the **show diagnostic content** privileged EXEC command to display the test names in the test ID list.
- *test-id*—Enter the **show diagnostic content** command to display the test numbers in the test ID list.
- *test-id-range*—Enter the **show diagnostic content** command to display the test numbers in the test ID list. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).
- *hh*—Enter the hours from 0 to 24.
- *mm*—Enter the minutes from 0 to 60.
- *ss*—Enter the seconds from 0 to 60.
- *milliseconds*—Enter the test time in milliseconds from 0 to 999.
- *day*—Enter the number of days between test from 0 to 20.
- Enter the **diagnostic monitor test 1** command to enable diagnostic monitoring.

You must configure the failure threshold and the interval between tests before enabling diagnostic monitoring.

When entering the **diagnostic monitor switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**} command, you must isolate network traffic by disabling all connected ports, and do not send test packets during the test.

Examples

This example shows how to configure a health-monitoring test:

```
Switch(config)# diagnostic monitor threshold switch 2 test 1 failure count 20
Switch(config)# diagnostic monitor interval switch 2 test 1 12:30:00 750 5
```

Related Commands

Command	Description
show diagnostic	Displays online diagnostic test results.

diagnostic schedule

Use the **diagnostic schedule** global configuration command to configure the diagnostic test schedule. Use the **no** form of this command to remove the schedule.

diagnostic schedule test {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**} {**daily** *hh*:*mm* | **on** *mm dd yyyy hh*:*mm* | **weekly** *day-of-week hh*:*mm*}

no diagnostic schedule test {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**} {**daily** *hh*:*mm* | **on** *mm dd yyyy hh*:*mm* | **weekly** *day-of-week hh*:*mm*}

Syntax Description

test	Specify the tests to be scheduled.
name	Specify the name of the test. For more information, see the "Usage Guidelines" section.
test-id	Specify the ID number of the test. The range is from 1 to 7. For more information, see the "Usage Guidelines" section.
test-id-range	Specify more than one test with the range of test ID numbers. For more information, see the "Usage Guidelines" section.
all	Specify all of the diagnostic tests.
basic	Specify the basic on-demand diagnostic tests.
non-disruptive	Specify the nondisruptive health-monitoring tests.
daily *hh*:*mm*	Specify the daily scheduling of the diagnostic tests. For formatting information, see the "Usage Guidelines" section.
on *mm dd yyyy hh*:*mm*	Specify the scheduling of the diagnostic tests on a specific day and time. For formatting information, see the "Usage Guidelines" section.
weekly *day-of-week hh*:*mm*	Specify the weekly scheduling of the diagnostic tests. For formatting information, see the "Usage Guidelines" section.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Usage Guidelines

Use these guidelines when scheduling testing:

- *name*—Enter the **show diagnostic content** privileged EXEC command to display the test names in the test ID list.
- *test-id*—Enter the **show diagnostic content** command to display the test numbers in the test ID list.
- *test-id-range*—Enter the **show diagnostic content** command to display the test numbers in the test ID list. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).
- *hh*:*mm*—Enter the time as a 2-digit number (for a 24-hour clock) for hours:minutes; the colon (:) is required, such as 12:30.

- For *mm dd yyyy*:
  - *mm*—Spell out the month, such as January, February, and so on, with upper case or lower case characters.
  - *dd*—Enter the day as a 2-digit number, such as 03 or 16.
  - *yyyy*—Enter the year as a 4-digit number, such as 2006.
- *day-of-week*—Spell out the day of the week, such as Monday, Tuesday, and so on, with upper case or lower case characters.

Examples

This example shows how to schedule diagnostic testing for a specific day and time:

```
Switch(config)# diagnostic schedule test 1,2,4-6 on november 3 2006 23:10
```

This example shows how to schedule diagnostic testing to occur weekly at a specific time on a switch:

```
Switch(config)# diagnostic schedule test TestPortAsicMem weekly friday 09:23
```

Related Commands

Command	Description
show diagnostic	Displays online diagnostic test results.

diagnostic start

Use the **diagnostic start** privileged EXEC command to run an online diagnostic test.

diagnostic start test {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**}

Syntax Description

test	Specify the tests to run.
name	Specify the name of a test. For more information, see the "Usage Guidelines" section.
test-id	Specify the ID number of a test. The range is from 1 to 7. For more information, see the "Usage Guidelines" section.
test-id-range	Specify more than one test with the range of test ID numbers. For more information, see the "Usage Guidelines" section.
all	Specify all the diagnostic tests.
basic	Specify the basic on-demand diagnostic tests.
non-disruptive	Specify the nondisruptive health-monitoring tests.

Defaults

This command has no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The switch supports these tests:

```
ID   Test Name [On-Demand Test Attributes]
---  ----------------------------------------
1    TestPortAsicStackPortLoopback    [B*N****]
2    TestPortAsicLoopback             [B*D*R**]
3    TestPortAsicCam                  [B*D*R**]
4    TestPortAsicRingLoopback         [B*D*R**]
5    TestMicRingLoopback              [B*D*R**]
6    TestPortAsicMem                  [B*D*R**]
7    TestInlinePwrCtlr                [B*D*R**]
---  ----------------------------------------
```

When specifying a test name, use the **show diagnostic content** privileged EXEC command to display the test ID list. To specify test 3 by using the test name, enter the **diagnostic start switch** *number* **test TestPortAsicCam** privileged EXEC command.

If specifying more than one test to run, use the *test-id-range* parameter, and enter integers separated by a comma and a hyphen. For example, to specify tests 2, 3, and 4, enter the **diagnostic start switch** *number* **test 2-4** command. To specify tests 1, 3, 4, 5, and 6, enter the **diagnostic start switch** *number* **test 1,3-6** command.

After starting the tests by using the **diagnostic start** command, you cannot stop the testing process.

Examples

This example shows how to start diagnostic test 1 on the switch:

```
Switch# diagnostic start test 1
Switch#
06:27:50: %DIAG-6-TEST_RUNNING: Switch: Running TestPortAsicStackPortLoopback{ID=1} ...
(switch-1)
06:27:51: %DIAG-6-TEST_OK: Switch: TestPortAsicStackPortLoopback{ID=1} has completed
successfully
```

Related Commands

Command	Description
show diagnostic	Displays online diagnostic test results.

duplex

Use the **duplex** interface configuration command to specify the duplex mode of operation for a port. Use the **no** form of this command to return the port to its default value.

duplex {**auto** | **full** | **half**}

no duplex

Syntax Description

auto	Enable automatic duplex configuration; port automatically detects whether it should run in full- or half-duplex mode, depending on the attached device mode.
full	Enable full-duplex mode.
half	Enable half-duplex mode (only for interfaces operating at 10 or 100 Mb/s). You cannot configure half-duplex mode for interfaces operating at 1000 or 10,000 Mb/s.

Defaults

The default is **auto** for Gigabit Ethernet ports.

You cannot configure the duplex mode on 10-Gigabit Ethernet ports; it is always **full**.

The default is **full** for the 100BASE- LX small form-factor pluggable (SFP) modules.

The default is **half** for the 100BASE-FX SFP modules.

Duplex options are not supported on the 1000BASE-*x* (where -*x* is -BX, -CWDM, -LX, -SX, or -ZX) SFP modules.

For information about which SFP modules are supported on your switch, see the product release notes.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

For Gigabit Ethernet ports, setting the port to **auto** has the same effect as specifying **full** if the attached device does not autonegotiate the duplex parameter.

Note Half-duplex mode is supported on Gigabit Ethernet interfaces if the duplex mode is **auto** and the connected device is operating at half duplex. However, you cannot configure these interfaces to operate in half-duplex mode.

Certain ports can be configured to be either full duplex or half duplex. Applicability of this command depends on the device to which the switch is attached.

If both ends of the line support autonegotiation, we highly recommend using the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do use the **auto** setting on the supported side.

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

You can configure the duplex setting when the speed is set to **auto**.

Caution Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

For guidelines on setting the switch speed and duplex parameters, see the "Configuring Interface Characteristics" chapter in the software configuration guide for this release.

Examples

This example shows how to configure an interface for full-duplex operation:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# duplex full
```

You can verify your setting by entering the **show interfaces** privileged EXEC command.

Related Commands

Command	Description
show interfaces	Displays the interface settings on the switch.
speed	Sets the speed on a 10/100 or 10/100/1000 Mb/s interface.

errdisable detect cause

Use the **errdisable detect cause** global configuration command to enable error-disabled detection for a specific cause or all causes. Use the **no** form of this command to disable the error-disabled detection feature.

errdisable detect cause {**all** | **bpduguard** | **dtp-flap** | **gbic-invalid** | **l2ptguard** |**link-flap** | **loopback** | **pagp-flap** | **sfp-config-mismatch** | **small-frame**}

no errdisable detect cause {**all** | **bpduguard** |**dtp-flap** | **gbic-invalid** | **l2ptguard** |**link-flap** | **loopback** | **pagp-flap** | **sfp-config-mismatch** | **small-frame**}

For the BPDU guard feature, you can use this command to globally configure the switch to shut down just the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

When the per-VLAN error-disable feature is turned off and a BPDU guard violation occurs, the entire port is disabled. Use the **no** form of this command to disable the per-VLAN error-disable feature.

errdisable detect cause bpduguard shutdown vlan

no errdisable detect cause bpduguard shutdown vlan

Syntax Description

all	Enable error detection for all error-disabled causes.
bpduguard shutdown vlan	Enable per-VLAN error-disable for BPDU guard.
dtp-flap	Enable error detection for the Dynamic Trunking Protocol (DTP) flapping.
gbic-invalid	Enable error detection for an invalid Gigabit Interface Converter (GBIC) module. **Note** This error refers to an invalid small form-factor pluggable (SFP) module.
l2ptguard	Enable error detection for a Layer 2 protocol-tunnel error-disabled cause.
link-flap	Enable error detection for link-state flapping.
loopback	Enable error detection for detected loopbacks.
pagp-flap	Enable error detection for the Port Aggregation Protocol (PAgP) flap error-disabled cause.
sfp-config-mismatch	Enable error detection on an SFP configuration mismatch.
small-frame	See the **errdisable detect cause small-frame** command.

Command Default

Detection is enabled for all causes. All causes, except for per-VLAN error disabling**,** are configured to shut down the entire port.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

A cause (**link-flap**, **dhcp-rate-limit**, and so forth) is the reason for the error-disabled state. When a cause is detected on an interface, the interface is placed in an error-disabled state, an operational state that is similar to a link-down state.

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the BPDU guard feature, you can configure the switch to shut down just the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

If you set a recovery mechanism for the cause by entering the **errdisable recovery** global configuration command for the cause, the interface is brought out of the error-disabled state and allowed to retry the operation when all causes have timed out. If you do not set a recovery mechanism, you must enter the **shutdown** and then the **no shutdown** commands to manually recover an interface from the error-disabled state.

Examples

This example shows how to enable error-disabled detection for the link-flap error-disabled cause:

```
Switch(config)# errdisable detect cause link-flap
```

This command shows how to globally configure BPDU guard for per-VLAN error disable:

```
switch(config)# errdisable detect cause bpduguard shutdown vlan
```

You can verify your setting by entering the **show errdisable detect** privileged EXEC command.

Related Commands

Command	Description
show errdisable detect	Displays error-disabled detection information.
show interfaces status err-disabled	Displays interface status or a list of interfaces in the error-disabled state.
clear errdisable interface	Clears the error-disabled state from a port or VLAN that was error disabled by the per-VLAN error disable feature.

errdisable detect cause small-frame

Use the **errdisable detect cause small-frame** global configuration command to allow any switch port to be error disabled if incoming VLAN-tagged packets are small frames (67 bytes or less) and arrive at the minimum configured rate (the threshold). Use the **no** form of this command to return to the default setting.

errdisable detect cause small-frame

no errdisable detect cause small-frame

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This command globally enables the small-frame arrival feature. Use the **small violation-rate** interface configuration command to set the threshold for each port.

You can configure the port to be automatically re-enabled by using the **errdisable recovery cause small-frame** global configuration command. You configure the recovery time by using the **errdisable recovery interval** *interval* global configuration command.

Examples

This example shows how to enable the switch ports to be put into the error-disabled mode if incoming small frames arrive at the configured threshold:

```
Switch(config)# errdisable detect cause small-frame
```

You can verify your setting by entering the **show interfaces** privileged EXEC command.

Related Commands

Command	Description
errdisable recovery cause small-frame	**Enables the recovery timer.**
errdisable recovery interval	Specifies the time to recover from the specified error-disabled state.
show interfaces	Displays the interface settings on the switch, including input and output flow control.
small-frame violation rate	Configures the rate (threshold) for incoming small frames to cause a port to be put into the error-disabled state.

errdisable recovery

Use the **errdisable recovery** global configuration command to configure the recovery mechanism variables. Use the **no** form of this command to return to the default setting.

errdisable recovery {**cause** {**all** | **bpduguard** | **channel-misconfig** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **loopback** | **pagp-flap** | **sfp-mismatch** | **small-frame** | **udld**}} | {**interval** *interval*}

no errdisable recovery {**cause** {**all** | **bpduguard** | **channel-misconfig** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **loopback** | **pagp-flap** | **sfp-mismatch** | **small-frame** | **udld**}}| {**interval** *interval*}

Syntax Description

cause	Enable the error-disabled mechanism to recover from a specific cause.
all	Enable the timer to recover from all error-disabled causes.
bpduguard	Enable the timer to recover from the bridge protocol data unit (BPDU) guard error-disabled state.
channel-misconfig	Enable the timer to recover from the EtherChannel misconfiguration error-disabled state.
dtp-flap	Enable the timer to recover from the Dynamic Trunking Protocol (DTP) flap error-disabled state.
gbic-invalid	Enable the timer to recover from an invalid Gigabit Interface Converter (GBIC) module error-disabled state. **Note** This error refers to an invalid small form-factor pluggable (SFP) error-disabled state.
l2ptguard	Enable the timer to recover from a Layer 2 protocol tunnel error-disabled state.
link-flap	Enable the timer to recover from the link-flap error-disabled state.
loopback	Enable the timer to recover from a loopback error-disabled state.
pagp-flap	Enable the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disabled state.
sfp-config-mismatch	Enable error detection on an SFP configuration mismatch.
small-frame	See the **errdisable recovery cause small-frame** command.
udld	Enable the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.
interval *interval*	Specify the time to recover from the specified error-disabled state. The range is 30 to 86400 seconds. The same interval is applied to all causes. The default interval is 300 seconds. **Note** The error-disabled recovery timer is initialized at a random differential from the configured interval value. The difference between the actual timeout value and the configured value can be up to 15 percent of the configured interval.

Defaults

Recovery is disabled for all causes.

The default recovery interval is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

A cause (**all**, **bpduguard**, and so forth) is defined as the reason that the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in the error-disabled state, an operational state similar to link-down state.

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the BPDU guard and port-security features, you can configure the switch to shut down just the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

If you do not enable the recovery for the cause, the interface stays in the error-disabled state until you enter the **shutdown** and the **no shutdown** interface configuration commands. If you enable the recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out.

Otherwise, you must enter the **shutdown** and then the **no shutdown** commands to manually recover an interface from the error-disabled state.

Examples

This example shows how to enable the recovery timer for the BPDU guard error-disabled cause:

```
Switch(config)# errdisable recovery cause bpduguard
```

This example shows how to set the timer to 500 seconds:

```
Switch(config)# errdisable recovery interval 500
```

You can verify your settings by entering the **show errdisable recovery** privileged EXEC command.

Related Commands

Command	Description
show errdisable recovery	Displays error-disabled recovery timer information.
show interfaces status err-disabled	Displays interface status or a list of interfaces in error-disabled state.
clear errdisable interface	Clears the error-disabled state from a port or VLAN that was error disabled by the per-VLAN error disable feature.

errdisable recovery cause small-frame

Use the **errdisable recovery cause small-frame** global configuration command to enable the recovery timer for ports to be automatically re-enabled after they are error disabled by the arrival of small frames. Use the **no** form of this command to return to the default setting.

errdisable recovery cause small-frame

no errdisable recovery cause small-frame

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This command enables the recovery timer for error-disabled ports. You configure the recovery time by using the errdisable **recovery interval** *interval interface configuration command.*

Examples

This example shows how to set the recovery timer:

```
Switch(config)# errdisable recovery cause small-frame
```

You can verify your setting by entering the **show interfaces** user EXEC command.

Related Commands

Command	Description
errdisable detect cause small-frame	Allows any switch port to be put into the error-disabled state if an incoming frame is smaller than the configured minimum size and arrives at the specified rate (threshold).
show interfaces	Displays the interface settings on the switch, including input and output flow control.
small-frame violation rate	Configures the size for an incoming (small) frame to cause a port to be put into the error-disabled state.

exception crashinfo

Use the **exception crashinfo** global configuration command to configure the switch to create the extended crashinfo file when the Cisco IOS image fails. Use the **no** form of this command to disable this feature.

exception crashinfo

no exception crashinfo

Syntax Description

This command has no arguments or keywords.

Defaults

The switch creates the extended crashinfo file.

Command Modes

Global configuration

Command History

12.2(53)EY	This command was introduced.

Usage Guidelines

The basic crashinfo file includes the Cisco IOS image name and version that failed and a list of the processor registers, and a stack trace. The extended crashinfo file includes additional information that can help determine the cause of the switch failure.

Use the **no exception crashinfo** global configuration command to configure the switch to not create the extended crashinfo file.

Examples

This example shows how to configure the switch to not create the extended crashinfo file:

```
Switch(config)# no exception crashinfo
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.

flowcontrol

Use the **flowcontrol** interface configuration command to set the receive flow-control state for an interface. When flow control **send** is operable and on for a device and it detects any congestion at its end, it notifies the link partner or the remote device of the congestion by sending a pause frame. When flow control **receive** is on for a device and it receives a pause frame, it stops sending any data packets. This prevents any loss of data packets during the congestion period.

Use the **receive off** keywords to disable flow control.

flowcontrol receive {**desired** | **off** | **on**}

Note The switch can receive, but not send, pause frames.

Syntax Description

receive	Set whether the interface can receive flow-control packets from a remote device.
desired	Allow an interface to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.
off	Turn off the ability of an attached device to send flow-control packets to an interface.
on	Allow an interface to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.

Defaults

The default is **flowcontrol receive off**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The switch does not support sending flow-control pause frames.

Note that the **on** and **desired** keywords have the same result.

When you use the **flowcontrol** command to set a port to control traffic rates during congestion, you are setting flow control on a port to one of these conditions:

- **receive on** or **desired**: The port cannot send pause frames, but can operate with an attached device that is required to or is able to send pause frames. The port can receive pause frames.
- **receive off**: Flow control does not operate in either direction. In case of congestion, no indication is given to the link partner, and no pause frames are sent or received by either device.

Table 2-1 shows the flow control results on local and remote ports for a combination of settings. The table assumes that **receive desired** has the same results as using the **receive on** keywords.

Table 2-1 Flow Control Settings and Local and Remote Port Flow Control Resolution

Flow Control Settings		Flow Control Resolution	
Local Device	**Remote Device**	**Local Device**	**Remote Device**
send off/receive on	**send on/receive on**	Receives only	Sends and receives
	send on/receive off	Receives only	Sends only
	send desired/receive on	Receives only	Sends and receives
	send desired/receive off	Receives only	Sends only
	send off/receive on	Receives only	Receives only
	send off/receive off	Does not send or receive	Does not send or receive
send off/receive off	**send on/receive on**	Does not send or receive	Does not send or receive
	send on/receive off	Does not send or receive	Does not send or receive
	send desired/receive on	Does not send or receive	Does not send or receive
	send desired/receive off	Does not send or receive	Does not send or receive
	send off/receive on	Does not send or receive	Does not send or receive
	send off/receive off	Does not send or receive	Does not send or receive

Examples

This example shows how to configure the local port to not support flow control by the remote port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# flowcontrol receive off
```

You can verify your settings by entering the **show interfaces** privileged EXEC command.

Related Commands

Command	Description
show interfaces	Displays the interface settings on the switch, including input and output flow control.

hw-module

Use the **hw-module** global configuration command to enable on-board failure logging (OBFL). Use the **no** form of this command to disable this feature.

hw-module module [*switch-number*] **logging onboard** [**message level** *level*]

no hw-module module [*switch-number*] **logging onboard** [**message level**]

Syntax Description

switch-number	The switch number is always **1**.
message level *level*	(Optional) Specify the severity of the hardware-related messages that are stored in the flash memory. The range is from 1 to 7.

Defaults

OBFL is enabled, and all messages appear.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

We recommend that you keep OBFL enabled and do not erase the data stored in the flash memory.

To ensure that the time stamps in the OBFL data logs are accurate, you should manually set the system clock, or configure it by using Network Time Protocol (NTP).

If you do not enter the **message level** *level* parameter, all the hardware-related messages generated by the switch are stored in the flash memory.

Examples

This example shows how to enable OBFL on a switch and to specify that only severity 1 hardware-related messages are stored in the flash memory of the switch:

```
Switch(config)# hw-module module 1 logging onboard message level 1
```

You can verify your settings by entering the **onboard** privileged EXEC command.

Related Commands

Command	Description
clear logging onboard	Removes the OBFL data in the flash memory.
onboard	Displays OBFL information.

interface port-channel

Use the **interface port-channel** global configuration command to access or create the port-channel logical interface. Use the **no** form of this command to remove the port-channel.

interface port-channel *port-channel-number*

no interface port-channel *port-channel-number*

Syntax Description

port-channel-number	Port-channel number. The range is 1 to 48.

Defaults

No port-channel logical interfaces are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface first before assigning a physical port to a channel group. Instead, you can use the **channel-group** interface configuration command. It automatically creates the port-channel interface when the channel group gets its first physical port. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number,* or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

Only one port channel in a channel group is allowed.

Follow these guidelines when you use the **interface port-channel** command:

- If you want to use the Cisco Discovery Protocol (CDP), you must configure it only on the physical port and not on the port-channel interface.

You can verify your setting by entering the **show running-config** privileged EXEC or **show etherchannel** *channel-group-number* **detail** privileged EXEC command.

For a complete list of configuration guidelines, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

Examples

This example shows how to create a port-channel interface with a port channel number of 5:

```
Switch(config)# interface port-channel 5
```

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
show etherchannel	Displays EtherChannel information for a channel.
show running-config	Displays the operating configuration.

interface range

Use the **interface range** global configuration command to enter interface range configuration mode and to execute a command on multiple ports at the same time. Use the **no** form of this command to remove an interface range.

interface range {*port-range* | **macro** *name*}

no interface range {*port-range* | **macro** *name*}

Syntax Description

port-range	Port range. For a list of valid values for *port-range*, see the "Usage Guidelines" section.
macro *name*	Specify the name of a macro.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When you enter interface range configuration mode, all interface parameters you enter are attributed to all interfaces within the range.

For VLANs, you can use the **interface range** command only on existing VLAN switch virtual interfaces (SVIs). To display VLAN SVIs, enter the **show running-config** privileged EXEC command. VLANs not displayed cannot be used in the **interface range** command. The commands entered under **interface range** command are applied to all existing VLAN SVIs in the range.

All configuration changes made to an interface range are saved to NVRAM, but the interface range itself is not saved to NVRAM.

You can enter the interface range in two ways:

- Specifying up to five interface ranges
- Specifying a previously defined interface-range macro

All interfaces in a range must be the same type; that is, ~~all Fast Ethernet ports,~~ all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs. However, you can define up to five interface ranges with a single command, with each range separated by a comma.

Valid values for *port-range* type and interface:

- **vlan** *vlan-ID - vlan-ID*, where VLAN ID is from 1 to 4094
- **gigabitethernet** module/{*first port*} - {*last port*}, where module is always **0**
- **tengigabitethernet** module/{*first port*} - {*last port*}, where module is always **0**

  For physical interfaces:

  - module is always 0
  - the range is *type* **0/***number - number* (for example, **gigabitethernet0/1 - 2**)
- **port-channel** *port-channel-number - port-channel-number*, where *port-channel-number* is from 1 to 48

Note When you use the **interface range** command with port channels, the first and last port channel number in the range must be active port channels.

When you define a range, you must enter a space between the first entry and the hyphen (-):

```
interface range gigabitethernet0/1 -2
```

When you define multiple ranges, you must still enter a space after the first entry and before the comma (,):

```
interface range gigabitethernet0/1 - 2, gigabitethernet0/1 - 2
```

You cannot specify both a macro and an interface range in the same command.

You can also specify a single interface in *port-range*. The command is then similar to the **interface** *interface-id* global configuration command.

For more information about configuring interface ranges, see the software configuration guide for this release.

Examples

This example shows how to use the **interface range** command to enter interface-range configuration mode to apply commands to two ports:

```
Switch(config)# interface range gigabitethernet0/1 - 2
Switch(config-if-range)#
```

This example shows how to use a port-range macro *macro1* for the same function. The advantage is that you can reuse *macro1* until you delete it.

```
Switch(config)# define interface-range macro1 gigabitethernet0/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)#
```

Related Commands

Command	Description
define interface-range	Creates an interface range macro.
show running-config	Displays the operating configuration.

interface vlan

Use the **interface vlan** global configuration command to create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode. Use the **no** form of this command to delete an SVI.

interface vlan *vlan-id*

no interface vlan *vlan-id*

Syntax Description

vlan-id	VLAN number. The range is 1 to 4094.

Defaults

The default VLAN interface is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

SVIs are created the first time that you enter the **interface vlan** *vlan-id* command for a particular VLAN. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.

Note When you create an SVI, it does not become active until it is associated with a physical port.

If you delete an SVI by entering the **no interface vlan** *vlan-id* command, the deleted interface is no longer visible in the output from the **show interfaces** privileged EXEC command.

Note You cannot delete the VLAN 1 interface.

You can re-instate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but the previous configuration is gone.

The interrelationship between the number of SVIs configured on a switch and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables.

Examples

This example shows how to create a new SVI with VLAN ID 23 and to enter interface configuration mode:

```
Switch(config)# interface vlan 23
Switch(config-if)#
```

You can verify your setting by entering the **show interfaces** and **show interfaces vlan** *vlan-id* privileged EXEC commands.

Related Commands

Command	Description
show interfaces vlan *vlan-id*	Displays the administrative and operational status of all interfaces or the specified VLAN.

ip access-group

Use the **ip access-group** interface configuration command to control access to a Layer 2 interface. Use the **no** form of this command to remove all access groups or the specified access group from the interface.

ip access-group {*access-list-number* | *name*} {**in**}

no ip access-group [*access-list-number* | *name*] {**in**}

Syntax Description

access-list-number	The number of the IP access control list (ACL). The range is 1 to 199 or 1300 to 2699.
name	The name of an IP ACL, specified in the **ip access-list** global configuration command.
in	Specify filtering on inbound packets.

Defaults

No access list is applied to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can apply named or numbered standard or extended IP access lists to an interface. To define an access list by name, use the **ip access-list** global configuration command. To define a numbered access list, use the **access list** global configuration command. You can used numbered standard access lists ranging from 1 to 99 and 1300 to 1999 or extended access lists ranging from 100 to 199 and 2000 to 2699.

These are limitations for applying an access list to Layer 2 interfaces (port ACLs):

- You can only apply ACLs in the inbound direction; the **out** keyword is not supported for Layer 2 interfaces.
- You can only apply one IP ACL per interface.
- Layer 2 interfaces Port ACLs do not support logging; if the **log** keyword is specified in the IP ACL, it is ignored.
- An IP ACL applied to a Layer 2 interface only filters IP packets.

For standard inbound access lists, after the switch receives a packet, it checks the source address of the packet against the access list. IP extended access lists can optionally check other fields in the packet, such as the destination IP address, protocol type, or port numbers. If the access list permits the packet, the switch continues to process the packet. If the access list denies the packet, the switch discards the packet. If the specified access list does not exist, all packets are passed.

Examples

This example shows how to apply IP access list 101 to inbound packets on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 101 in
```

You can verify your settings by entering the **show ip interface, show access-lists,** or **show ip access-lists** privileged EXEC command.

Related Commands

Command	Description
access list	Configures a numbered ACL.
ip access-list	Configures a named ACL.
show access-lists	Displays ACLs configured on the switch.
show ip access-lists	Displays IP ACLs configured on the switch.
show ip interface	Displays information about interface status and configuration.

ip address

Use the **ip address** interface configuration command to set an IP address for the switch or an IP address for each switch virtual interface (SVI) on the switch. Use the **no** form of this command to remove an IP address or to disable IP processing.

ip address *ip-address subnet-mask* [**secondary**]

no ip address [*ip-address subnet-mask*] [**secondary**]

Syntax Description

ip-address	IP address.
subnet-mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Defaults

No IP address is defined.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If you remove the switch IP address through a Telnet session, your connection to the switch will be lost.

Hosts can find subnet masks using the Internet Control Message Protocol (ICMP) Mask Request message. Routers respond to this request with an ICMP Mask Reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the switch detects another host using one of its IP addresses, it will send an error message to the console.

You can use the optional keyword **secondary** to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and ARP requests are handled properly, as are interface routes in the IP routing table.

Note If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

If your switch receives its IP address from a Bootstrap Protocol (BOOTP) or a DHCP server and you remove the switch IP address by using the **no ip address** command, IP processing is disabled, and the BOOTP or the DHCP server cannot reassign the address.

Examples

This example shows how to configure the IP address for the Layer 2 switch on a subnetted network:

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.

ip admission

Use the **ip admission** interface configuration command to enable web authentication. You can also use this command in fallback-profile mode. Use the **no** form of this command to disable web authentication.

ip admission *rule*

no ip admission

Syntax Description

rule	Apply an IP admission rule to the interface.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **ip admission** command applies a web authentication rule to a switch port.

Examples

This example shows how to apply a web authentication rule to a switchport:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip admission rule1
```

Related Commands

Command	Description
flowcontrol	Enable web authentication on a port
ip admission name proxy http	Enable web authentication globally on a switch
show ip admission	Displays information about NAC cached entries or the NAC configuration. For more information, see the *Network Admission Control Software Configuration Guide* on Cisco.com.

ip admission name proxy http

Use the **ip admission name proxy http** global configuration command to enable web authentication. Use the **no** form of this command to disable web authentication.

ip admission name *proxy http*

no ip admission name *proxy htt***p**

Syntax Description

This command has no arguments or keywords.

Defaults

Web authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **ip admission name proxy http** command globally enables web authentication on a switch.

After you enable web authentication on a switch, use the **ip access-group in** and **ip admission** *web-rule* interface configuration commands to enable web authentication on a specific interface.

Examples

This example shows how to configure only web authentication on a switchport:

```
Switch# configure terminal
Switch(config) ip admission name http-rule proxy http
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 101 in
Switch(config-if)# ip admission rule
Switch(config-if)# end
```

Related Commands

Command	Description
flowcontrol	Create a web authentication fallback profile.
ip admission	Enable web authentication on a port
show ip admission	Displays information about NAC cached entries or the NAC configuration. For more information, see the *Network Admission Control Software Configuration Guide* on Cisco.com.

ip igmp filter

Use the **ip igmp filter** interface configuration command to control whether or not all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an Internet Group Management Protocol (IGMP) profile to the interface. Use the **no** form of this command to remove the specified profile from the interface.

ip igmp filter *profile number*

no ip igmp filter

Syntax Description

profile number	The IGMP profile number to be applied. The range is 1 to 4294967295.

Defaults

No IGMP filters are applied.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to ~~routed ports,~~ switch virtual interfaces (SVIs) or ports that belong to an EtherChannel group.

An IGMP profile can be applied to one or more switch port interfaces, but one port can have only one profile applied to it.

Examples

This example shows how to apply IGMP profile 22 to a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp filter 22
```

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

Related Commands

Command	Description
ip igmp profile	Configures the specified IGMP profile number.
show ip igmp profile	Displays the characteristics of the specified IGMP profile.
show running-config interface *interface-id*	Displays the running configuration on the switch interface, including the IGMP profile (if any) that is applied to an interface.

ip igmp max-groups

Use the **ip igmp max-groups** interface configuration command to set the maximum number of Internet Group Management Protocol (IGMP) groups that a Layer 2 interface can join or to configure the IGMP throttling action when the maximum number of entries is in the forwarding table. Use the **no** form of this command to set the maximum back to the default, which is to have no maximum limit, or to return to the default throttling action, which is to drop the report.

ip igmp max-groups {*number* | **action** {**deny** | **replace**}}

no ip igmp max-groups {*number* | **action**}

Syntax Description

number	The maximum number of IGMP groups that an interface can join. The range is 0 to 4294967294. The default is no limit.
action deny	When the maximum number of entries is in the IGMP snooping forwarding table, drop the next IGMP join report. This is the default action.
action replace	When the maximum number of entries is in the IGMP snooping forwarding table, replace the existing group with the new group for which the IGMP report was received.

Defaults

The default maximum number of groups is no limit.

After the switch learns the maximum number of IGMP group entries on an interface, the default throttling action is to drop the next IGMP report that the interface receives and to not add an entry for the IGMP group to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces. You cannot set IGMP maximum groups for ~~routed ports,~~ switch virtual interfaces (SVIs) or ports that belong to an EtherChannel group.

Follow these guidelines when configuring the IGMP throttling action:

- If you configure the throttling action as **deny** and set the maximum group limitation, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out, when the maximum number of entries is in the forwarding table, the switch drops the next IGMP report received on the interface.
- If you configure the throttling action as **replace** and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the switch replaces a randomly selected multicast entry with the received IGMP report.
- When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups** {**deny | replace**} command has no effect.

Examples

This example shows how to limit to 25 the number of IGMP groups that a port can join:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp max-groups 25
```

This example shows how to configure the switch to replace the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the forwarding table:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip igmp max-groups action replace
```

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

Related Commands

Command	Description
show running-config interface *interface-id*	Displays the running configuration on the switch interface, including the maximum number of IGMP groups that an interface can join and the throttling action.

ip igmp profile

Use the **ip igmp profile** global configuration command to create an Internet Group Management Protocol (IGMP) profile and enter IGMP profile configuration mode. From this mode, you can specify the configuration of the IGMP profile to be used for filtering IGMP membership reports from a switchport. Use the **no** form of this command to delete the IGMP profile.

ip igmp profile *profile number*

no ip igmp profile *profile number*

Syntax Description

profile number	The IGMP profile number being configured. The range is 1 to 4294967295.

Defaults

No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When you are in IGMP profile configuration mode, you can create the profile by using these commands:

- **deny**: specifies that matching addresses are denied; this is the default condition.
- **exit**: exits from igmp-profile configuration mode.
- **no**: negates a command or resets to its defaults.
- **permit**: specifies that matching addresses are permitted.
- **range**: specifies a range of IP addresses for the profile. This can be a single IP address or a range with a start and an end address.

  When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.

You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.

Examples

This example shows how to configure IGMP profile 40 that permits the specified range of IP multicast addresses:

```
Switch(config)# ip igmp profile 40
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

You can verify your settings by using the **show ip igmp profile** privileged EXEC command.

Related Commands

Command	Description
ip igmp filter	Applies the IGMP profile to the specified interface.
show ip igmp profile	Displays the characteristics of all IGMP profiles or the specified IGMP profile number.

ip igmp snooping

Use the **ip igmp snooping** global configuration command to globally enable Internet Group Management Protocol (IGMP) snooping on the switch or to enable it on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

ip igmp snooping [**vlan** *vlan-id*]

no ip igmp snooping [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Enable IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.

Defaults

IGMP snooping is globally enabled on the switch.

IGMP snooping is enabled on VLAN interfaces.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When IGMP snooping is enabled globally, it is enabled in all the existing VLAN interfaces. When IGMP snooping is globally disabled, it is disabled on all the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Examples

This example shows how to globally enable IGMP snooping:

```
Switch(config)# ip igmp snooping
```

This example shows how to enable IGMP snooping on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays the snooping configuration.
show ip igmp snooping groups	Displays IGMP snooping multicast information.
show ip igmp snooping mrouter	Displays the IGMP snooping router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier configured on a switch.

ip igmp snooping last-member-query-interval

Use the **ip igmp snooping last-member-query-interval** global configuration command to enable the Internet Group Management Protocol (IGMP) configurable-leave timer globally or on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

ip igmp snooping [**vlan** *vlan-id*] **last-member-query-interval** *time*

no ip igmp snooping [**vlan** *vlan-id*] **last-member-query-interval**

Syntax Descriptiont

vlan *vlan-id*	(Optional) Enable IGMP snooping and the leave timer on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
time	Interval time out in seconds. The range is 100 to 32768 milliseconds.

Defaults

The default timeout setting is 1000 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When IGMP snooping is globally enabled, IGMP snooping is enabled on all the existing VLAN interfaces. When IGMP snooping is globally disabled, IGMP snooping is disabled on all the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Configuring the leave timer on a VLAN overrides the global setting.

The IGMP configurable leave time is only supported on devices running IGMP Version 2.

The configuration is saved in NVRAM.

Examples

This example shows how to globally enable the IGMP leave timer for 2000 milliseconds:

```
Switch(config)# ip igmp snooping last-member-query-interval 2000
```

This example shows how to configure the IGMP leave timer for 3000 milliseconds on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3000
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
ip igmp snooping vlan static	Configures a Layer 2 port as a multicast router port.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	Displays the IGMP snooping configuration.

ip igmp snooping querier

Use the **ip igmp snooping querier** global configuration command to globally enable the Internet Group Management Protocol (IGMP) querier function in Layer 2 networks. Use the command with keywords to enable and configure the IGMP querier feature on a VLAN interface. Use the **no** form of this command to return to the default settings.

ip igmp snooping querier [**vlan** *vlan-id*] [**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** [**count** *count* | **interval** *interval*] | **timer expiry** | **version** *version*]

no ip igmp snooping querier [**vlan** *vlan-id*] [**address | max-response-time | query-interval | tcn query** { **count** *count* | **interval** *interval*} | **timer expiry | version**]

Syntax Description

vlan *vlan-id*	(Optional) Enable IGMP snooping and the IGMP querier function on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
address *ip-address*	(Optional) Specify a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.
max-response-time *response-time*	(Optional) Set the maximum time to wait for an IGMP querier report. The range is 1 to 25 seconds.
query-interval *interval-count*	(Optional) Set the interval between IGMP queriers. The range is 1 to 18000 seconds.
tcn query[count *count* **| interval** *interval*]	(Optional) Set parameters related to Topology Change Notifications (TCNs). The keywords have these meanings: • **count** *count*—Set the number of TCN queries to be executed during the TCN interval time. The range is 1 to 10. • **interval** *interval*—Set the TCN query interval time. The range is 1 to 255.
timer expiry	(Optional) Set the length of time until the IGMP querier expires. The range is 60 to 300 seconds.
version *version*	(Optional) Select the IGMP version number that the querier feature uses. Select 1 or 2.

Defaults

The IGMP snooping querier feature is globally disabled on the switch.

When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast-enabled device.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use this command to enable IGMP snooping to detect the IGMP version and IP address of a device that sends IGMP query messages, which is also called a *querier*.

By default, the IGMP snooping querier is configured to detect devices that use IGMP *Version 2* (IGMPv2) but does not detect clients that are using IGMP *Version 1* (IGMPv1). You can manually configure the **max-response-time** value when devices use IGMPv2. You cannot configure the **max-response-time** when devices use IGMPv1. (The value cannot be configured and is set to zero).

Non-RFC compliant devices running IGMPv1 might reject IGMP general query messages that have a non-zero value as the **max-response-time** value. If you want the devices to accept the IGMP general query messages, configure the IGMP snooping querier to run IGMPv1.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Examples

This example shows how to globally enable the IGMP snooping querier feature:

```
Switch(config)# ip igmp snooping querier
```

This example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

```
Switch(config)# ip igmp snooping querier max-response-time 25
```

This example shows how to set the IGMP snooping querier interval time to 60 seconds:

```
Switch(config)# ip igmp snooping querier query-interval 60
```

This example shows how to set the IGMP snooping querier TCN query count to 25:

```
Switch(config)# ip igmp snooping querier tcn count 25
```

This example shows how to set the IGMP snooping querier timeout to 60 seconds:

```
Switch(config)# ip igmp snooping querier timeout expiry 60
```

This example shows how to set the IGMP snooping querier feature to version 2:

```
Switch(config)# ip igmp snooping querier version 2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays the IGMP snooping configuration.
show ip igmp snooping groups	Displays IGMP snooping multicast information.
show ip igmp snooping mrouter	Displays the IGMP snooping router ports.

ip igmp snooping report-suppression

Use the **ip igmp snooping report-suppression** global configuration command to enable Internet Group Management Protocol (IGMP) report suppression. Use the **no** form of this command to disable IGMP report suppression and to forward all IGMP reports to multicast routers.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Defaults

IGMP report suppression is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP router suppression is enabled (the default), the switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the switch forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression by entering the **no ip igmp snooping report-suppression** command, all IGMP reports are forwarded to all the multicast routers.

Examples

This example shows how to disable report suppression:

```
Switch(config)# no ip igmp snooping report-suppression
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.

ip igmp snooping tcn

Use the **ip igmp snooping tcn** global configuration command to configure the Internet Group Management Protocol (IGMP) Topology Change Notification (TCN) behavior. Use the **no** form of this command to return to the default settings.

ip igmp snooping tcn {**flood query count** *count* | **query solicit**}

no ip igmp snooping tcn {**flood query count** | **query solicit**}

Syntax Description

flood query count *count*	Specify the number of IGMP general queries for which the multicast traffic is flooded. The range is 1 to 10.
query solicit	Send an IGMP leave message (global leave) to speed the process of recovering from the flood mode caused during a TCN event.

Defaults

The TCN flood query count is 2.

The TCN query solicitation is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use **ip igmp snooping tcn flood query count** global configuration command to control the time that multicast traffic is flooded after a TCN event. If you set the TCN flood query count to 1 by using the **ip igmp snooping tcn flood query count** command, the flooding stops after receiving 1 general query. If you set the count to 7, the flooding of multicast traffic due to the TCN event lasts until 7 general queries are received. Groups are relearned based on the general queries received during the TCN event.

Use the **ip igmp snooping tcn query solicit** global configuration command to enable the switch to send the global leave message whether or not it is the spanning-tree root. This command also speeds the process of recovering from the flood mode caused during a TCN event.

Examples

This example shows how to specify 7 as the number of IGMP general queries for which the multicast traffic is flooded:

```
Switch(config)# no ip igmp snooping tcn flood query count 7
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping tcn flood	Specifies flooding on an interface as the IGMP snooping spanning-tree TCN behavior.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.

ip igmp snooping tcn flood

Use the **ip igmp snooping tcn flood** interface configuration command to specify multicast flooding as the Internet Group Management Protocol (IGMP) snooping spanning-tree Topology Change Notification (TCN) behavior. Use the **no** form of this command to disable the multicast flooding.

ip igmp snooping tcn flood

no ip igmp snooping tcn flood

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast flooding is enabled on an interface during a spanning-tree TCN event.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When the switch receives a TCN, multicast traffic is flooded to all the ports until two general queries are received. If the switch has many ports with attached hosts that are subscribed to different multicast groups, the flooding might exceed the capacity of the link and cause packet loss.

You can change the flooding query count by using the **ip igmp snooping tcn flood query count** *count* global configuration command.

Examples

This example shows how to disable the multicast flooding on an interface:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no ip igmp snooping tcn flood
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping tcn	Configures the IGMP TCN behavior on the switch.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.

ip igmp snooping vlan immediate-leave

Use the **ip igmp snooping immediate-leave** global configuration command to enable Internet Group Management Protocol (IGMP) snooping immediate-leave processing on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

ip igmp snooping vlan *vlan-id* **immediate-leave**

no ip igmp snooping vlan *vlan-id* **immediate-leave**

Syntax Description

vlan-id	Enable IGMP snooping and the Immediate-Leave feature on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.

Defaults

IGMP immediate-leave processing is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

You should configure the Immediate- Leave feature only when there is a maximum of one receiver on every port in the VLAN. The configuration is saved in NVRAM.

The Immediate-Leave feature is supported only with IGMP Version 2 hosts.

Examples

This example shows how to enable IGMP immediate-leave processing on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1 immediate-leave
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays the snooping configuration.
show ip igmp snooping groups	Displays IGMP snooping multicast information.
show ip igmp snooping mrouter	Displays the IGMP snooping router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier configured on a switch.

ip igmp snooping vlan static

Use the **ip igmp snooping static** global configuration command to enable Internet Group Management Protocol (IGMP) snooping and to statically add a Layer 2 port as a member of a multicast group. Use the **no** form of this command to remove ports specified as members of a static multicast group.

ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

Syntax Description

vlan-id	Enable IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
ip-address	Add a Layer 2 port as a member of a multicast group with the specified group IP address.
interface *interface-id*	Specify the interface of the member port. The keywords have these meanings: • **gigabitethernet** *interface number*—a Gigabit Ethernet IEEE 802.3z interface. • **tengigabitethernet** *interface number*—a 10-Gigabit Ethernet IEEE 802.3z interface. • **port-channel** *interface number*—a channel interface. The range is 0 to 48.

Defaults

By default, there are no ports statically configured as members of a multicast group.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

Examples

This example shows how to statically configure a host on an interface:

```
Switch(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface gigabitethernet0/1
Configuring port gigabitethernet0/1 on group 0100.5e02.0203
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays the snooping configuration.
show ip igmp snooping groups	Displays IGMP snooping multicast information.
show ip igmp snooping mrouter	Displays the IGMP snooping router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier configured on a switch.

ip ssh

Use the **ip ssh** global configuration command to configure the switch to run Secure Shell (SSH) Version 1 or SSH Version 2. This command is available only when your switch is running the cryptographic (encrypted) software image. Use the **no** form of this command to return to the default setting.

ip ssh version [**1** | **2**]

no ip ssh version [**1** | **2**]

Syntax Description

1	(Optional) Configure the switch to run SSH Version 1 (SSHv1).
2	(Optional) Configure the switch to run SSH Version 2 (SSHv2).

Defaults

The default version is the latest SSH version supported by the SSH client.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If you do not enter this command or if you do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.

The switch supports an SSHv1 or an SSHv2 server. It also supports an SSHv1 client. For more information about the SSH server and the SSH client, see the software configuration guide for this release.

A Rivest, Shamir, and Adelman (RSA) key pair generated by an SSHv1 server can be used by an SSHv2 server and the reverse.

Examples

This example shows how to configure the switch to run SSHv2:

```
Switch(config)# ip ssh version 2
```

You can verify your settings by entering the **show ip ssh** or **show ssh** privileged EXEC command.

Related Commands

Command	Description
show ip ssh	Displays if the SSH server is enabled and displays the version and configuration information for the SSH server.
show ssh	Displays the status of the SSH server.

ipv6 mld snooping

Use the **ipv6 mld snooping** global configuration command without keywords to enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN. Use the **no** form of this command to disable MLD snooping on the switch or the VLAN.

ipv6 mld snooping [**vlan** *vlan-id*]

no ipv6 mld snooping [**vlan** *vlan-id*]

Syntax DescriptionT

vlan *vlan-id*	(Optional) Enable or disable IPv6 MLD snooping on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.

Defaults

MLD snooping is globally disabled on the switch.

MLD snooping is enabled on all VLANs. However, MLD snooping must be globally enabled before VLAN snooping will take place.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When MLD snooping is globally disabled, it is disabled on all the existing VLAN interfaces. When you globally enable MLD snooping, it is enabled on all VLAN interfaces that are in the default state (enabled). VLAN configuration will override global configuration on interfaces on which MLD snooping has been disabled.

If MLD snooping is globally disabled, you cannot enable it on a VLAN. If MLD snooping is globally enabled, you can disable it on individual VLANs.

When the IPv6 multicast router is a Catalyst 6500 switch and you are using extended VLANs (in the range 1006 to 4094), IPv6 MLD snooping must be enabled on the extended VLAN on the Catalyst 6500 switch in order for the Catalyst 2360 switch to receive queries on the VLAN. For normal-range VLANs (1 to 1005), it is not necessary to enable IPv6 MLD snooping on the VLAN on the Catalyst 6500 switch.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples

This example shows how to globally enable MLD snooping:

```
Switch(config)# ipv6 mld snooping
```

This example shows how to disable MLD snooping on a VLAN:

```
Switch(config)# no ipv6 mld snooping vlan 11
```

You can verify your settings by entering the **show ipv6 mld snooping** user EXEC command.

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLD snooping configuration.

ipv6 mld snooping last-listener-query-count

Use the **ipv6 mld snooping last-listener-query-count** global configuration command to configure IP version 6 (IPv6) Multicast Listener Discovery Mulitcast Address Specific Queries (MASQs) or that will be sent before aging out a client. Use the **no** form of this command to reset the query count to the default settings.

ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-count** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-count**

Syntax Description

vlan *vlan-id*	(Optional) Configure last-listener query count on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
integer_value	The range is 1 to 7.

Command Default

The default global count is 2.

The default VLAN count is 0 (the global count is used).

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

In MLD snooping, the IPv6 multicast router periodically sends out queries to hosts belonging to the multicast group. If a host wants to leave a multicast group, it can silently leave or it can respond to the query with a Multicast Listener Done message (equivalent to an IGMP Leave message). When Immediate Leave is not configured (which it should not be if multiple clients for a group exist on the same port), the configured last-listener query count determines the number of MASQs that are sent before an MLD client is aged out.

When the last-listener query count is set for a VLAN, this count overrides the value configured globally.When the VLAN count is not configured (set to the default of 0), the global count is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples

This example shows how to globally set the last-listener query count:

```
Switch(config)# ipv6 mld snooping last-listener-query-count 1
```

This example shows how to set the last-listener query count for VLAN 10:

```
Switch(config)# ipv6 mld snooping vlan 10 last-listener-query-count 3
```

You can verify your settings by entering the **show ipv6 mld snooping** [**vlan** *vlan-id*] user EXEC command.

Related Commands

Command	Description
ipv6 mld snooping last-listener-query-interval	Sets IPv6 MLD snooping last-listener query interval.
show ipv6 mld snooping querier	Displays MLD snooping configuration.

ipv6 mld snooping last-listener-query-interval

Use the **ipv6 mld snooping last-listener-query-interval** global configuration command to configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping last-listener query interval on the switch or on a VLAN. This time interval is the maximum time that a multicast router waits after issuing a Mulitcast Address Specific Query (MASQ) before deleting a port from the multicast group. Use the **no** form of this command to reset the query time to the default settings.

ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-interval** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-interval**

Syntax Description

vlan *vlan-id*	(Optional) Configure last-listener query interval on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
integer_value	Set the time period (in thousands of a second) that a multicast router to wait after issuing a MASQ before deleting a port from the multicast group. The range is 100 to 32,768. The default is 1000 (1 second),

Command Default

The default global query interval (maximum response time) is 1000 (1 second).

The default VLAN query interval (maximum response time) is 0 (the global count is used).

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

In MLD snooping, when the IPv6 multicast router receives an MLD leave message, it sends out queries to hosts belonging to the multicast group. If there are no responses from a port to a MASQ for a length of time, the router deletes the port from the membership database of the multicast address. The last listener query interval is the maximum time that the router waits before deleting a nonresponsive port from the multicast group.

When a VLAN query interval is set, this overrides the global query interval. When the VLAN interval is set at 0, the global value is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples

This example shows how to globally set the last-listener query interval to 2 seconds:

```
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
```

This example shows how to set the last-listener query interval for VLAN 1 to 5.5 seconds:

```
Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 5500
```

You can verify your settings by entering the **show ipv6 MLD snooping** [**vlan** *vlan-id*] user EXEC command.

Related Commands

Command	Description
ipv6 mld snooping last-listener-query-count	Sets IPv6 MLD snooping last-listener query count.
show ipv6 mld snooping querier	Sets IPv6 MLD snooping last-listener query interval.

ipv6 mld snooping listener-message-suppression

Use the **ipv6 mld snooping listener-message-suppression** global configuration command to enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping listener message suppression. Use the **no** form of this command to disable MLD snooping listener message suppression.

ipv6 mld snooping listener-message-suppression

no ipv6 mld snooping listener-message-suppression

Command Default

The default is for MLD snooping listener message suppression to be disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

MLD snooping listener message suppression is equivalent to IGMP snooping report suppression. When enabled, received MLDv1 reports to a group are forwarded to IPv6 multicast routers only once in every report-forward time. This prevents the forwarding of duplicate reports.

Examples

This example shows how to enable MLD snooping listener-message-suppression:

```
Switch(config)# ipv6 mld snooping listener-message-suppression
```

This example shows how to disable MLD snooping listener-message-suppression:

```
Switch(config)# no ipv6 mld snooping listener-message-suppression
```

You can verify your settings by entering the **show ipv6 mld snooping** [**vlan** *vlan-id*] user EXEC command.

Related Commands

Command	Description
ipv6 mld snooping	Enables IPv6 MLD snooping.
show ipv6 mld snooping	Displays MLD snooping configuration.

ipv6 mld snooping robustness-variable

Use the **ipv6 mld snooping robustness-variable** global configuration command to configure the number of IP version 6 (IPv6) Multicast Listener Discovery (MLD) queries that the switch sends before deleting a listener that does not respond, or enter a VLAN ID to configure on a per-VLAN basis. Use the **no** form of this command to reset the variable to the default settings.

ipv6 mld snooping [**vlan** *vlan-id*] **robustness-variable** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **robustness-variable**

Syntax Description

vlan *vlan-id*	(Optional) Configure the robustness variable on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
integer_value	The range is 1 to 3.

Command Default

The default global robustness variable (number of queries before deleting a listener) is 2.

The default VLAN robustness variable (number of queries before aging out a multicast address) is 0, which means that the system uses the global robustness variable for aging out the listener.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Robustness is measured in terms of the number of MLDv1 queries sent with no response before a port is removed from a multicast group. A port is deleted when there are no MLDv1 reports received for the configured number of MLDv1 queries. The global value determines the number of queries that the switch waits before deleting a listener that does not respond and applies to all VLANs that do not have a VLAN value set.

The robustness value configured for a VLAN overrides the global value. If the VLAN robustness value is 0 (the default), the global value is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples

This example shows how to configure the global robustness variable so that the switch sends out three queries before it deletes a listener port that does not respond:

```
Switch(config)# ipv6 mld snooping robustness-variable 3
```

This example shows how to configure the robustness variable for VLAN 1. This value overrides the global configuration for the VLAN:

```
Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 1
```

You can verify your settings by entering the **show ipv6 mld snooping** [**vlan** *vlan-id*] user EXEC command.

Related Commands

Command	Description
ipv6 mld snooping last-listener-query-count	Sets IPv6 MLD snooping last-listener query count.
show ipv6 mld snooping	Displays MLD snooping configuration.

ipv6 mld snooping tcn

Use the **ipv6 mld snooping tcn** global configuration commands to configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) Topology Change Notifications (TCNs). Use the **no** form of the commands to reset the default settings.

ipv6 mld snooping tcn {**flood query count** *integer_value* | **query solicit**}

no ipv6 mld snooping tcn {**flood query count** *integer_value* | **query solicit**}

Syntax Description

flood query count *integer_value*	Set the flood query count, which is the number of queries that are sent before forwarding multicast data to only those ports requesting to receive it. The range is 1 to 10.
query solicit	Enable soliciting of TCN queries.

Command Default

TCN query soliciting is disabled.

When enabled, the default flood query count is 2.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When TCN solicitation is enabled by using the **ipv6 mld snooping tcn query solicit** global configuration command, MLDv1 snooping sets the VLAN to flood all IPv6 multicast traffic with a configured number of MLDv1 queries before it begins sending multicast data only to selected ports. You set this value by using the **ipv6 mld snooping tcn flood query count** global configuration command. The default is to send two queries. The switch also generates MLDv1 global Done messages with valid link-local IPv6 source addresses when the switch becomes the STP root in the VLAN or when it is configured by the user. This is same as done in IGMP snooping.

Examples

This example shows how to enable TCN query soliciting:

```
Switch(config)# ipv6 mld snooping tcn query solicit.
```

This example shows how to set the flood query count to 5:

```
Switch(config)# ipv6 mld snooping tcn flood query count 5.
```

You can verify your settings by entering the **show ipv6 mld snooping** [**vlan** *vlan-id*] user EXEC command.

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLD snooping configuration.

ipv6 mld snooping vlan

Use the **ipv6 mld snooping vlan** global configuration command to configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping parameters on the VLAN interface. Use the **no** form of this command to reset the parameters to the default settings.

ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ipv6-multicast-address* **interface** *interface-id*]

no ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ip-address* **interface** *interface-id*]

Syntax Description

vlan *vlan-id*	Specify a VLAN number. The range is 1 to 1001 and 1006 to 4094.
immediate-leave	(Optional) Enable MLD Immediate-Leave processing on a VLAN interface. Use the **no** form of the command to disable the Immediate Leave feature on the interface.
mrouter interface	(Optional) Configure a multicast router port. The **no** form of the command removes the configuration.
static *ipv6-multicast-address*	(Optional) Configure a multicast group with the specified IPv6 multicast address.
interface *interface-id*	Add a Layer 2 port to the group. The mrouter or static interface can be a physical port or a **port-channel** interface in the range of 1 to 48.

Command Default

MLD snooping Immediate-Leave processing is disabled.

By default, there are no static IPv6 multicast groups.

By default, there are no multicast router ports.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You should only configure the Immediate-Leave feature when there is only one receiver on every port in the VLAN. The configuration is saved in NVRAM.

The **static** keyword is used for configuring the MLD member ports statically.

The configuration and the static ports and groups are saved in NVRAM.

When the IPv6 multicast router is a Catalyst 6500 switch and you are using extended VLANs (in the range 1006 to 4094), IPv6 MLD snooping must be enabled on the extended VLAN on the Catalyst 6500 switch in order for the Catalyst 2360 switch to receive queries on the VLAN. For normal-range VLANs (1 to 1005), it is not necessary to enable IPv6 MLD snooping on the VLAN on the Catalyst 6500 switch.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples

This example shows how to enable MLD Immediate-Leave processing on VLAN 1:

```
Switch(config)# ipv6 mld snooping vlan 1 immediate-leave
```

This example shows how to disable MLD Immediate-Leave processing on VLAN 1:

```
Switch(config)# no ipv6 mld snooping vlan 1 immediate-leave
```

This example shows how to configure a port as a multicast router port:

```
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet0/2
```

This example shows how to configure a static multicast group:

```
Switch(config)# ipv6 mld snooping vlan 2 static FF12::34 interface gigabitethernet0/2
```

You can verify your settings by entering the **show ipv6 mld snooping vlan** *vlan-id* user EXEC command.

Related Commands

Command	Description
ipv6 mld snooping	Enables IPv6 MLD snooping.
ipv6 mld snooping vlan	Configures IPv6 MLD snooping on the VLAN.
show ipv6 mld snooping	Displays IPv6 MLD snooping configuration.

lacp port-priority

Use the **lacp port-priority** interface configuration command to configure the port priority for the Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default setting.

lacp port-priority *priority*

no lacp port-priority

Syntax Description

priority	Port priority for LACP. The range is 1 to 65535.

Defaults

The default is 32768.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **lacp port-priority** interface configuration command determines which ports are bundled and which ports are put in hot-standby mode when there are more than eight ports in an LACP channel group.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.

In port-priority comparisons, a numerically *lower* value has a *higher* priority: When there are more than eight ports in an LACP channel-group, the eight ports with the numerically lowest values (highest priority values) for LACP port priority are bundled into the channel group, and the lower-priority ports are put in hot-standby mode. If two or more ports have the same LACP port priority (for example, they are configured with the default setting of 65535) an internal value for the port number determines the priority.

Note The LACP port priorities are only effective if the ports are on the switch that controls the LACP link. See the **lacp system-priority** global configuration command for determining which switch controls the link.

Use the **show lacp internal** privileged EXEC command to display LACP port priorities and internal port number values.

For information about configuring LACP on physical ports, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

Examples

This example shows how to configure the LACP port priority on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# lacp port-priority 1000
```

You can verify your settings by entering the **show lacp** [*channel-group-number*] **internal** privileged EXEC command.

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
lacp system-priority	Configures the LACP system priority.
show lacp [*channel-group-number*] **internal**	Displays internal information for all channel groups or for the specified channel group.

lacp system-priority

Use the **lacp system-priority** global configuration command to configure the system priority for the Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default setting.

lacp system-priority *priority*

no lacp system-priority

Syntax Description

priority	System priority for LACP. The range is 1 to 65535.

Defaults

The default is 32768.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **lacp system-priority** command determines which switch in an LACP link controls port priorities.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in an LACP channel-group, the switch on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other switch (the noncontrolling end of the link) are ignored.

In priority comparisons, numerically lower values have higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both switches have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the switch MAC address) determines which switch is in control.

The **lacp system-priority** command applies to all LACP EtherChannels on the switch.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).

For more information about configuring LACP on physical ports, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

Examples

This example shows how to set the LACP system priority:

```
Switch(config)# lacp system-priority 20000
```

You can verify your settings by entering the **show lacp sys-id** privileged EXEC command.

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
lacp port-priority	Configures the LACP port priority.
show lacp sys-id	Displays the system identifier that is being used by LACP.

link state group

Use the **link state group** interface configuration command to configure a port as a member of a link-state group. Use the **no** form of this command to remove the port from the link-state group.

link state group [*number*] {**upstream** | **downstream**}

no link state group [*number*] {**upstream** | **downstream**}

Syntax Description

number	(Optional) Specify the link-state group number. The group number can be from 1 to 2. The default is 1.
upstream	Configure a port as an upstream port for a specific link-state group.
downstream	Configure a port as a downstream port for a specific link-state group.

Defaults

The default group is group 1.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **link state group** interface configuration command to configure a port as an upstream or downstream interface for the specified link-state group. If the group number is omitted, the default group number is 1.

To enable link-state tracking, create a *link-state group*, and specify the interfaces that are assigned to the link-state group. An interface can be an aggregation of ports (an EtherChannel), a single physical port in access or trunk mode~~, or a routed port~~. In a link-state group, these interfaces are bundled together. The *downstream interfaces* are bound to the *upstream interfaces*. Interfaces connected to servers are referred to as downstream interfaces, and interfaces connected to distribution switches and network devices are referred to as upstream interfaces.

For more information about the interactions between the downstream and upstream interfaces, see the "Configuring EtherChannels and Link-State Tracking" chapter of the software configuration guide for this release.

Follow these guidelines to avoid configuration problems:

- An interface that is defined as an upstream interface cannot also be defined as a downstream interface in the same or a different link-state group. The reverse is also true.
- An interface cannot be a member of more than one link-state group.
- You can configure only two link-state groups per switch.

Examples

This example shows how to configure the interfaces as **upstream** in group 2:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/11 - 14
Switch(config-if-range)# link state group 2 upstream
Switch(config-if-range)# end
Switch(config-if)# end
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
link state track	Enables a link-state group.
show running-config	Displays the operating configuration.

link state track

Use the **link state track** global configuration command to enable a link-state group. Use the **no** form of this command to disable a link-state group.

link state track [*number*]

no link state track [*number*]

Syntax Description

number	(Optional) Specify the link-state group number. The group number can be from 1 to 2. The default is 1.

Defaults

Link-state tracking is disabled for all groups.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **link state track** global configuration command to enable a link-state group.

Examples

This example shows how enable link-state group 2:

```
Switch(config)# link state track 2
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
link state group	Configures an interface as a member of a link-state group.
show running-config	Displays the operating configuration.

location (global configuration)

Use the **location global configuration** command to configure location information for an endpoint. Use the **no** form of this command to remove the location information.

location {**admin-tag** *string* | **civic-location identifier** *id* | **elin-location** *string* **identifier** *id*}

no location {**admin-tag** *string* | **civic-location identifier** *id* | **elin-location** *string* **identifier** *id*}

Syntax Description

admin-tag	Configure administrative tag or site information.
civic-location	Configure civic location information.
elin-location	Configure emergency location information (ELIN).
identifier id	Specify the ID for the civic location or the elin location. The ID range is 1 to 4095. **Note** The identifier for the civic location in the LLDP-MED TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes.
string	Specify the site or location information in alphanumeric format.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

After entering the **location civic-location identifier** *id* global configuration command, you enter civic location configuration mode. In this mode, you can enter the civic location and the postal location information.

The civic-location identifier must not exceed 250 bytes.

Use the **no lldp med-tlv-select location** information interface configuration command to disable the location TLV. The location TLV is enabled by default. For more information, see the "Configuring LLDP and LLDP-MED" chapter of the software configuration guide for this release.

Examples

This example shows how to configure civic location information on the switch:

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
```

```
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

You can verify your settings by entering the **show location civic-location** privileged EXEC command.

This example shows how to configure the emergency location information location on the switch:

```
Switch (config)# location elin-location 14085553881 identifier 1
```

You can verify your settings by entering the **show location elin** privileged EXEC command.

Related Commands

Command	Description
location (interface configuration)	Configures the location information for an interface.
show location	Displays the location information for an endpoint.

location (interface configuration)

Use the **location interface** command to enter location information for an interface. Use the **no** form of this command to remove the interface location information.

location {**additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id*}

no location {**additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id*}

Syntax Description

additional-location-information	Configure additional information for a location or place.
civic-location-id	Configure global civic location information for an interface.
elin-location-id	Configure emergency location information for an interface.
id	Specify the ID for the civic location or the elin location. The ID range is 1 to 4095. **Note** The identifier for the civic location in the LLDP-MED TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes.
word	Specify a word or phrase that provides additional location information.

Defaults

This command has no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

After entering the **location civic-location-id** *id* interface configuration command, you enter civic location configuration mode. In this mode, you can enter the additional location information.

The civic-location identifier must not exceed 250 bytes.

Examples

These examples show how to enter civic location information for an interface:

```
Switch(config-if)# interface gigabitethernet0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end

Switch(config-if)# interface gigabitethernet0/2
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end
```

You can verify your settings by entering the **show location civic interface** privileged EXEC command.

This example shows how to enter emergency location information for an interface:

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# location elin-location-id 1
Switch(config-if)# end
```

You can verify your settings by entering the **show location elin interface** privileged EXEC command.

Related Commands

Command	Description
location (global configuration)	Configures the location information for an endpoint.
show location	Displays the location information for an endpoint.

logging file

Use the **logging file** global configuration command to set logging file parameters. Use the **no** form of this command to return to the default setting.

logging file *filesystem*:*filename* [*max-file-size* | **nomax** [*min-file-size*]] [*severity-level-number* | *type*]

no logging file *filesystem*:*filename* [*severity-level-number* | *type*]

Syntax Description

filesystem:*filename*	Alias for a flash file system. Contains the path and name of the file that contains the log messages. The syntax for the local flash file system: **flash:**
max-file-size	(Optional) Specify the maximum logging file size. The range is 4096 to 2147483647.
nomax	(Optional) Specify the maximum file size of 2147483647.
min-file-size	(Optional) Specify the minimum logging file size. The range is 1024 to 2147483647.
severity-level-number	(Optional) Specify the logging severity level. The range is 0 to 7. See the *type* option for the meaning of each level.
type	(Optional) Specify the logging type. These keywords are valid: • **emergencies**—System is unusable (severity 0). • **alerts**—Immediate action needed (severity 1). • **critical**—Critical conditions (severity 2). • **errors**—Error conditions (severity 3). • **warnings**—Warning conditions (severity 4). • **notifications**—Normal but significant messages (severity 5). • **informational**—Information messages (severity 6). • **debugging**—Debugging messages (severity 7).

Defaults

The minimum file size is 2048 bytes; the maximum file size is 4096 bytes.

The default severity level is 7 (**debugging** messages and numerically lower levels).

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The log file is stored in ASCII text format in an internal buffer on the switch. You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. If the switch fails, the log is lost unless you had previously saved it to flash memory by using the **logging file flash:***filename* global configuration command.

After saving the log to flash memory by using the **logging file flash:***filename* global configuration command, you can use the **more flash:***filename* privileged EXEC command to display its contents.

The command rejects the minimum file size if it is greater than the maximum file size minus 1024; the minimum file size then becomes the maximum file size minus 1024.

Specifying a *level* causes messages at that level and numerically lower levels to be displayed.

Examples

This example shows how to save informational log messages to a file in flash memory:

```
Switch(config)# logging file flash:logfile informational
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.

mac address-table aging-time

Use the **mac address-table aging-time** global configuration command to set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. Use the **no** form of this command to return to the default setting. The aging time applies to all VLANs or a specified VLAN.

mac address-table aging-time {**0** | *10-1000000*} [**vlan** *vlan-id*]

no mac address-table aging-time {**0** | *10-1000000*} [**vlan** *vlan-id*]

Syntax Description

0	This value disables aging. Static address entries are never aged or removed from the table.
10-1000000	Aging time in seconds. The range is 10 to 1000000 seconds.
vlan *vlan-id*	(Optional) Specify the VLAN ID to which to apply the aging time. The range is 1 to 4094.

Defaults

The default is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If hosts do not send continuously, increase the aging time to record the dynamic entries for a longer time. Increasing the time can reduce the possibility of flooding when the hosts send again.

If you do not specify a specific VLAN, this command sets the aging time for all VLANs.

Examples

This example shows how to set the aging time to 200 seconds for all VLANs:

```
Switch(config)# mac address-table aging-time 200
```

You can verify your setting by entering the **show mac address-table aging-time** privileged EXEC command.

Related Commands

Command	Description
show mac address-table aging-time	Displays the MAC address table aging time for all VLANs or the specified VLAN.

mac address-table static

Use the **mac address-table static** global configuration command to add static addresses to the MAC address table. Use the **no** form of this command to remove static entries from the table.

mac address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

no mac address-table static *mac-addr* **vlan** *vlan-id* [**interface** *interface-id*]

Syntax Description

mac-addr	Destination MAC address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.
vlan *vlan-id*	Specify the VLAN for which the packet with the specified MAC address is received. The range is 1 to 4094.
interface *interface-id*	Interface to which the received packet is forwarded. Valid interfaces include physical ports and port channels.

Defaults

No static addresses are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Examples

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination, the packet is forwarded to the specified interface:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet0/1
```

You can verify your setting by entering the **show mac address-table** privileged EXEC command.

Related Commands

Command	Description
show mac address-table static	Displays static MAC address table entries only.

mac address-table static drop

Use the **mac address-table static drop** global configuration command to enable unicast MAC address filtering and to configure the switch to drop traffic with a specific source or destination MAC address. Use the **no** form of this command to return to the default setting.

mac address-table static *mac-addr* **vlan** *vlan-id* **drop**

no mac address-table static *mac-addr* **vlan** *vlan-id*

Syntax Description

mac-addr	Unicast source or destination MAC address. Packets with this MAC address are dropped.
vlan *vlan-id*	Specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.

Defaults

Unicast MAC address filtering is disabled. The switch does not drop traffic for specific source or destination MAC addresses.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Follow these guidelines when using this feature:

- Multicast MAC addresses, broadcast MAC addresses, and router MAC addresses are not supported. Packets that are forwarded to the CPU are also not supported.
- If you add a unicast MAC address as a static address and configure unicast MAC address filtering, the switch either adds the MAC address as a static address or drops packets with that MAC address, depending on which command was entered last. The second command that you entered overrides the first command.

  For example, if you enter the **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* global configuration command followed by the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** command, the switch drops packets with the specified MAC address as a source or destination.

  If you enter the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** global configuration command followed by the **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* command, the switch adds the MAC address as a static address.

Examples

This example shows how to enable unicast MAC address filtering and to configure the switch to drop packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in VLAN 4 with this MAC address as its source or destination, the packet is dropped:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

This example shows how to disable unicast MAC address filtering:

```
Switch(config)# no mac address-table static c2f3.220a.12f4 vlan 4
```

You can verify your setting by entering the **show mac address-table static** privileged EXEC command.

Related Commands

Command	Description
show mac address-table static	Displays only static MAC address table entries.

match (class-map configuration)

Use the **match** class-map configuration command to define the match criteria to classify traffic. Use the **no** form of this command to remove the match criteria.

match {**access-group** *acl-index-or-name* | **input-interface** *interface-id-list* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}

no match {**access-group** *acl-index-or-name* | **input-interface** *interface-id-list* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}

Syntax Description

access-group *acl-index-or-name*	Number or name of an IP standard or extended access control list (ACL). For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
input-interface *interface-id-list*	Specify the physical ports to which the interface-level class map in a hierarchical policy map applies. This command can only be used in the child-level policy map and must be the only match condition in the child-level policy map. You can specify up to six entries in the list by specifying a port (counts as one entry), a list of ports separated by a space (each port counts as an entry), or a range of ports separated by a hyphen (counts as two entries).
ip dscp *dscp-list*	List of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly-used value.
ip precedence *ip-precedence-list*	List of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly-used value

Defaults

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **match** command is used to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group matching to the Ether Type/Len are supported.

Is above statement correct?

If you enter the **class-map** {**match-all** | **match-any**} *class-map-name* global configuration command, you can enter these **match** commands:

- **match access-group** *acl-name*

Note The ACL must be an extended named ACL.

- **match input-interface** *interface-id-list*
- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

You cannot enter the **match access-group** *acl-index* command.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-all** and **match-any** keywords are equivalent.

For the **match ip dscp** *dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

Use the **input-interface** *interface-id-list* keyword when you are configuring an interface-level class map in a hierarchical policy map. For the *interface-id-list*, you can specify up to six entries.

Examples

This example shows how to create a class map called *class2*, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

This example shows how to create a class map called *class3*, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using *acl1*:

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# no match ip precedence
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
```

This example shows how to specify a list of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet0/1 gigabitethernet0/2
Switch(config-cmap)# exit
```

This example shows how to specify a range of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet0/1 - gigabitethernet0/5
Switch(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map	Displays quality of service (QoS) class maps.

mdix auto

Use the **mdix auto** interface configuration command to enable the automatic medium-dependent interface crossover (auto-MDIX) feature on the interface. When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately. Use the **no** form of this command to disable auto-MDIX.

mdix auto

no mdix auto

Syntax Description

This command has no arguments or keywords.

Defaults

Auto-MDIX is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When you enable auto-MDIX on an interface, you must also set the interface speed and duplex to **auto** so that the feature operates correctly.

When auto-MDIX (and autonegotiation of speed and duplex) is enabled on one or both of connected interfaces, link up occurs, even if the cable type (straight-through or crossover) is incorrect.

Auto-MDIX is supported on all 10/100 and 10/100/1000 Mb/s interfaces and on 10/100/1000BASE-TX small form-factor pluggable (SFP) module interfaces. It is not supported on 1000BASE-SX or -LX SFP module interfaces.

Examples

This example shows how to enable auto-MDIX on a port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

You can verify the operational state of auto-MDIX on the interface by entering the **show controllers ethernet-controller** *interface-id* **phy** privileged EXEC command.

Related Commands

Command	Description
show controllers ethernet-controller *interface-id* **phy**	Displays general information about internal registers of an interface, including the operational state of auto-MDIX.

media-type rj45

Use the **media-type rj45** line configuration command to manually select the RJ-45 console connection for input, whether or not there is a device connected to the USB console port. Use the **no** form of this command to return to the default setting. The USB console takes precedence if devices are connected to both consoles.

media-type rj45

no media-type rj45

Syntax Description

This command has no arguments or keywords.

Defaults

The default is that the switch uses the USB console connector for input.

Command Modes

Line configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The switch has a USB mini-Type B console connector and a USB console connector. Console output displays on devices connected to both connectors, but console input is active on only one input at a time, with the USB connector taking precedence. When you configure the **media-type rj45** line configuration command, USB console operation is disabled and input always remains with the RJ-45 console.

Entering the **no media-type rj45** line configuration command immediately activates the USB console when it is connected to a powered-on device with a terminal emulation application.

Removing the USB connector always enables input from the RJ-45 connector.

Examples

This example configures the switch to always use the RJ-45 console input:

```
Switch(config)# line console 0
Switch(config-line)# media-type rj45
```

This example configures the switch to always use the USB console input if there is a connected powered-on device:

```
Switch(config)# line console 0
Switch(config-line)# no media-type rj45
```

You can verify your setting by entering the **show running config** privileged EXEC command.

Related Commands

Command	Description
usb-inactivity-timeout	Specifies an inactivity timeout for the USB console port.

mls qos

Use the **mls qos** global configuration command to enable quality of service (QoS) for the entire switch. When the **mls qos** command is entered, QoS is enabled with the default parameters on all ports in the system. Use the **no** form of this command to reset all the QoS-related statistics and to disable the QoS features for the entire switch.

mls qos

no mls qos

Syntax Description

This command has no arguments or keywords.

Defaults

QoS is disabled. There is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

When QoS is enabled with the **mls qos** global configuration command and all other QoS settings are set to their defaults, traffic is classified as best effort (the DSCP and CoS value is set to 0) without any policing. No policy maps are configured. The default port trust state on all ports is untrusted. The default ingress and egress queue settings are in effect.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

QoS must be globally enabled to use QoS classification, policing, mark down or drop, queueing, and traffic shaping features. You can create a policy-map and attach it to a port before entering the **mls qos** command. However, until you enter the **mls qos** command, QoS processing is disabled.

Policy-maps and class-maps used to configure QoS are not deleted from the configuration by the **no mls qos** command, but entries corresponding to policy maps are removed from the switch hardware to save system resources. To re-enable QoS with the previous configurations, use the **mls qos** command.

Toggling the QoS status of the switch with this command modifies (reallocates) the sizes of the queues. During the queue size modification, the queue is temporarily shut down during the hardware reconfiguration, and the switch drops newly arrived packets for this queue.

Examples

This example shows how to enable QoS on the switch:

```
Switch(config)# mls qos
```

You can verify your settings by entering the **show mls qos** privileged EXEC command.

Related Commands

Command	Description
show mls qos	Displays QoS information.

mls qos cos

Use the **mls qos cos** interface configuration command to define the default class of service (CoS) value of a port or to assign the default CoS to all incoming packets on the port. Use the **no** form of this command to return to the default setting.

mls qos cos {*default-cos* | **override**}

no mls qos cos {*default-cos* | **override**}

Syntax Description

default-cos	Assign a default CoS value to a port. If packets are untagged, the default CoS value becomes the packet CoS value. The CoS range is 0 to 7.
override	Override the CoS of the incoming packets, and apply the default CoS value on the port to all incoming packets.

Defaults

The default CoS value for a port is 0.

CoS override is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can use the default value to assign a CoS and Differentiated Services Code Point (DSCP) value to all incoming packets that are untagged (if the incoming packet does not have a CoS value). You also can assign a default CoS and DSCP value to all incoming packets by using the **override** keyword.

Use the **override** keyword when all incoming packets on certain ports deserve higher or lower priority than packets entering from other ports. Even if a port is previously set to trust DSCP, CoS, or IP precedence, this command overrides the previously configured trust state, and all the incoming CoS values are assigned the default CoS value configured with the **mls qos cos** command. If an incoming packet is tagged, the CoS value of the packet is modified with the default CoS of the port at the ingress port.

Examples

This example shows how to configure the default port CoS to 4 on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 4
```

This example shows how to assign all the packets entering a port to the default port CoS value of 4 on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos cos 4
Switch(config-if)# mls qos cos override
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface	Displays quality of service (QoS) information.

mls qos queue-set output buffers

Use the **mls qos queue-set output buffers** global configuration command to allocate buffers to a queue-set (four egress queues per port). Use the **no** form of this command to return to the default setting.

mls qos queue-set output *qset-id* **buffers** *allocation1 ... allocation4*

no mls qos queue-set output *qset-id* **buffers**

Syntax Description

qset-id	ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.
allocation1 ... allocation4	Buffer space allocation (percentage) for each queue (four values for queues 1 to 4). For *allocation1*, *allocation3*, and *allocation4*, the range is 0 to 99. For *allocation2*, the range is 1 to 100 (including the CPU buffer). Separate each value with a space.

Defaults

All allocation values are equally mapped among the four queues (25, 25, 25, 25). Each queue has 1/4 of the buffer space.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Specify four allocation values, and separate each with a space.

Allocate buffers according to the importance of the traffic; for example, give a large percentage of the buffer to the queue with the highest-priority traffic.

To configure different classes of traffic with different characteristics, use this command with the **mls qos queue-set output** *qset-id* **threshold** global configuration command.

Note The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Examples

This example shows how to map a port to queue-set 2. It allocates 40 percent of the buffer space to egress queue 1 and 20 percent to egress queues 2, 3, and 4:

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **buffers** or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
radius-server dead-criteria	Maps a port to a queue-set.
show mls qos interface buffers	Displays quality of service (QoS) information.
show mls qos queue-set	Displays egress queue settings for the queue-set.

mls qos queue-set output threshold

Use the **mls qos queue-set output threshold** global configuration command to configure the weighted tail-drop (WTD) thresholds, to guarantee the availability of buffers, and to configure the maximum memory allocation to a queue-set (four egress queues per port). Use the **no** form of this command to return to the default setting.

mls qos queue-set output *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold*

no mls qos queue-set output *qset-id* **threshold** [*queue-id*]

Syntax Description

qset-id	ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.
queue-id	Specific queue in the queue-set on which the command is performed. The range is 1 to 4.
drop-threshold1 *drop-threshold2*	Two WTD thresholds expressed as a percentage of the allocated memory of the queue. The range is 1 to 3200 percent.
reserved-threshold	Amount of memory to be guaranteed (reserved) for the queue and expressed as a percentage of the allocated memory. The range is 1 to 100 percent.
maximum-threshold	Enable a queue in the full condition to get more buffers than are reserved for it. This is the maximum memory the queue can have before the packets are dropped. The range is 1 to 3200 percent.

Defaults

When quality of service (QoS) is enabled, WTD is enabled.

Table 2-2 shows the default WTD threshold settings.

Table 2-2 Default Egress Queue WTD Threshold Settings

Feature	Queue 1	Queue 2	Queue 3	Queue 4
WTD drop threshold 1	100 percent	200 percent	100 percent	100 percent
WTD drop threshold 2	100 percent	200 percent	100 percent	100 percent
Reserved threshold	50 percent	100 percent	50 percent	50 percent
Maximum threshold	400 percent	400 percent	400 percent	400 percent

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **mls qos queue-set output** *qset-id* **buffers** global configuration command to allocate a fixed number of buffers to the four queues in a queue-set.

The drop-threshold percentages can exceed 100 percent and can be up to the maximum (if the maximum threshold exceeds 100 percent).

While buffer ranges allow individual queues in the queue-set to use more of the common pool when available, the maximum number of packets for each queue is still internally limited to 400 percent, or 4 times the allocated number of buffers. One packet can use one 1 or more buffers.

Note The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

The switch uses a buffer allocation scheme to reserve a minimum amount of buffers for each egress queue, to prevent any queue or port from consuming all the buffers and depriving other queues, and to decide whether to grant buffer space to a requesting queue. The switch decides whether the target queue has not consumed more buffers than its reserved amount (under-limit), whether it has consumed all of its maximum buffers (over-limit), and whether the common pool is empty (no free buffers) or not empty (free buffers). If the queue is not over-limit, the switch can allocate buffer space from the reserved pool or from the common pool (if it is not empty). If there are no free buffers in the common pool or if the queue is over-limit, the switch drops the frame.

Examples

This example shows how to map a port to queue-set 2. It configures the drop thresholds for queue 2 to 40 and 60 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory this queue can have before packets are dropped:

```
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **buffers** or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to a queue-set.
radius-server dead-criteria	Maps a port to a queue-set.
show mls qos interface buffers	Displays QoS information.
show mls qos queue-set	Displays egress queue settings for the queue-set.

mls qos srr-queue output cos-map

Use the **mls qos srr-queue output cos-map** global configuration command to map class of service (CoS) values to an egress queue or to map CoS values to a queue and to a threshold ID. Use the **no** form of this command to return to the default setting.

mls qos srr-queue output cos-map queue *queue-id* {*cos1...cos8* | **threshold** *threshold-id cos1...cos8*}

no mls qos srr-queue output cos-map

Syntax Description

queue *queue-id*	Specify a queue number. For *queue-id*, the range is 1 to 4.
cos1...cos8	Map CoS values to an egress queue. For *cos1...cos8*, enter up to eight values, and separate each value with a space. The range is 0 to 7.
threshold *threshold-id cos1...cos8*	Map CoS values to a queue threshold ID. For *threshold-id*, the range is 1 to 3. For *cos1...cos8*, enter up to eight values, and separate each value with a space. The range is 0 to 7.

Defaults

Table 2-3 shows the default CoS output queue threshold map:

Table 2-3 Default Cos Output Queue Threshold Map

CoS Value	Queue ID–Threshold ID
0, 1	2–1
2, 3	3–1
4	4–1
5	1–1
6, 7	4–1

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.

Note The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your quality of service (QoS) solution.

You can assign two weighted tail-drop (WTD) threshold percentages to an egress queue by using the **mls qos queue-set output** *qset-id* **threshold** global configuration command.

You can map each CoS value to a different queue and threshold combination, allowing the frame to follow different behavior.

Examples

This example shows how to map a port to queue-set 1. It maps CoS values 0 to 3 to egress queue 1 and to threshold ID 1. It configures the drop thresholds for queue 1 to 50 and 70 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped.

```
Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# queue-set 1
```

You can verify your settings by entering the **show mls qos maps**, the **show mls qos interface** [*interface-id*] **buffers**, or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos trust	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
radius-server dead-criteria	Maps a port to a queue-set.
show mls qos interface buffers	Displays QoS information.
show mls qos maps	Displays QoS mapping information.
show mls qos queue-set	Displays egress queue settings for the queue-set.

mls qos trust

Use the **mls qos trust** interface configuration command to configure the port trust state. Use the **no** form of this command to return a port to its untrusted state.

mls qos trust [**cos**]

no mls qos trust [**cos**]

Syntax Description

cos	(Optional) Classify an ingress packet by using the packet CoS value. For an untagged packet, use the port default CoS value.

Defaults

The port is not trusted. If no keyword is specified when you enter the command, the default is **dscp**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Packets entering a quality of service (QoS) domain are classified at the edge of the domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain. Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

Examples

This example shows how to configure a port to trust the CoS labels of all traffic received on that port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust cos
```

Related Commands

Command	Description
mls qos cos	Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port.
show mls qos interface	Displays QoS information.

monitor session

Use the **monitor session** global configuration command to start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) source or destination session, to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance), to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, and to limit (filter) SPAN source traffic to specific VLANs. Use the **no** form of this command to remove the SPAN or RSPAN session or to remove source or destination interfaces or filters from the SPAN or RSPAN session. For destination interfaces, the encapsulation options are ignored with the **no** form of the command.

monitor session *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]} | {**remote vlan** *vlan-id*}

no monitor session *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]} | {**remote vlan** *vlan-id*}

monitor session *session_number* **filter vlan** *vlan-id* [**,** | **-**]

monitor session *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]}| {**remote vlan** *vlan-id*}

no monitor session {*session_number* | **all** | **local** | **remote**}

no monitor session *session_number* **filter vlan** *vlan-id* [**,** | **-**]

no monitor session *session_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]}| {**remote vlan** *vlan-id*}

Syntax Description

session_number	Specify the session number identified with the SPAN or RSPAN session. The range is 1 to 66.
destination	Specify the SPAN or RSPAN destination. A destination must be a physical port.
interface *interface-id*	Specify the destination or source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type, module, and port number). For **source interface**, **port channel** is also a valid interface type, and the valid range is 1 to 48.
encapsulation replicate	(Optional) Specify that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). These keywords are valid only for local SPAN. For RSPAN, the RSPAN VLAN ID overwrites the original VLAN ID; therefore, packets are always sent untagged.
ingress	(Optional) Enable ingress traffic forwarding.
dot1q vlan *vlan-id*	Accept incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.
untagged vlan *vlan-id*	Accept incoming packets with untagged encapsulation with the specified VLAN as the default VLAN.

vlan *vlan-id*	When used with only the **ingress** keyword, set default VLAN for ingress traffic.
remote vlan *vlan-id*	Specify the remote VLAN for an RSPAN source or destination session. The range is 2 to 1001 and 1006 to 4094. The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).
,	(Optional) Specify a series of interfaces or VLANs, or separate a range of interfaces or VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specify a range of interfaces or VLANs. Enter a space before and after the hyphen.
filter vlan *vlan-id*	Specify a list of VLANs as filters on trunk source ports to limit SPAN source traffic to specific VLANs. The *vlan-id* range is 1 to 4094.
source	Specify the SPAN or RSPAN source. A source can be a physical port, a port channel, or a VLAN.
both, rx, tx	(Optional) Specify the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.
source vlan *vlan-id*	Specify the SPAN source interface as a VLAN ID. The range is 1 to 4094.
all, **local**, **remote**	Specify **all**, **local**, or **remote** with the **no monitor session** command to clear all SPAN and RSPAN, all local SPAN, or all RSPAN sessions.

Defaults

No monitor sessions are configured.

On a source interface, the default is to monitor both received and transmitted traffic.

On a trunk interface used as a source port, all VLANs are monitored.

If **encapsulation replicate** is not specified on a local SPAN destination port, packets are sent in native form with no encapsulation tag.

Ingress forwarding is disabled on destination ports.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Traffic that enters or leaves source ports or source VLANs can be monitored by using SPAN or RSPAN. Traffic routed to source ports or source VLANs cannot be monitored.

You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch.

You can have a maximum of 64 destination ports on a switch.

Each session can include multiple ingress or egress source ports or VLANs, but you cannot combine source ports and source VLANs in a single session. Each session can include multiple destination ports.

When you use VLAN-based SPAN (VSPAN) to analyze network traffic in a VLAN or set of VLANs, all active ports in the source VLANs become source ports for the SPAN or RSPAN session. Trunk ports are included as source ports for VSPAN, and only packets with the monitored VLAN ID are sent to the destination port.

You can monitor traffic on a single port or VLAN or on a series or range of ports or VLANs. You select a series or range of interfaces or VLANs by using the [**,** | **-**] options.

If you specify a series of VLANs or interfaces, you must enter a space before and after the comma. If you specify a range of VLANs or interfaces, you must enter a space before and after the hyphen (**-**).

EtherChannel ports cannot be configured as SPAN or RSPAN destination ports. A physical port that is a member of an EtherChannel group can be used as a destination port, but it cannot participate in the EtherChannel group while it is as a SPAN destination.

You can monitor individual ports while they participate in an EtherChannel, or you can monitor the entire EtherChannel bundle by specifying the **port-channel** number as the RSPAN source interface.

A port used as a destination port cannot be a SPAN or RSPAN source, nor can a port be a destination port for more than one session at a time.

VLAN filtering refers to analyzing network traffic on a selected set of VLANs on trunk source ports. By default, all VLANs are monitored on trunk source ports. You can use the **monitor session** *session_number* **filter vlan** *vlan-id* command to limit SPAN traffic on trunk source ports to only the specified VLANs.

VLAN monitoring and VLAN filtering are mutually exclusive. If a VLAN is a source, VLAN filtering cannot be enabled. If VLAN filtering is configured, a VLAN cannot become a source.

If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.

Destination ports can be configured to act in these ways:

- When you enter **monitor session** *session_number* **destination interface** *interface-id* with no other keywords, egress encapsulation is untagged, and ingress forwarding is not enabled.
- When you enter **monitor session** *session_number* **destination interface** *interface-id* **ingress**, egress encapsulation is untagged; ingress encapsulation depends on the keywords that follow—**dot1q**~~**, isl,**~~ or **untagged**.
- When you enter **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate** with no other keywords, egress encapsulation replicates the source interface encapsulation; ingress forwarding is not enabled. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)
- When you enter **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate ingress**, egress encapsulation replicates the source interface encapsulation; ingress encapsulation depends on the keywords that follow—**dot1q** or **untagged**. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)

Examples

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 to destination port 2:

```
Switch(config)# monitor session 1 source interface gigabitethernet0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
```

This example shows how to delete a destination port from an existing local SPAN session:

```
Switch(config)# no monitor session 2 destination gigabitethernet0/2
```

This example shows how to limit SPAN traffic in an existing session only to specific VLANs:

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

This example shows how to configure RSPAN source session 1 to monitor multiple source interfaces and to configure the destination RSPAN VLAN 900.

```
Switch(config)# monitor session 1 source interface gigabitethernet0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

This example shows how to configure an RSPAN destination session 10 in the switch receiving the monitored traffic.

```
Switch(config)# monitor session 10 source remote vlan 900
Switch(config)# monitor session 10 destination interface gigabitethernet0/2
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports IEEE 802.1Q encapsulation. Egress traffic replicates the source; ingress traffic uses IEEE 802.1Q encapsulation.

```
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
dot1q ingress dot1q vlan 5
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support encapsulation. Egress traffic and ingress traffic are untagged.

```
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 ingress
untagged vlan 5
```

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

Related Commands

Command	Description
show monitor	Displays SPAN session information.
show running-config	Displays the operating configuration.

pagp learn-method

Use the **pagp learn-method** interface configuration command to learn the source address of incoming packets received from an EtherChannel port. Use the **no** form of this command to return to the default setting.

pagp learn-method {**aggregation-port** | **physical-port**}

no pagp learn-method

Syntax Description

aggregation-port	Specify address learning on the logical port-channel. The switch sends packets to the source using any of the ports in the EtherChannel. This setting is the default. With aggregate-port learning, it is not important on which physical port the packet arrives.
physical-port	Specify address learning on the physical port within the EtherChannel. The switch sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address.

Defaults

The default is aggregation-port (logical port channel).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The learn method must be configured the same at both ends of the link.

Note The switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner to the switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command and to set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

Examples

This example shows how to set the learning method to learn the address on the physical port within the EtherChannel:

```
Switch(config-if)# pagp learn-method physical-port
```

This example shows how to set the learning method to learn the address on the port-channel within the EtherChannel:

```
Switch(config-if)# pagp learn-method aggregation-port
```

You can verify your settings by entering the **show running-config** privileged EXEC command or the **show pagp** *channel-group-number* **internal** privileged EXEC command.

Related Commands

Command	Description
pagp port-priority	Selects a port over which all traffic through the EtherChannel is sent.
show pagp	Displays PAgP channel-group information.
show running-config	Displays the operating configuration.

pagp port-priority

Use the **pagp port-priority** interface configuration command to select a port over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent. If all unused ports in the EtherChannel are in hot-standby mode, they can be placed into operation if the currently selected port and link fails. Use the **no** form of this command to return to the default setting.

pagp port-priority *priority*

no pagp port-priority

Syntax Description

priority	A priority number ranging from 0 to 255.

Defaults

The default is 128.

Command Modes

Interface configuration

Command History12.

Release	Modification
12.2(53)EY	This command was introduced.

2(46)EY

The physical port with the highest priority that is operational and has membership in the same EtherChannel is the one selected for PAgP transmission.

Note The switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner to the switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command and to set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

Examples

This example shows how to set the port priority to 200:

```
Switch(config-if)# pagp port-priority 200
```

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show pagp** *channel-group-number* **internal** privileged EXEC command.

Related Commands

Command	Description
pagp learn-method	Provides the ability to learn the source address of incoming packets.
show pagp	Displays PAgP channel-group information.
show running-config	Displays the operating configuration.

port-channel load-balance

Use the **port-channel load-balance** global configuration command to set the load-distribution method among the ports in the EtherChannel. Use the **no** form of this command to return to the default setting.

port-channel load-balance {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}

no port-channel load-balance

Syntax Description

dst-ip	Load distribution is based on the destination host IP address.
dst-mac	Load distribution is based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
src-dst-ip	Load distribution is based on the source and destination host IP address.
src-dst-mac	Load distribution is based on the source and destination host MAC address.
src-ip	Load distribution is based on the source host IP address.
src-mac	Load distribution is based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.

Defaults

The default is **src-mac**.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

For information about when to use these forwarding methods, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

Examples

This example shows how to set the load-distribution method to **dst-mac**:

```
Switch(config)# port-channel load-balance dst-mac
```

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show etherchannel load-balance** privileged EXEC command.

Related Commands

Command	Description
interface port-channel	Accesses or creates the port channel.
show etherchannel	Displays EtherChannel information for a channel.
show running-config	Displays the operating configuration.

priority-queue

Use the **priority-queue** interface configuration command to enable the egress expedite queue on a port. Use the **no** form of this command to return to the default setting.

priority-queue out

no priority-queue out

Syntax Description

out	Enable the egress expedite queue.

Defaults

The egress expedite queue is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When you configure the **priority-queue out** command, the shaped round robin (SRR) weight ratios are affected because there is one fewer queue participating in SRR. This means that *weight1* in the **srr-queue bandwidth shape** or the **srr-queue bandwidth shape** interface configuration command is ignored (not used in the ratio calculation). The expedite queue is a priority queue, and it is serviced until empty before the other queues are serviced.

Follow these guidelines when the expedite queue is enabled or the egress queues are serviced based on their SRR weights:

- If the egress expedite queue is enabled, it overrides the SRR shaped and shared weights for queue 1.
- If the egress expedite queue is disabled and the SRR shaped and shared weights are configured, the shaped mode overrides the shared mode for queue 1, and SRR services this queue in shaped mode.
- If the egress expedite queue is disabled and the SRR shaped weights are not configured, SRR services the queue in shared mode.

Examples

This example shows how to enable the egress expedite queue when the SRR weights are configured. The egress expedite queue overrides the configured SRR weights.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
```

This example shows how to disable the egress expedite queue after the SRR shaped and shared weights are configured. The shaped mode overrides the shared mode.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# no priority-queue out
```

You can verify your settings by entering the **show mls qos interface** *interface-id* **queueing** or the **show running-config** privileged EXEC command.

radius-server dead-criteria

Use the **radius-server dead-criteria** global configuration command to configure the conditions that determine when a RADIUS server is considered unavailable or *dead*. Use the **no** form of this command to return to the default settings.

radius-server dead-criteria [**time** *seconds* [**tries** *number*] | **tries** *number*]

no radius-server dead-criteria [**time** *seconds* [**tries** *number*] | **tries** *number*]

Syntax Description

time *seconds*	(Optional) Set the time in seconds during which the switch does not need to get a valid response from the RADIUS server. The range is from 1 to 120 seconds.
tries *number*	(Optional) Set the number of times that the switch does not get a valid response from the RADIUS server before the server is considered unavailable. The range is from 1 to 100.

Defaults

The switch dynamically determines the *seconds* value that is from 10 to 60 seconds.

The switch dynamically determines the *tries* value that is from 10 to 100.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

We recommend that you configure the *seconds* and *number* parameters as follows:

- Use the **radius-server timeout** *seconds* global configuration command to specify the time in seconds during which the switch waits for a RADIUS server to respond before the authentication times out. The switch dynamically determines the default *seconds* value that is from 10 to 60 seconds.
- Use the **radius-server retransmit** *retries* global configuration command to specify the number of times the switch tries to reach the RADIUS servers before considering the servers to be unavailable. The switch dynamically determines the default *tries* value that is from 10 to 100.
- The *seconds* parameter is less than or equal to the number of retransmission attempts times the time in seconds before the authentication times out.
- The *tries* parameter should be the same as the number of retransmission attempts.

Examples

This example shows how to configure 60 as the **time** and 10 as the number of **tries**, the conditions that determine when a RADIUS server is considered unavailable

```
Switch(config)# radius-server dead-criteria time 60 tries 10
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
radius-server retransmit *retries*	Specifies the number of times that the switch tries to reach the RADIUS servers before considering the servers to be unavailable.
radius-server timeout *seconds*	Specifies the time in seconds during which the switch waits for a RADIUS server to respond before the authentication times out.
show running-config	Displays the operating configuration.

radius-server host

Use the **radius-server host** global configuration command to configure the RADIUS server parameters, including the RADIUS accounting and authentication. Use the **no** form of this command to return to the default settings.

radius-server host *ip-address* [**acct-port** *udp-port*] [**auth-port** *udp-port*][**test username** *name* [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**]] [**key** *string*]

no radius-server host *ip-address*

Syntax Description

ip-address	Specify the IP address of the RADIUS server.
acct-port *udp-port*	(Optional) Specify the UDP port for the RADIUS accounting server. The range is from 0 to 65536.
auth-port *udp-port*	(Optional) Specify the UDP port for the RADIUS authentication server. The range is from 0 to 65536.
key *string*	(Optional) Specify the authentication and encryption key for all RADIUS communication between the switch and the RADIUS daemon. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in this command. Leading spaces are ignored, but spaces within and at the end of the key are used. If there are spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
test username *name*	(Optional) Enable automatic server testing of the RADIUS server status, and specify the username to be used.
idle-time *time*	(Optional) Set the interval of time in minutes after which the switch sends test packets to the server. The range is from 1 to 35791 minutes.
ignore-acct-port	(Optional) Disables testing on the RADIUS-server accounting port.
ignore-auth-port	(Optional) Disables testing on the RADIUS-server authentication port.

Defaults

The UDP port for the RADIUS accounting server is 1646.

The UDP port for the RADIUS authentication server is 1645.

Automatic server testing is disabled.

The idle time is 60 minutes (1 hour).

When the automatic testing is enabled, testing occurs on the accounting and authentication UDP ports.

The authentication and encryption key (*string*) is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

We recommend that you configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to nondefault values.

Use the **test username** *name* keywords to enable automatic server testing of the RADIUS server status and to specify the username to be used.

You can configure the authentication and encryption key by using the **radius-server host** *ip-address* **key** *string* or the **radius-server key** {**0** *string* | **7** *string* | *string*} global configuration command. Always configure the key as the last item in this command.

Examples

This example shows how to configure 1500 as the UDP port for the accounting server and 1510 as the UDP port for the authentication server:

```
Switch(config)# radius-server host 1.1.1.1 acct-port 1500 auth-port 1510
```

This example shows how to configure the UDP port for the accounting server and the authentication server, enable automated testing of the RADIUS server status, specify the username to be used, and configure a key string:

```
Switch(config)# radius-server host 1.1.1.2 acct-port 800 auth-port 900 test username
aaafail idle-time 75 key abc123
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
radius-server key {**0** *string* | **7** *string* | *string*}	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
show running-config	Displays the operating configuration.

rcommand

Use the **rcommand** user EXEC command on the cluster command switch to start a Telnet session and to execute commands on a cluster member switch from the cluster command switch. To end the session, enter the **exit** command.

rcommand {*n* | **commander** | **mac-address** *hw-addr*}

Syntax Description

n	Provide the number that identifies a cluster member. The range is 0 to 15.
commander	Provide access to the cluster command switch from a cluster member switch.
mac-address *hw-addr*	MAC address of the cluster member switch.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This command is available only on the cluster command switch.

If the switch is the cluster command switch but the cluster member switch *n* does not exist, an error message appears. To get the switch number, enter the **show cluster members** privileged EXEC command on the cluster command switch.

You can use this command to access a cluster member switch from the cluster command-switch prompt or to access a cluster command switch from the member-switch prompt.

For Catalyst 2350, 2360, 2940, 2950, 2960, 2970, 3550, 3560, 3560-E, 3750, and 3750-E switches, the Telnet session accesses the member-switch command-line interface (CLI) at the same privilege level as on the cluster command switch. For example, if you execute this command at user level on the cluster command switch, the cluster member switch is accessed at user level. If you use this command on the cluster command switch at privileged level, the command accesses the remote device at privileged level. If you use an intermediate enable-level lower than *privileged*, access to the cluster member switch is at user level.

For Catalyst 1900 and 2820 switches running standard edition software, the Telnet session accesses the menu console (the menu-driven interface) if the cluster command switch is at privilege level 15. If the cluster command switch is at privilege level 1, you are prompted for the password before being able to access the menu console. Cluster command switch privilege levels map to the cluster member switches running standard edition software as follows:

- If the cluster command switch privilege level is from 1 to 14, the cluster member switch is accessed at privilege level 1.
- If the cluster command switch privilege level is 15, the cluster member switch is accessed at privilege level 15.

The Catalyst 1900 and 2820 CLI is available only on switches running Enterprise Edition Software.

This command will not work if the vty lines of the cluster command switch have access-class configurations.

You are not prompted for a password because the cluster member switches inherited the password of the cluster command switch when they joined the cluster.

Examples

This example shows how to start a session with member 3. All subsequent commands are directed to member 3 until you enter the **exit** command or close the session.

```
Switch# rcommand 3
Switch-3# show version
Cisco Internet Operating System Software ...
...
Switch-3# exit
Switch#
```

Related Commands

Command	Description
show cluster members	Displays information about the cluster members.

reload

Use the **reload** privileged EXEC command to reload the switch and to put a configuration change into effect.

reload [*LINE* | **at** | **cancel** | **in** | **standby-cpu**]

Syntax Description

LINE	Specify the reason for the reload.
at	Specify the time in hh:mm for the reload to occur.
cancel	Cancel the pending reload.
in	Specify a time interval in mmm or hhh:mm for reloads to occur.
standby-cpu	Reload the standby route processor (RP).

Defaults

Immediately reloads the switch and puts a configuration change into effect.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Examples

This example shows how to reload the switch:

```
Switch(config)# reload
System configuration has been modified. Save? [yes/no]: y
```

Related Commands

Command	Description
rcommand	Accesses a specific cluster member.
show system mtu	Displays the global maximum transmission unit (MTU) or maximum packet size set for the switch.

rmon collection stats

Use the **rmon collection stats** interface configuration command to collect Ethernet group statistics, which include usage statistics about broadcast and multicast packets, and error statistics about cyclic redundancy check (CRC) alignment errors and collisions. Use the **no** form of this command to return to the default setting.

rmon collection stats *index* [**owner** *name*]

no rmon collection stats *index* [**owner** *name*]

Syntax Description

index	Remote Network Monitoring (RMON) collection control index. The range is 1 to 65535.
owner *name*	(Optional) Owner of the RMON collection.

Defaults

The RMON statistics collection is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The RMON statistics collection command is based on hardware counters.

For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > System Management Commands > RMON Commands**.

Examples

This example shows how to collect RMON statistics for the owner *root*:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# rmon collection stats 2 owner root
```

You can verify your setting by entering the **show rmon statistics** privileged EXEC command.

Related Commands

Command	Description
show rmon statistics	Displays RMON statistics.

service password-recovery

Use the **service password-recovery** global configuration command to enable the password-recovery mechanism (the default). This mechanism allows an end user with physical access to the switch to hold down the **Mode** button and interrupt the boot process while the switch is powering up and to assign a new password. Use the **no** form of this command to disable part of the password-recovery functionality. When the password-recovery mechanism is disabled, interrupting the boot process is allowed only if the user agrees to set the system back to the default configuration.

service password-recovery

no service password-recovery

Syntax Description

This command has no arguments or keywords.

Defaults

The password-recovery mechanism is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

As a system administrator, you can use the **no service password-recovery** command to disable some of the functionality of the password recovery feature by allowing an end user to reset a password only by agreeing to return to the default configuration.

To use the password-recovery procedure, a user with physical access to the switch holds down the **Mode** button while the unit powers up and for a second or two after the LED above port 1X turns off. When the button is released, the system continues with initialization.

If the password-recovery mechanism is disabled, this message appears:

```
The password-recovery mechanism has been triggered, but
is currently disabled.  Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.  However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?
```

If the user chooses not to reset the system to the default configuration, the normal boot process continues, as if the **Mode** button had not been pressed. If you choose to reset the system to the default configuration, the configuration file in flash memory is deleted, and the VLAN database file, *flash:vlan.dat* (if present), is deleted.

Note If you use the **no service password-recovery** command to control end user access to passwords, we recommend that you save a copy of the config file in a location away from the switch in case the end user uses the password recovery procedure and sets the system back to default values. Do not keep a backup copy of the config file on the switch.

If the switch is operating in VTP transparent mode, we recommend that you also save a copy of the vlan.dat file in a location away from the switch.

You can verify if password recovery is enabled or disabled by entering the **show version** privileged EXEC command.

Examples

This example shows how to disable password recovery so that a user can only reset a password by agreeing to return to the default configuration.

```
Switch(config)# no service-password recovery
Switch(config)# exit
```

Related Commands

Command	Description
show version	Displays version information for the hardware and firmware.

setup

Use the **setup** privileged EXEC command to configure the switch with its initial configuration.

setup

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When you use the **setup** command, make sure that you have this information:

- IP address and network mask
- Password strategy for your environment
- Whether the switch will be used as the cluster command switch and the cluster name

When you enter the **setup** command, an interactive dialog, called the System Configuration Dialog, appears. It guides you through the configuration process and prompts you for information. The values shown in brackets next to each prompt are the default values last set by using either the **setup** command facility or the **configure** privileged EXEC command.

Help text is provided for each prompt. To access help text, press the question mark (**?**) key at a prompt.

To return to the privileged EXEC prompt without making changes and without running through the entire System Configuration Dialog, press **Ctrl-C**.

When you complete your changes, the setup program shows you the configuration command script that was created during the setup session. You can save the configuration in NVRAM or return to the setup program or the command-line prompt without saving it.

Examples

This is an example of output from the **setup** command:

```
Switch# setup
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.
```

```
Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

Enter host name [Switch]:host-name

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: enable-secret-password

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: enable-password

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: terminal-password

  Configure SNMP Network Management? [no]: yes
  Community string [public]:

Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration

Interface                  IP-Address      OK? Method Status                Protocol
Vlan1                      172.20.135.202  YES NVRAM  up                    up

GigabitEthernet0/1         unassigned      YES unset  up                    up

GigabitEthernet0/2         unassigned      YES unset  up                    down

<output truncated>

Port-channel1              unassigned      YES unset  up                    down

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface vlan1:
Configure IP on this interface? [yes]: yes
IP address for this interface: ip_address
Subnet mask for this interface [255.0.0.0]: subnet_mask

Would you like to enable as a cluster command switch? [yes/no]: yes

Enter cluster name: cluster-name

The following configuration command script was created:

hostname host-name
enable secret 5 $1$LiBw$0Xc1wyT.PXPkuhFwqyhVi0
enable password enable-password
line vty 0 15
password terminal-password
snmp-server community public
!
no ip routing
!
interface GigabitEthernet0/1
no ip address
!
interface GigabitEthernet0/2
no ip address
```

```
!

cluster enable cluster-name
!
end
Use this configuration? [yes/no]: yes
!
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

Enter your selection [2]:
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
show version	Displays version information for the hardware and firmware.

setup express

Use the **setup express** global configuration command to enable Express Setup mode. Use the **no** form of this command to disable Express Setup mode.

setup express

no setup express

Syntax Description

This command has no arguments or keywords.

Defaults

Express Setup is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When Express Setup is enabled on a new (unconfigured) switch, pressing the Mode button for 2 seconds activates Express Setup. You can access the switch through an Ethernet port by using the IP address 10.0.0.1 and then can configure the switch with the web-based Express Setup program or the command-line interface (CLI)-based setup program.

When you press the Mode button for 2 seconds on a configured switch, the LEDs above the Mode button start blinking. If you press the Mode button for a total of 10 seconds, the switch configuration is deleted, and the switch reboots. The switch can then be configured like a new switch, either through the web-based Express Setup program or the CLI-based setup program.

Note As soon as you make any change to the switch configuration (including entering *no* at the beginning of the CLI-based setup program), configuration by Express Setup is no longer available. You can only run Express Setup again by pressing the Mode button for 10 seconds. This deletes the switch configuration and reboots the switch.

If Express Setup is active on the switch, entering the **write memory** or **copy running-configuration startup-configuration** privileged EXEC commands deactivates Express Setup. The IP address 10.0.0.1 is no longer valid on the switch, and your connection using this IP address ends.

The primary purpose of the **no setup express** command is to prevent someone from deleting the switch configuration by pressing the Mode button for 10 seconds.

Examples

This example shows how to enable Express Setup mode:

```
Switch(config)# setup express
```

You can verify that Express Setup mode is enabled by pressing the Mode button:

- On an unconfigured switch, the LEDs above the Mode button turn solid green after 3 seconds.
- On a configured switch, the mode LEDs begin blinking after 2 seconds and turn solid green after 10 seconds.

Caution If you *hold* the Mode button down for a total of 10 seconds, the configuration is deleted, and the switch reboots.

This example shows how to disable Express Setup mode:

```
Switch(config)# no setup express
```

You can verify that Express Setup mode is disabled by pressing the Mode button. The mode LEDs do not turn solid green *or* begin blinking green if Express Setup mode is not enabled on the switch.

Related Commands

Command	Description
show setup express	Displays if Express Setup mode is active.

show access-lists

Use the **show access-lists** privileged EXEC command to display access control lists (ACLs) configured on the switch.

show access-lists [*name* | *number* | **hardware counters** | **ipc**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

name	(Optional) Name of the ACL.
number	(Optional) ACL number. The range is 1 to 2699.
hardware counters	(Optional) Display global hardware ACL statistics for switched and routed packets.
ipc	(Optional) Display Interprocess Communication (IPC) protocol access-list configuration download information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The switch supports only IP standard and extended access lists. Therefore, the allowed numbers are only 1 to 199 and 1300 to 2699.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show access-lists** command:

```
Switch# show access-lists
Standard IP access list 1
    10 permit 1.1.1.1
    20 permit 2.2.2.2
    30 permit any
    40 permit 0.255.255.255, wildcard bits 12.0.0.0
Standard IP access list videowizard_1-1-1-1
    10 permit 1.1.1.1
Standard IP access list videowizard_10-10-10-10
    10 permit 10.10.10.10
Extended IP access list 121
    10 permit ahp host 10.10.10.10 host 20.20.10.10 precedence routine
```

```
Extended IP access list CMP-NAT-ACL
    Dynamic Cluster-HSRP deny   ip any any
    10 deny ip any host 19.19.11.11
    20 deny ip any host 10.11.12.13
    Dynamic Cluster-NAT permit ip any any
    10 permit ip host 10.99.100.128 any
    20 permit ip host 10.46.22.128 any
    30 permit ip host 10.45.101.64 any
    40 permit ip host 10.45.20.64 any
    50 permit ip host 10.213.43.128 any
    60 permit ip host 10.91.28.64 any
    70 permit ip host 10.99.75.128 any
    80 permit ip host 10.38.49.0 any
```

This is an example of output from the **show access-lists hardware counters** command:

```
Switch# show access-lists hardware counters
L2 ACL INPUT Statistics
     Drop:                All frame count: 855
     Drop:                All bytes count: 94143
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 2121
     Forwarded:           All bytes count: 180762
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0

 L3 ACL INPUT Statistics
     Drop:                All frame count: 0
     Drop:                All bytes count: 0
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 13586
     Forwarded:           All bytes count: 1236182
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0

 L2 ACL OUTPUT Statistics
     Drop:                All frame count: 0
     Drop:                All bytes count: 0
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 232983
     Forwarded:           All bytes count: 16825661
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0
```

```
L3 ACL OUTPUT Statistics
    Drop:                All frame count: 0
    Drop:                All bytes count: 0
    Drop And Log:        All frame count: 0
    Drop And Log:        All bytes count: 0
    Bridge Only:         All frame count: 0
    Bridge Only:         All bytes count: 0
    Bridge Only And Log: All frame count: 0
    Bridge Only And Log: All bytes count: 0
    Forwarding To CPU:   All frame count: 0
    Forwarding To CPU:   All bytes count: 0
    Forwarded:           All frame count: 514434
    Forwarded:           All bytes count: 39048748
    Forwarded And Log:   All frame count: 0
    Forwarded And Log:   All bytes count: 0
```

Related Commands

Command	Description
access-list	Configures a standard or extended numbered access list on the switch.
ip access list	Configures a named IP access list on the switch.

show archive status

Use the **show archive status** privileged EXEC command to display the status of a new image being downloaded to a switch with the HTTP or the TFTP protocol.

show archive status [**|** {**begin | exclude | include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If you use the **archive download-sw** privileged EXEC command to download an image to a TFTP server, the output of the **archive download-sw** command shows the status of the download.

If you do not have a TFTP server, you can use Network Assistant or the embedded device manager to download the image by using HTTP. The **show archive status** command shows the progress of the download.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

These are examples of output from the **show archive status** command:

```
Switch# show archive status
IDLE: No upgrade in progress

Switch# show archive status
LOADING: Upgrade in progress

Switch# show archive status
EXTRACT: Extracting the image

Switch# show archive status
VERIFY: Verifying software

Switch# show archive status
RELOAD: Upgrade completed. Reload pending
```

Related Commands

Command	Description
archive download-sw	Downloads a new image from a TFTP server to the switch.

show boot

Use the **show boot** privileged EXEC command to display the settings of the boot environment variables.

show boot [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show boot** command. Table 2-4 describes each field in the display.

```
Switch# show boot
BOOT path-list      : flash:c2360-unversalk9-tar
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : yes
HELPER path-list    :
Auto upgrade        : yes
Auto upgrade path   :
------------------
<output truncated>
```

Table 2-4 show boot Field Descriptions

Field	Description
BOOT path-list	Displays a semicolon separated list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.
Config file	Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
Private Config file	Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
Enable Break	Displays whether a break during booting is enabled or disabled. If it is set to yes, on, or 1, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system is initialized.
Manual Boot	Displays whether the switch automatically or manually boots. If it is set to no or 0, the boot loader attempts to automatically boot up the system. If it is set to anything else, you must manually boot up the switch from the boot loader mode.
Helper path-list	Displays a semicolon separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.

Related Commands

Command	Description
boot config-file	Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
boot enable-break	Enables interrupting the automatic boot process.
boot manual	Enables manually booting the switch during the next boot cycle.
boot private-config-file	Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the private configuration.
boot system	Specifies the Cisco IOS image to load during the next boot cycle.

show class-map

Use the **show class-map** user EXEC command to display quality of service (QoS) class maps, which define the match criteria to classify traffic.

show class-map [*class-map-name*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

class-map-name	(Optional) Display the contents of the specified class map.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show class-map** command:

```
Switch> show class-map
Class Map match-all videowizard_10-10-10-10 (id 2)
   Match access-group name videowizard_10-10-10-10

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all dscp5 (id 3)
   Match ip dscp 5
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
match (class-map configuration)	Defines the match criteria to classify traffic.

show cluster

Use the **show cluster** user EXEC command to display the cluster status and a summary of the cluster to which the switch belongs. This command can be entered on the cluster command switch and cluster member switches.

show cluster [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If you enter this command on a switch that is not a cluster member, the error message `Not a management cluster member` appears.

On a cluster member switch, this command displays the identity of the cluster command switch, the switch member number, and the state of its connectivity with the cluster command switch.

On a cluster command switch, this command displays the cluster name and the total number of members. It also shows the cluster status and time since the status changed. If redundancy is enabled, it displays the primary and secondary command-switch information.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output when the **show cluster** command is entered on the active cluster command switch:

```
Switch> show cluster
Command switch for cluster "Ajang"
        Total number of members:        7
        Status:                         1 members are unreachable
        Time since last status change:  0 days, 0 hours, 2 minutes
        Redundancy:                     Enabled
                Standby command switch: Member 1
                Standby Group:          Ajang_standby
                Standby Group Number:   110
        Heartbeat interval:             8
        Heartbeat hold-time:            80
        Extended discovery hop count:   3
```

This is an example of output when the **show cluster** command is entered on a cluster member switch:

```
Switch1> show cluster
Member switch for cluster "hapuna"
        Member number:                  3
        Management IP address:          192.192.192.192
        Command switch mac address:     0000.0c07.ac14
        Heartbeat interval:             8
        Heartbeat hold-time:            80
```

This is an example of output when the **show cluster** command is entered on a cluster member switch that is configured as the standby cluster command switch:

```
Switch> show cluster
Member switch for cluster "hapuna"
        Member number:                  3 (Standby command switch)
        Management IP address:          192.192.192.192
        Command switch mac address:     0000.0c07.ac14
        Heartbeat interval:             8
        Heartbeat hold-time:            80
```

This is an example of output when the **show cluster** command is entered on the cluster command switch that has lost connectivity with member 1:

```
Switch> show cluster
Command switch for cluster "Ajang"
        Total number of members:        7
        Status:                         1 members are unreachable
        Time since last status change:  0 days, 0 hours, 5 minutes
        Redundancy:                     Disabled
        Heartbeat interval:             8
        Heartbeat hold-time:            80
        Extended discovery hop count:   3
```

This is an example of output when the **show cluster** command is entered on a cluster member switch that has lost connectivity with the cluster command switch:

```
Switch> show cluster
Member switch for cluster "hapuna"
        Member number:                  <UNKNOWN>
        Management IP address:          192.192.192.192
        Command switch mac address:     0000.0c07.ac14
        Heartbeat interval:             8
        Heartbeat hold-time:            80
```

Related Commands

Command	Description
cluster enable	Enables a command-capable switch as the cluster command switch, assigns a cluster name, and optionally assigns a member number to it.
show cluster candidates	Displays a list of candidate switches.
show cluster members	Displays information about the cluster members.

show cluster candidates

Use the **show cluster candidates** privileged EXEC command on a cluster command switch to display a list of candidate switches.

show cluster candidates [**detail** | **mac-address** *H.H.H.*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

detail	(Optional) Display detailed information for all candidates.
mac-address *H.H.H.*	(Optional) MAC address of the cluster candidate.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This command is available only on the cluster command switch.

If the switch is not a cluster command switch, the command displays an empty line at the prompt.

The SN in the display means *switch member number*. If E appears in the SN column, it means that the switch is discovered through extended discovery. If E does not appear in the SN column, it means that the *switch member number* is the upstream neighbor of the candidate switch. The hop count is the number of devices the candidate is from the cluster command switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show cluster candidates** command:

```
Switch> show cluster candidates
                                                                  |---Upstream---|
       MAC Address    Name         Device Type      PortIf  FEC Hops SN PortIf  FEC

       00d0.7961.c4c0 StLouis-2    WS-C2360-48TD   Gi0/1      2   1  Fa0/11
       00d0.bbf5.e900 ldf-dist-128 WS-C3524-XL      Fa0/7        1   0  Fa0/24
       00e0.1e7e.be80 1900_Switch  1900             3        0   1   0  Fa0/11
       00e0.1e9f.7a00 Surfers-24   WS-C2924-XL      Fa0/5        1   0  Fa0/3
       00e0.1e9f.8c00 Surfers-12-2 WS-C2912-XL      Fa0/4        1   0  Fa0/7
       00e0.1e9f.8c40 Surfers-12-1 WS-C2912-XL      Fa0/1        1   0  Fa0/9
```

This is an example of output from the **show cluster candidates** command that uses the MAC address of a cluster member switch directly connected to the cluster command switch:

```
Switch> show cluster candidates mac-address 00d0.7961.c4c0
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
        Device type:            cisco WS-C2360-48TD-S
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 0)
        Local port:             Gi0/1   FEC number:
        Upstream port:          GI0/11  FEC Number:
Hops from cluster edge: 1
        Hops from command device: 1
```

This is an example of output from the **show cluster candidates** command that uses the MAC address of a cluster member switch three hops from the cluster edge:

```
Switch> show cluster candidates mac-address 0010.7bb6.1cc0
Device 'Ventura' with mac address number 0010.7bb6.1cc0
        Device type:            cisco WS-C2912MF-XL
        Upstream MAC address:   0010.7bb6.1cd4
        Local port:             Fa2/1   FEC number:
        Upstream port:          Fa0/24  FEC Number:
        Hops from cluster edge: 3
        Hops from command device: -
```

This is an example of output from the **show cluster candidates detail** command:

```
Switch> show cluster candidates detail
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
        Device type:            cisco WS-C3512-XL
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 1)
        Local port:             Fa0/3   FEC number:
        Upstream port:          Fa0/13  FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
Device '1900_Switch' with mac address number 00e0.1e7e.be80
        Device type:            cisco 1900
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 2)
        Local port:             3       FEC number: 0
        Upstream port:          Fa0/11  FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
Device 'Surfers-24' with mac address number 00e0.1e9f.7a00
        Device type:            cisco WS-C2924-XL
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 3)
        Local port:             Fa0/5   FEC number:
        Upstream port:          Fa0/3   FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
```

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show cluster members	Displays information about the cluster members.

show cluster members

Use the **show cluster members** privileged EXEC command on a cluster command switch to display information about the cluster members.

show cluster members [*n* | **detail**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

n	(Optional) Number that identifies a cluster member. The range is 0 to 15.
detail	(Optional) Display detailed information for all cluster members.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This command is available only on the cluster command switch.

If the cluster has no members, this command displays an empty line at the prompt.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show cluster members** command. The SN in the display means *switch number.*

```
Switch# show cluster members
                                                |---Upstream---|
SN MAC Address    Name          PortIf FEC Hops   SN PortIf  FEC  State
0  0002.4b29.2e00 StLouis1                 0                    Up   (Cmdr)
1  0030.946c.d740 tal-switch-1 Fa0/13       1     0  Gi0/1       Up
2  0002.b922.7180 nms-2820     10      0    2     1  Fa0/18      Up
3  0002.4b29.4400 SanJuan2     Gi0/1        2     1  Fa0/11      Up
4  0002.4b28.c480 GenieTest    Gi0/2        2     1  Fa0/9       Up
```

This is an example of output from the **show cluster members** for cluster member 3:

```
Switch# show cluster members 3
Device 'SanJuan2' with member number 3
        Device type:            cisco WS-C2360-48TD-SD
        MAC address:            0002.4b29.4400
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             Gi0/1   FEC number:
        Upstream port:          GI0/11  FEC Number:
        Hops from command device: 2
```

This is an example of output from the **show cluster members detail** command:

```
Switch# show cluster members detail
Device 'StLouis1' with member number 0 (Command Switch)
        Device type:            cisco C2360-48TD-SD
        MAC address:            0002.4b29.2e00
        Upstream MAC address:
        Local port:                     FEC number:
        Upstream port:                  FEC Number:
        Hops from command device: 0

Device 'tal-switch-14' with member number 1
        Device type:            cisco WS-C3548-XL
        MAC address:            0030.946c.d740
        Upstream MAC address:   0002.4b29.2e00 (Cluster member 0)
        Local port:             Fa0/13  FEC number:
        Upstream port:          Gi0/1   FEC Number:
        Hops from command device: 1
Device 'nms-2820' with member number 2
        Device type:            cisco 2820
        MAC address:            0002.b922.7180
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             10      FEC number: 0
        Upstream port:          Fa0/18  FEC Number:
        Hops from command device: 2
Device 'SanJuan2' with member number 3
        Device type:            cisco WS-C2360-48TD-SD
        MAC address:            0002.4b29.4400
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             Gi0/1   FEC number:
        Upstream port:          Fa0/11  FEC Number:
        Hops from command device: 2

Device 'GenieTest' with member number 4
        Device type:            cisco SeaHorse
        MAC address:            0002.4b28.c480
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             Gi0/2   FEC number:
        Upstream port:          Fa0/9   FEC Number:
        Hops from command device: 2
Device 'Palpatine' with member number 5
        Device type:            cisco WS-C2924M-XL
        MAC address:            00b0.6404.f8c0
        Upstream MAC address:   0002.4b29.2e00 (Cluster member 0)
        Local port:             Gi1   FEC number:
        Upstream port:          Gi0/7   FEC Number:
        Hops from command device: 1
```

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show cluster candidates	Displays a list of candidate switches.

show controllers cpu-interface

Use the **show controllers cpu-interface** privileged EXEC command to display the state of the CPU network interface ASIC and the send and receive statistics for packets reaching the CPU.

show controllers cpu-interface [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is a partial output example from the **show controllers cpu-interface** command:

```
Switch# show controllers cpu-interface
cpu-queue-frames  retrieved  dropped    invalid    hol-block
----------------- ---------- ---------- ---------- ----------
rpc               4523063    0          0          0
stp               1545035    0          0          0
ipc               1903047    0          0          0
routing protocol  96145      0          0          0
L2 protocol       79596      0          0          0
remote console    0          0          0          0
sw forwarding     5756       0          0          0
host              225646     0          0          0
broadcast         46472      0          0          0
cbt-to-spt        0          0          0          0
igmp snooping     68411      0          0          0
icmp              0          0          0          0
logging           0          0          0          0
rpf-fail          0          0          0          0
queue14           0          0          0          0
cpu heartbeat     1710501    0          0          0
```

```
Supervisor ASIC receive-queue parameters
----------------------------------------
 queue 0 maxrecevsize 5EE pakhead 1419A20 paktail 13EAED4
 queue 1 maxrecevsize 5EE pakhead 15828E0 paktail 157FBFC
 queue 2 maxrecevsize 5EE pakhead 1470D40 paktail 1470FE4
 queue 3 maxrecevsize 5EE pakhead 19CDDD0 paktail 19D02C8

<output truncated>

Supervisor ASIC Mic Registers
-----------------------------
MicDirectPollInfo               80000800
MicIndicationsReceived          00000000
MicInterruptsReceived           00000000
MicPcsInfo                      0001001F
MicPlbMasterConfiguration       00000000
MicRxFifosAvailable             00000000
MicRxFifosReady                 0000BFFF
MicTimeOutPeriod:       FrameTOPeriod: 00000EA6 DirectTOPeriod: 00004000

<output truncated>

MicTransmitFifoInfo:
Fifo0:   StartPtrs:     038C2800        ReadPtr:        038C2C38
        WritePtrs:      038C2C38        Fifo_Flag:      8A800800
        Weights:        001E001E
Fifo1:  StartPtr:       03A9BC00        ReadPtr:        03A9BC60
        WritePtrs:      03A9BC60        Fifo_Flag:      89800400
        writeHeaderPtr: 03A9BC60
Fifo2:  StartPtr:       038C8800        ReadPtr:        038C88E0
        WritePtrs:      038C88E0        Fifo_Flag:      88800200
        writeHeaderPtr: 038C88E0
Fifo3:  StartPtr:       03C30400        ReadPtr:        03C30638
        WritePtrs:      03C30638        Fifo_Flag:      89800400
        writeHeaderPtr: 03C30638
Fifo4:  StartPtr:       03AD5000        ReadPtr:        03AD50A0
        WritePtrs:      03AD50A0        Fifo_Flag:      89800400
        writeHeaderPtr: 03AD50A0
Fifo5:  StartPtr:       03A7A600        ReadPtr:        03A7A600
        WritePtrs:      03A7A600        Fifo_Flag:      88800200
        writeHeaderPtr: 03A7A600
Fifo6:  StartPtr:       03BF8400        ReadPtr:        03BF87F0
        WritePtrs:      03BF87F0        Fifo_Flag:      89800400

<output truncated>
```

Related Commands

Command	Description
show controllers ethernet-controller	Displays per-interface send and receive statistics read from the hardware or the interface internal registers.
show interfaces	Displays the administrative and operational status of all interfaces or a specified interface.

show controllers ethernet-controller

Use the **show controllers ethernet-controller** privileged EXEC command without keywords to display per-interface send and receive statistics read from the hardware. Use with the **phy** keyword to display the interface internal registers or the **port-asic** keyword to display information about the port ASIC.

show controllers ethernet-controller [*interface-id*] [**phy** [**detail**]] [**port-asic** {**configuration** | **statistics**}] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	The physical interface (including type, module, and port number).
phy	(Optional) Display the status of the internal registers on the switch physical layer device (PHY) for the device or the interface. This display includes the operational state of the automatic medium-dependent interface crossover (auto-MDIX) feature on an interface.
detail	(Optional) Display details about the PHY internal registers.
port-asic	(Optional) Display information about the port ASIC internal registers.
configuration	Display port ASIC internal register configuration.
statistics	Display port ASIC statistics, including the Rx/Sup Queue and miscellaneous statistics.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC (only supported with the *interface-id* keywords in user EXEC mode)

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This display without keywords provides traffic statistics, basically the RMON statistics for all interfaces or for the specified interface.

When you enter the **phy** or **port-asic** keywords, the displayed information is useful primarily for Cisco technical support representatives troubleshooting the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show controllers ethernet-controller** command for an interface. Table 2-5 describes the *Transmit* fields, and Table 2-6 describes the *Receive* fields.

```
Switch# show controllers ethernet-controller gigabitethernet0/1
Transmit GigabitEthernet0/1            Receive
         0 Bytes                             0 Bytes
         0 Unicast frames                    0 Unicast frames
         0 Multicast frames                  0 Multicast frames
         0 Broadcast frames                  0 Broadcast frames
         0 Too old frames                    0 Unicast bytes
         0 Deferred frames                   0 Multicast bytes
         0 MTU exceeded frames               0 Broadcast bytes
         0 1 collision frames                0 Alignment errors
         0 2 collision frames                0 FCS errors
         0 3 collision frames                0 Oversize frames
         0 4 collision frames                0 Undersize frames
         0 5 collision frames                0 Collision fragments
         0 6 collision frames
         0 7 collision frames                0 Minimum size frames
         0 8 collision frames                0 65 to 127 byte frames
         0 9 collision frames                0 128 to 255 byte frames
         0 10 collision frames               0 256 to 511 byte frames
         0 11 collision frames               0 512 to 1023 byte frames
         0 12 collision frames               0 1024 to 1518 byte frames
         0 13 collision frames               0 Overrun frames
         0 14 collision frames               0 Pause frames
         0 15 collision frames               0 Symbol error frames
         0 Excessive collisions
         0 Late collisions                   0 Invalid frames, too large
         0 VLAN discard frames               0 Valid frames, too large
         0 Excess defer frames               0 Invalid frames, too small
         0 64 byte frames                    0 Valid frames, too small
         0 127 byte frames
         0 255 byte frames                   0 Too old frames
         0 511 byte frames                   0 Valid oversize frames
         0 1023 byte frames                  0 System FCS error frames
         0 1518 byte frames                  0 RxPortFifoFull drop frame
         0 Too large frames
         0 Good (1 coll) frames
```

Table 2-5 Transmit Field Descriptions

Field	Description
Bytes	The total number of bytes sent on an interface.
Unicast Frames	The total number of frames sent to unicast addresses.
Multicast frames	The total number of frames sent to multicast addresses.
Broadcast frames	The total number of frames sent to broadcast addresses.
Too old frames	The number of frames dropped on the egress port because the packet aged out.
Deferred frames	The number of frames that are not sent after the time exceeds 2*maximum-packet time.
MTU exceeded frames	The number of frames that are larger than the maximum allowed frame size.
1 collision frames	The number of frames that are successfully sent on an interface after one collision occurs.
2 collision frames	The number of frames that are successfully sent on an interface after two collisions occur.
3 collision frames	The number of frames that are successfully sent on an interface after three collisions occur.
4 collision frames	The number of frames that are successfully sent on an interface after four collisions occur.

Table 2-5 Transmit Field Descriptions (continued)

Field	Description
5 collision frames	The number of frames that are successfully sent on an interface after five collisions occur.
6 collision frames	The number of frames that are successfully sent on an interface after six collisions occur.
7 collision frames	The number of frames that are successfully sent on an interface after seven collisions occur.
8 collision frames	The number of frames that are successfully sent on an interface after eight collisions occur.
9 collision frames	The number of frames that are successfully sent on an interface after nine collisions occur.
10 collision frames	The number of frames that are successfully sent on an interface after ten collisions occur.
11 collision frames	The number of frames that are successfully sent on an interface after 11 collisions occur.
12 collision frames	The number of frames that are successfully sent on an interface after 12 collisions occur.
13 collision frames	The number of frames that are successfully sent on an interface after 13 collisions occur.
14 collision frames	The number of frames that are successfully sent on an interface after 14 collisions occur.
15 collision frames	The number of frames that are successfully sent on an interface after 15 collisions occur.
Excessive collisions	The number of frames that could not be sent on an interface after 16 collisions occur.
Late collisions	After a frame is sent, the number of frames dropped because late collisions were detected while the frame was sent.
VLAN discard frames	The number of frames dropped on an interface because the CFI[1] bit is set.
Excess defer frames	The number of frames that are not sent after the time exceeds the maximum-packet time.
64 byte frames	The total number of frames sent on an interface that are 64 bytes.
127 byte frames	The total number of frames sent on an interface that are from 65 to 127 bytes.
255 byte frames	The total number of frames sent on an interface that are from 128 to 255 bytes.
511 byte frames	The total number of frames sent on an interface that are from 256 to 511 bytes.
1023 byte frames	The total number of frames sent on an interface that are from 512 to 1023 bytes.
1518 byte frames	The total number of frames sent on an interface that are from 1024 to 1518 bytes.
Too large frames	The number of frames sent on an interface that are larger than the maximum allowed frame size.
Good (1 coll) frames	The number of frames that are successfully sent on an interface after one collision occurs. This value does not include the number of frames that are not successfully sent after one collision occurs.

1. CFI = Canonical Format Indicator

Table 2-6 Receive Field Descriptions

Field	Description
Bytes	The total amount of memory (in bytes) used by frames received on an interface, including the FCS[1] value and the incorrectly formed frames. This value excludes the frame header bits.
Unicast frames	The total number of frames successfully received on the interface that are directed to unicast addresses.
Multicast frames	The total number of frames successfully received on the interface that are directed to multicast addresses.
Broadcast frames	The total number of frames successfully received on an interface that are directed to broadcast addresses.

Table 2-6 Receive Field Descriptions (continued)

Field	Description
Unicast bytes	The total amount of memory (in bytes) used by unicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Multicast bytes	The total amount of memory (in bytes) used by multicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Broadcast bytes	The total amount of memory (in bytes) used by broadcast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Alignment errors	The total number of frames received on an interface that have alignment errors.
FCS errors	The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values.
Oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size.
Undersize frames	The number of frames received on an interface that are smaller than 64 bytes.
Collision fragments	The number of collision fragments received on an interface.
Minimum size frames	The total number of frames that are the minimum frame size.
65 to 127 byte frames	The total number of frames that are from 65 to 127 bytes.
128 to 255 byte frames	The total number of frames that are from 128 to 255 bytes.
256 to 511 byte frames	The total number of frames that are from 256 to 511 bytes.
512 to 1023 byte frames	The total number of frames that are from 512 to 1023 bytes.
1024 to 1518 byte frames	The total number of frames that are from 1024 to 1518 bytes.
Overrun frames	The total number of overrun frames received on an interface.
Pause frames	The number of pause frames received on an interface.
Symbol error frames	The number of frames received on an interface that have symbol errors.
Invalid frames, too large	The number of frames received that were larger than maximum allowed MTU[2] size (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error.
Valid frames, too large	The number of frames received on an interface that are larger than the maximum allowed frame size.
Invalid frames, too small	The number of frames received that are smaller than 64 bytes (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error.
Valid frames, too small	The number of frames received on an interface that are smaller than 64 bytes (or 68 bytes for VLAN-tagged frames) and that have valid FCS values. The frame size includes the FCS bits but excludes the frame header bits.
Too old frames	The number of frames dropped on the ingress port because the packet aged out.
Valid oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size and have valid FCS values. The frame size includes the FCS value but does not include the VLAN tag.

Table 2-6 Receive Field Descriptions (continued)

Field	Description
System FCS error frames	The total number of frames received on an interface that have a valid length (in bytes) but that do not have the correct FCS values.
RxPortFifoFull drop frames	The total number of frames received on an interface that are dropped because the ingress queue is full.

1. FCS = frame check sequence
2. MTU = maximum transmission unit

This is an example of output from the **show controllers ethernet-controller phy** command for a specific interface:

```
Switch# show controllers ethernet-controller gigabitethernet0/2 phy
Control Register                        :  0001 0001 0100 0000
 Control STATUS                         :  0111 1001 0100 1001
 Phy ID 1                               :  0000 0001 0100 0001
 Phy ID 2                               :  0000 1100 0010 0100
 Auto-Negotiation Advertisement         :  0000 0011 1110 0001
 Auto-Negotiation Link Partner          :  0000 0000 0000 0000
 Auto-Negotiation Expansion Reg         :  0000 0000 0000 0100
 Next Page Transmit Register            :  0010 0000 0000 0001
 Link Partner Next page Registe         :  0000 0000 0000 0000
 1000BASE-T Control Register            :  0000 1111 0000 0000
 1000BASE-T Status Register             :  0100 0000 0000 0000
 Extended Status Register               :  0011 0000 0000 0000
 PHY Specific Control Register          :  0000 0000 0111 1000
 PHY Specific Status Register           :  1000 0001 0100 0000
 Interrupt Enable                       :  0000 0000 0000 0000
 Interrupt Status                       :  0000 0000 0100 0000
 Extended PHY Specific Control          :  0000 1100 0110 1000
 Receive Error Counter                  :  0000 0000 0000 0000
 Reserved Register 1                    :  0000 0000 0000 0000
 Global Status                          :  0000 0000 0000 0000
 LED Control                            :  0100 0001 0000 0000
 Manual LED Override                    :  0000 1000 0010 1010
 Extended PHY Specific Control          :  0000 0000 0001 1010
 Disable Receiver 1                     :  0000 0000 0000 1011
 Disable Receiver 2                     :  1000 0000 0000 0100
 Extended PHY Specific Status           :  1000 0100 1000 0000
 Auto-MDIX                              :  On   [AdminState=1   Flags=0x00052248]
```

This is an example of output from the **show controllers ethernet-controller tengigabitethernet0/1 phy** command:

```
Switch# show controllers ethernet-controller tengigabitethernet0/1 phy
TenGigabitEthernet0/1 (gpn: 29, port-number: 1)
------------------------------------------------------------
X2 Serial EEPROM Contents:
Non-Volatile Register (NVR) Fields
X2 MSA Version supported :0x1E
NVR Size in bytes :0x100
Number of bytes used :0x100
Basic Field Address :0xB
Customer Field Address :0x77
Vendor Field Address :0xA7
Extended Vendor Field Address :0x100
Reserved :0x0
Transceiver type :0x2 =X2
Optical connector type :0x1 =SC
```

```
Bit encoding:0x1 =NRZ
Normal BitRate in multiple of 1M b/s :0x2848
Protocol Type:0x1 =10GgE
Standards Compliance Codes :
10GbE Code Byte 0 :0x4 =10GBASE-ER
10GbE Code Byte 1 :0x0
SONET/SDH Code Byte 0:0x0
SONET/SDH Code Byte 1:0x0
SONET/SDH Code Byte 2:0x0
SONET/SDH Code Byte 3:0x0
10GFC Code Byte 0 :0x0
10GFC Code Byte 1 :0x0
10GFC Code Byte 2 :0x0
10GFC Code Byte 3 :0x0
Transmission range in10m :0xFA0
Fibre Type :
Fibre Type Byte 0 :0x20 =SM, Generic
Fibre Type Byte 1 :0x0 =Unspecified
<output truncated>
```

This is an example of output from the **show controllers ethernet-controller port-asic configuration** command:

```
Switch# show controllers ethernet-controller port-asic configuration
================================================================================
Switch 1, PortASIC 0 Registers
--------------------------------------------------------------------------------
DeviceType                          : 000101BC
Reset                               : 00000000
PmadMicConfig                       : 00000001
PmadMicDiag                         : 00000003
SupervisorReceiveFifoSramInfo       : 000007D0 000007D0 40000000
SupervisorTransmitFifoSramInfo      : 000001D0 000001D0 40000000
GlobalStatus                        : 00000800
IndicationStatus                    : 00000000
IndicationStatusMask                : FFFFFFFF
InterruptStatus                     : 00000000
InterruptStatusMask                 : 01FFE800
SupervisorDiag                      : 00000000
SupervisorFrameSizeLimit            : 000007C8
SupervisorBroadcast                 : 000A0F01
GeneralIO                           : 000003F9 00000000 00000004
StackPcsInfo                        : FFFF1000 860329BD 5555FFFF FFFFFFFF
                                      FF0FFF00 86020000 5555FFFF 00000000
StackRacInfo                        : 73001630 00000003 7F001644 00000003
                                      24140003 FD632B00 18E418E0 FFFFFFFF
StackControlStatus                  : 18E418E0
stackControlStatusMask              : FFFFFFFF
TransmitBufferFreeListInfo          : 00000854 00000800 00000FF8 00000000
                                      0000088A 0000085D 00000FF8 00000000
TransmitRingFifoInfo                : 00000016 00000016 40000000 00000000
                                      0000000C 0000000C 40000000 00000000
TransmitBufferInfo                  : 00012000 00000FFF 00000000 00000030
TransmitBufferCommonCount           : 00000F7A
TransmitBufferCommonCountPeak       : 0000001E
TransmitBufferCommonCommonEmpty     : 000000FF
NetworkActivity                     : 00000000 00000000 00000000 02400000
DroppedStatistics                   : 00000000
FrameLengthDeltaSelect              : 00000001
SneakPortFifoInfo                   : 00000000
MacInfo                             : 0EC0801C 00000001 0EC0801B 00000001
                                      00C0001D 00000001 00C0001E 00000001

<output truncated>
```

This is an example of output from the **show controllers ethernet-controller port-asic statistics** command:

```
Switch# show controllers ethernet-controller port-asic statistics
================================================================================
 Switch 1, PortASIC 0 Statistics
--------------------------------------------------------------------------------
         0 RxQ-0, wt-0 enqueue frames            0 RxQ-0, wt-0 drop frames
   4118966 RxQ-0, wt-1 enqueue frames            0 RxQ-0, wt-1 drop frames
         0 RxQ-0, wt-2 enqueue frames            0 RxQ-0, wt-2 drop frames

         0 RxQ-1, wt-0 enqueue frames            0 RxQ-1, wt-0 drop frames
       296 RxQ-1, wt-1 enqueue frames            0 RxQ-1, wt-1 drop frames
   2836036 RxQ-1, wt-2 enqueue frames            0 RxQ-1, wt-2 drop frames

         0 RxQ-2, wt-0 enqueue frames            0 RxQ-2, wt-0 drop frames
         0 RxQ-2, wt-1 enqueue frames            0 RxQ-2, wt-1 drop frames
    158377 RxQ-2, wt-2 enqueue frames            0 RxQ-2, wt-2 drop frames

         0 RxQ-3, wt-0 enqueue frames            0 RxQ-3, wt-0 drop frames
         0 RxQ-3, wt-1 enqueue frames            0 RxQ-3, wt-1 drop frames
         0 RxQ-3, wt-2 enqueue frames            0 RxQ-3, wt-2 drop frames


        15 TxBufferFull Drop Count               0 Rx Fcs Error Frames
         0 TxBufferFrameDesc BadCrc16            0 Rx Invalid Oversize Frames
         0 TxBuffer Bandwidth Drop Cou           0 Rx Invalid Too Large Frames
         0 TxQueue Bandwidth Drop Coun           0 Rx Invalid Too Large Frames
         0 TxQueue Missed Drop Statist           0 Rx Invalid Too Small Frames
        74 RxBuffer Drop DestIndex Cou           0 Rx Too Old Frames
         0 SneakQueue Drop Count                 0 Tx Too Old Frames
         0 Learning Queue Overflow Fra           0 System Fcs Error Frames
         0 Learning Cam Skip Count

        15 Sup Queue 0 Drop Frames               0 Sup Queue 8 Drop Frames
         0 Sup Queue 1 Drop Frames               0 Sup Queue 9 Drop Frames
         0 Sup Queue 2 Drop Frames               0 Sup Queue 10 Drop Frames
         0 Sup Queue 3 Drop Frames               0 Sup Queue 11 Drop Frames
         0 Sup Queue 4 Drop Frames               0 Sup Queue 12 Drop Frames
         0 Sup Queue 5 Drop Frames               0 Sup Queue 13 Drop Frames
         0 Sup Queue 6 Drop Frames               0 Sup Queue 14 Drop Frames
         0 Sup Queue 7 Drop Frames               0 Sup Queue 15 Drop Frames
================================================================================
 Switch 1, PortASIC 1 Statistics
--------------------------------------------------------------------------------
         0 RxQ-0, wt-0 enqueue frames            0 RxQ-0, wt-0 drop frames
        52 RxQ-0, wt-1 enqueue frames            0 RxQ-0, wt-1 drop frames
         0 RxQ-0, wt-2 enqueue frames            0 RxQ-0, wt-2 drop frames

<output truncated>
```

Related Commands

Command	Description
show controllers cpu-interface	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
show controllers tcam	Displays the state of registers for all hardware memory in the system and for hardware interface ASICs that are content addressable memory controllers.
show idprom	Displays the IDPROM information for the specified interface.

show controllers ethernet-controller fastethernet

Use the **show controllers ethernet-controller fastethernet** privileged EXEC command to display information about the Ethernet management port, including the port status and the per-interface send and receive statistics read from the hardware.

show controllers ethernet-controller fastethernet 0 [**phy** [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

phy [**detail**]	(Optional) Display the status of the internal registers on the switch physical layer device (PHY) for the Ethernet management port on the switch. Use the **detail** keyword to display details about the PHY internal registers. This display includes the operational state of the automatic medium-dependent interface crossover (auto-MDIX) feature on an interface.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC (only supported with the **fastethernet 0** keywords in user EXEC mode)

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The output display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show controllers ethernet-controller fastethernet 0** command. See Table 2-5 and Table 2-6 for descriptions of the *Transmit* and *Receive* fields.

```
Switch> show controller ethernet-controller fastethernet 0
     Transmit FastEthernet0                  Receive
         5925 Bytes                           33181 Bytes
            0 Unicast frames                     78 Unicast frames
           15 Multicast frames                  437 Multicast frames
            1 Broadcast frames                    0 Broadcast frames
            0 Too old frames                      0 Unicast bytes
            0 Deferred frames                     0 Multicast bytes
            0 MTU exceeded frames                 0 Broadcast bytes
            0 1 collision frames                  0 Alignment errors
            0 2 collision frames                  0 FCS errors
            0 3 collision frames                  0 Oversize frames
            0 4 collision frames                  0 Undersize frames
```

```
0 5 collision frames                    0 Collision fragments
0 6 collision frames
0 7 collision frames                    0 Minimum size frames
0 8 collision frames                    0 65 to 127 byte frames
0 9 collision frames                    0 128 to 255 byte frames
0 10 collision frames                   0 256 to 511 byte frames
0 11 collision frames                   0 512 to 1023 byte frames
0 12 collision frames                   0 1024 to 1518 byte frames
0 13 collision frames                   0 Overrun frames
0 14 collision frames                   0 Pause frames
0 15 collision frames
0 Excessive collisions                  0 Symbol error frames
0 Late collisions                       0 Invalid frames, too large
0 VLAN discard frames                   0 Valid frames, too large
0 Excess defer frames                   0 Invalid frames, too small
0 64 byte frames                        0 Valid frames, too small
0 127 byte frames
0 255 byte frames                       0 Too old frames
0 511 byte frames                       0 Valid oversize frames
0 1023 byte frames                      0 System FCS error frames
0 1518 byte frames                      0 RxPortFifoFull drop frame
0 Too large frames
0 Good (1 coll) frames
0 Good (>1 coll) frames
```

This is an example of output from the **show controllers ethernet-controller fastethernet 0 phy** command on a switch:

```
Switch# show controller ethernet-controller fastethernet 0 phy
FastEthernet0
------------------------------------------------------------
hw_if_index = 2 if_number = 2
PowerPC405 FastEthernet unit 0
PHY Hardware is Broadcom BCM5220 rev. 4 (id_register: 0x40, 0x61E4)

rx_intr: 0 tx_intr: 0 mac_err_isr: 0 phy_link_isr:0
Current station address 00d0.2bfd.d737, default address 00d0.2bfd.d737
MAL register dump:
malcr        0x00004082  0x100
malesr       0x00000000  0x101
malier       0x00000000  0x102
maltxcasr    0x80000000  0x104
maltxcarr    0x80000000  0x105
maltxeobisr  0x80000000  0x106
maltxdeir    0x00000000  0x107
malrxcasr    0x80000000  0x110
malrxcarr    0x80000000  0x111
malrxeobisr  0x80000000  0x112
malrxdeir    0x00000000  0x113
maltxctp0r   0x0F027880  0x120
malrxctp0r   0x0F0272C0  0x140
malrcbs0   0x00000060  0x160

<output truncated>
```

Related Commands

Command	Description
debug fastethernet	Enables debugging of the Ethernet management port.

show controllers tcam

Use the **show controllers tcam** privileged EXEC command to display the state of the registers for all hardware memory in the system and for all hardware interface ASICs that are content-addressable memory-controllers.

show controllers tcam [**asic** [**number**]] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

asic	(Optional) Display port ASIC hardware information.
number	(Optional) Display information for the specified port ASIC number. The range is from 0 to 15.
detail	(Optional) Display detailed hardware register information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show controllers tcam** command:

```
Switch# show controllers tcam
------------------------------------------------------------------------
TCAM-0 Registers
------------------------------------------------------------------------
  REV:    00B30103
  SIZE:   00080040
  ID:     00000000
  CCR:    00000000_F0000020

  RPID0:  00000000_00000000
  RPID1:  00000000_00000000
  RPID2:  00000000_00000000
  RPID3:  00000000_00000000
```

```
  HRR0:   00000000_E000CAFC
  HRR1:   00000000_00000000
  HRR2:   00000000_00000000
  HRR3:   00000000_00000000
  HRR4:   00000000_00000000
  HRR5:   00000000_00000000
  HRR6:   00000000_00000000
  HRR7:   00000000_00000000
<output truncated>

  GMR31:  FF_FFFFFFFF_FFFFFFFF
  GMR32:  FF_FFFFFFFF_FFFFFFFF
  GMR33:  FF_FFFFFFFF_FFFFFFFF

================================================================================
 TCAM related PortASIC 1 registers
================================================================================
LookupType:                   89A1C67D_24E35F00
LastCamIndex:                 0000FFE0
LocalNoMatch:                 000069E0
ForwardingRamBaseAddress:
                              00022A00 0002FE00 00040600 0002FE00 0000D400
                              00000000 003FBA00 00009000 00009000 00040600
                              00000000 00012800 00012900
```

Related Commands

Command	Description
show controllers cpu-interface	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
show controllers ethernet-controller	Displays per-interface send and receive statistics read from the hardware or the interface internal registers.

show controllers utilization

Use the **show controllers utilization** user EXEC command to display bandwidth utilization on the switch or specific ports.

show controllers [*interface-id*] **utilization** [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the switch interface.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show controllers utilization** command.

```
Switch> show controllers utilization
Port       Receive Utilization  Transmit Utilization
Gi0/2              0                    0
Gi0/3              0                    0
Gi0/4              0                    0
Gi0/5              0                    0
Gi0/6              0                    0
Gi0/7              0                    0
<output truncated>

Gi0/1              0                    0
Gi0/2              0                    0
<output truncated>

Switch Receive Bandwidth Percentage Utilization  : 0
Switch Transmit Bandwidth Percentage Utilization : 0

Switch Fabric Percentage Utilization : 0
```

This is an example of output from the **show controllers utilization** command on a specific port:

```
Switch> show controllers gigabitethernet0/1 utilization
Receive Bandwidth Percentage Utilization   : 0
Transmit Bandwidth Percentage Utilization  : 0
```

Table 2-7 show controllers utilization Field Descriptions

Field	Description
Receive Bandwidth Percentage Utilization	Displays the received bandwidth usage of the switch, which is the sum of the received traffic on all the ports divided by the switch receive capacity.
Transmit Bandwidth Percentage Utilization	Displays the transmitted bandwidth usage of the switch, which is the sum of the transmitted traffic on all the ports divided it by the switch transmit capacity.
Fabric Percentage Utilization	Displays the average of the transmitted and received bandwidth usage of the switch.

Related Commands

Command	Description
show controllers ethernet-controller	Displays the interface internal registers.

show diagnostic

Use the **show diagnostic** user EXEC command to display the online diagnostic test results and the supported test suites.

show diagnostic content [**|** {**begin | exclude | include**} *expression*]

show diagnostic post [**|**{**begin | exclude | include**} *expression*]

show diagnostic result [**detail | test** {*name* **|** *test-id* **|** *test-id-range* **| all**} [**detail**]] [**|** {**begin | exclude | include**} *expression*]

show diagnostic schedule [**|** {**begin | exclude | include**} *expression*]

show diagnostic status [**|** {**begin | exclude | include**} *expression*]

show diagnostic [**detail**] [**|** {**begin | exclude | include**} *expression*]

Syntax Description

content	Display test information including the test ID, the test attributes, and the supported coverage test levels for specific tests and for switches.
post	Display the power-on self-test (POST) results.
result	Display the diagnostic test results.
detail	(Optional) Display the detailed test results.
test	(Optional) Specify the test results to display: • *name*—Enter the name of the diagnostic test to display results only for this test. • *test-id*—Enter the test ID number to display results only for this test. • *test-id-range*—Enter the range of test ID numbers to display results only for these tests. • **all**—Enter this keyword to display results for all the tests.
schedule	Display the scheduled diagnostic tests.
status	Display the running diagnostic tests.
| begin	(Optional) Display begins with the line that matches the expression.
| exclude	(Optional) Display excludes lines that match the expression.
| include	(Optional) Display includes lines that match the specified expression.
expression	Expression in the output to use as a reference point.

Defaults

This command has no default setting.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **show diagnostic post** command output is the same as the **show post** command output.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This example shows how to display the online diagnostics that are configured on the switch:

```
Switch> show diagnostic content
:

Diagnostics test suite attributes:
     B/* - Basic ondemand test / NA
   P/V/* - Per port test / Per device test / NA
   D/N/* - Disruptive test / Non-disruptive test / NA
     S/* - Only applicable to standby unit / NA
     X/* - Not a health monitoring test / NA
     F/* - Fixed monitoring interval test / NA
     E/* - Always enabled monitoring test / NA
     A/I - Monitoring is active / Monitoring is inactive
     R/* - Switch will reload after test list completion / NA
     P/* - will partition stack / NA

                                                        Test Interval   Thre-
 ID   Test Name                                Attributes      day hh:mm:ss.ms shold
 ==== ================================== ============    =============== =====
   1) TestPortAsicStackPortLoopback ---> B*N****I**      not configured  n/a
   2) TestPortAsicLoopback ------------> B*D*X**IR*      not configured  n/a
   3) TestPortAsicCam -----------------> B*D*X**IR*      not configured  n/a
   4) TestPortAsicRingLoopback --------> B*D*X**IR*      not configured  n/a
   5) TestMicRingLoopback -------------> B*D*X**IR*      not configured  n/a
   6) TestPortAsicMem -----------------> B*D*X**IR*      not configured  n/a
```

This example shows how to display the diagnostic test results on a switch. You can also use the **show diagnostic switch** command to display these diagnostic results.

```
Switch> show diagnostic result
:   SerialNo : XXXXXXXXXXX

  Overall diagnostic result: PASS

  Test results: (. = Pass, F = Fail, U = Untested)

    1) TestPortAsicStackPortLoopback ---> .
    2) TestPortAsicLoopback ------------> U
    3) TestPortAsicCam -----------------> U
    4) TestPortAsicRingLoopback --------> U
    5) TestMicRingLoopback -------------> U
    6) TestPortAsicMem -----------------> U
    7) TestInlinePwrCtlr ---------------> U
```

This example shows how to display the running tests in a switch:

```
Switch> show diagnostic status

<BU> - Bootup Diagnostics, <HM> - Health Monitoring Diagnostics,
<OD> - OnDemand Diagnostics, <SCH> - Scheduled Diagnostics
```

```
====== ================================= ============================== ======
Card   Description                       Current Running Test           Run by
------ --------------------------------- ------------------------------ ------
                                         N/A                            N/A

====== ================================= ============================== ======

eXpresso-239-057_2350-48TD-S#
```

This example shows how to display the online diagnostic test schedule for a switch:

```
Switch> show diagnostic schedule
Current Time = 14:39:49 PST Tue Jul 5 2005
Diagnostic for Switch 1:
Schedule #1:
To be run daily 12:00
Test ID(s) to be executed: 1.
```

This example shows how to display the detailed switch results:

```
Switch> show diagnostic switch detail
:   SerialNo : XXXXXXXXXXX

  Overall diagnostic result: PASS

  Test results: (. = Pass, F = Fail, U = Untested)

  ____________________________________________________________________________

    1) TestPortAsicStackPortLoopback ---> .

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 19
          Last test execution time ----> Mar 01 1993 00:21:46
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> Mar 01 1993 00:21:46
          Total failure count ---------> 0
          Consecutive failure count ---> 0
  ____________________________________________________________________________

    2) TestPortAsicLoopback ------------> U

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 0
          Last test execution time ----> n/a
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> n/a
          Total failure count ---------> 0
          Consecutive failure count ---> 0
  ____________________________________________________________________________

    3) TestPortAsicCam -----------------> U

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 0
          Last test execution time ----> n/a
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> n/a
          Total failure count ---------> 0
          Consecutive failure count ---> 0
  ____________________________________________________________________________
```

```
    4) TestPortAsicRingLoopback --------> U

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 0
          Last test execution time ----> n/a
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> n/a
          Total failure count ---------> 0
          Consecutive failure count ---> 0
_____________________________________________________________________________

    5) TestMicRingLoopback -------------> U

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 0
          Last test execution time ----> n/a
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> n/a
          Total failure count ---------> 0
          Consecutive failure count ---> 0
_____________________________________________________________________________

    6) TestPortAsicMem ------------------> U

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 0
          Last test execution time ----> n/a
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> n/a
          Total failure count ---------> 0
          Consecutive failure count ---> 0
_____________________________________________________________________________

    7) TestInlinePwrCtlr ---------------> U

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 0
          Last test execution time ----> n/a
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> n/a
          Total failure count ---------> 0
          Consecutive failure count ---> 0
_____________________________________________________________________________
```

Related Commands

Command	Description
diagnostic monitor	Configures teh health-monitoring diagnostic test.
diagnostic schedule	Sets the scheduling of test-based online diagnostic testing.
diagnostic start	Starts the online diagnostic test.

show dtp

Use the **show dtp** privileged EXEC command to display Dynamic Trunking Protocol (DTP) information for the switch or for a specified interface.

show dtp [**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Display settings for the specified interface. Valid interfaces include physical ports (including type, module, and port number).
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show dtp** command:

```
Switch# show dtp
Global DTP information
        Sending DTP Hello packets every 30 seconds
        Dynamic Trunk timeout is 300 seconds
        21 interfaces using DTP
```

This is an example of output from the **show dtp interface** command:

```
Switch# show dtp interface gigabitethernet0/1
DTP information for GigabitEthernet0/1:
  TOS/TAS/TNS:                              ACCESS/AUTO/ACCESS
  TOT/TAT/TNT:                              NATIVE/NEGOTIATE/NATIVE
  Neighbor address 1:                       000943A7D081
  Neighbor address 2:                       000000000000
  Hello timer expiration (sec/state):       1/RUNNING
  Access timer expiration (sec/state):      never/STOPPED
  Negotiation timer expiration (sec/state): never/STOPPED
  Multidrop timer expiration (sec/state):   never/STOPPED
  FSM state:                                S2:ACCESS
  # times multi & trunk                     0
  Enabled:                                  yes
  In STP:                                   no
```

```
Statistics
----------
3160 packets received (3160 good)
0 packets dropped
    0 nonegotiate, 0 bad version, 0 domain mismatches, 0 bad TLVs, 0 other
6320 packets output (6320 good)
    3160 native, 3160 software encap isl, 0 isl hardware native
0 output errors
0 trunk timeouts
1 link ups, last link up on Mon Mar 01 1993, 01:02:29
0 link downs
```

Related Commands

Command	Description
show interfaces trunk	Displays interface trunking information.

show eap

Use the **show eap** privileged EXEC command to display Extensible Authentication Protocol (EAP) registration and session information for the switch or for the specified port.

show eap {{**registrations** [**method** [*name*] | **transport** [*name*]]} | {**sessions** [**credentials** *name* [**interface** *interface-id*] | **interface** *interface-id* | **method** *name* | **transport** *name*]}} [**credentials** *name* | **interface** *interface-id* | **transport** *name*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

registrations	Display EAP registration information.
method *name*	(Optional) Display EAP method registration information.
transport *name*	(Optional) Display EAP transport registration information.
sessions	Display EAP session information.
credentials *name*	(Optional) Display EAP method registration information.
interface *interface-id*	(Optional) Display the EAP information for the specified port (including type, and port number).
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When you use the **show eap registrations** privileged EXEC command with these keywords, the command output shows this information:

- None—All the lower levels used by EAP and the registered EAP methods.
- **method** *name* keyword—The specified method registrations.
- **transport** *name* keyword—The specific lower-level registrations.

When you use the **show eap sessions** privileged EXEC command with these keywords, the command output shows this information:

- None—All active EAP sessions.
- **credentials** *name* keyword—The specified credentials profile.
- **interface** *interface-id* keyword—The parameters for the specified interface.
- **method** *name* keyword—The specified EAP method.
- **transport** *name* keyword—The specified lower layer.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show eap registrations** privileged EXEC command:

```
Switch> show eap registrations
Registered EAP Methods:
  Method  Type            Name
    4     Peer            MD5

Registered EAP Lower Layers:
  Handle  Type            Name
    2     Authenticator   Dot1x-Authenticator
    1     Authenticator   MAB
```

This is an example of output from the **show eap registrations transport** privileged user EXEC command:

```
Switch> show eap registrations transport all
Registered EAP Lower Layers:
  Handle  Type            Name
    2     Authenticator   Dot1x-Authenticator
    1     Authenticator   MAB
```

This is an example of output from the **show eap sessions** privileged EXEC command:

```
Switch> show eap sessions
Role:                   Authenticator   Decision:               Fail
Lower layer:            Dot1x-AuthenticaInterface:              Gi0/1
Current method:         None            Method state:           Uninitialised
Retransmission count:   0  (max: 2)     Timer:                  Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle:             0x5200000A      Credentials profile:    None
Lower layer context ID: 0x93000004      Eap profile name:       None
Method context ID:      0x00000000      Peer Identity:          None
Start timeout (s):      1               Retransmit timeout (s): 30 (30)
Current ID:             2               Available local methods: None

Role:                   Authenticator   Decision:               Fail
Lower layer:            Dot1x-AuthenticaInterface:              Gi0/2
Current method:         None            Method state:           Uninitialised
Retransmission count:   0  (max: 2)     Timer:                  Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle:             0xA800000B      Credentials profile:    None
Lower layer context ID: 0x0D000005      Eap profile name:       None
Method context ID:      0x00000000      Peer Identity:          None
Start timeout (s):      1               Retransmit timeout (s): 30 (30)
Current ID:             2               Available local methods: None

<Output truncated>
```

This is an example of output from the **show eap sessions interface** *interface-id* privileged EXEC command:

```
Switch# show eap sessions gigabitethernet0/1
Role:                   Authenticator   Decision:               Fail
Lower layer:            Dot1x-AuthenticaInterface:              Gi0/1
Current method:         None            Method state:           Uninitialised
Retransmission count:   1  (max: 2)     Timer:                  Authenticator
ReqId Retransmit (timeout: 30s, remaining: 13s)
EAP handle:             0x5200000A      Credentials profile:    None
Lower layer context ID: 0x93000004      Eap profile name:       None
```

```
Method context ID:      0x00000000      Peer Identity:           None
Start timeout (s):      1               Retransmit timeout (s):  30 (30)
Current ID:             2               Available local methods: None
```

Related Commands

Command	Description
clear eap	Clears EAP session information for the switch or for the specified port.

show env

Use the **show env** user EXEC command to display fan, temperature, and power information for the switch.

show env {**all** | **fan** | **power** | **temperature** [**status**]} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

all	Display the fan and temperature environmental status and the status of the internal power supply.
fan	Display the switch fan status.
power	Display the switch internal power status.
temperature	Display the switch temperature status.
temperature status	(Optional) Display the switch internal temperature (not the external temperature) and the threshold values.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **show env** user EXEC command to display the information for the switch.

If you enter the **show env temperature status** command, the command output shows the switch temperature state and the threshold level.

You can also use the **show env temperature** command to display the switch temperature status. The command output shows the green and yellow states as *OK* and the red state as *FAULTY*. If you enter the **show env all** command, the command output is the same as the **show env temperature status** command output.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show env all** command on a switch:

```
Switch> show env all
FAN is OK
TEMPERATURE is OK
Temperature Value: 42 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 49 Degree Celsius
Red Threshold    : 69 Degree Celsius
```

```
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
 1  Built-in                                         Good
```

This is an example of output from the **show env power** command on a switch:

```
Switch> show env power
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
 1  Built-in                                         Good
```

This example shows how to display the temperature value, state, and the threshold values on a switch. Table 2-8 describes the temperature states in the command output.

```
Switch> show env temperature status
Temperature Value: 42 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 49 Degree Celsius
Red Threshold    : 69 Degree Celsius
```

Table 2-8 States in the show env temperature status Command Output

State	Description
Green	The switch temperature is in the *normal* operating range.
Yellow	The temperature is in the *warning* range. You should check the external temperature around the switch.
Red	The temperature is in the *critical* range. The switch might not run properly if the temperature is in this range.

show errdisable detect

Use the **show errdisable detect** user EXEC command to display error-disabled detection status.

show errdisable detect [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

A displayed `gbic-invalid` error reason refers to an invalid small form-factor pluggable (SFP) module.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

The error-disable reasons in the command output are listed in alphabetical order. The mode column shows how error disable is configured for each feature.

You can configure error-disabled detection in these modes:

- port mode—The entire physical port is error disabled if a violation occurs.
- vlan mode—The VLAN is error disabled if a violation occurs.
- port/vlan mode—The entire physical port is error disabled on some ports and per-VLAN error disabled on other ports.

Examples

This is an example of output from the **show errdisable detect** command:

```
Switch> show errdisable detect
ErrDisable Reason    Detection    Mode
-----------------    ---------    ----
arp-inspection       Enabled      port
bpduguard            Enabled      vlan
channel-misconfig    Enabled      port
community-limit      Enabled      port
dhcp-rate-limit      Enabled      port
dtp-flap             Enabled      port
gbic-invalid         Enabled      port
inline-power         Enabled      port
invalid-policy       Enabled      port
l2ptguard            Enabled      port
link-flap            Enabled      port
loopback             Enabled      port
```

```
lsgroup              Enabled      port
pagp-flap            Enabled      port
psecure-violation    Enabled      port/vlan
security-violatio    Enabled      port
sfp-config-mismat    Enabled      port
storm-control        Enabled      port
udld                 Enabled      port
vmps                 Enabled      port
```

Related Commands

Command	Description
errdisable detect cause	Enables error-disabled detection for a specific cause or all causes.
show errdisable flap-values	Displays error condition recognition information.
show errdisable recovery	Displays error-disabled recovery timer information.
show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

show errdisable flap-values

Use the **show errdisable flap-values** user EXEC command to display conditions that cause an error to be recognized for a cause.

show errdisable flap-values [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The *Flaps* column in the display shows how many changes to the state within the specified time interval will cause an error to be detected and a port to be disabled. See the "Examples" section for an example of the display.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show errdisable flap-values** command, which shows that an error will be assumed and the port shut down if three Dynamic Trunking Protocol (DTP)-state (port mode access/trunk) or Port Aggregation Protocol (PAgP) flap changes occur during a 30-second interval, or if 5 link-state (link up/down) changes occur during a 10-second interval:

```
Switch> show errdisable flap-values
ErrDisable Reason    Flaps    Time (sec)
-----------------    ------   ----------
pagp-flap              3        30
dtp-flap               3        30
link-flap              5        10
```

Related Commands

Command	Description
errdisable detect cause	Enables error-disabled detection for a specific cause or all causes.
show errdisable detect	Displays error-disabled detection status.
show errdisable recovery	Displays error-disabled recovery timer information.
show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

show errdisable recovery

Use the **show errdisable recovery** user EXEC command to display the error-disabled recovery timer information.

show errdisable recovery [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

A *gbic-invalid error-disable* reason refers to an invalid small form-factor pluggable (SFP) module interface.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show errdisable recovery** command:

```
Switch> show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Enabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Disabled
loopback             Disabled
```

```
Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface    Errdisable reason    Time left(sec)
---------    -----------------    --------------
Gi0/2        link-flap             279
```

Note Though visible in the output, the unicast-flood field is not valid.

Related Commands

Command	Description
errdisable recovery	Configures the recover mechanism variables.
show errdisable detect	Displays error-disabled detection status.
show errdisable flap-values	Displays error condition recognition information.
show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

show etherchannel

Use the **show etherchannel** user EXEC command to display EtherChannel information for a channel.

show etherchannel [*channel-group-number* {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 48.
detail	Display detailed EtherChannel information.
load-balance	Display the load-balance or frame-distribution scheme among ports in the port channel.
port	Display EtherChannel port information.
port-channel	Display port-channel information.
protocol	Display the protocol that is being used in the EtherChannel.
summary	Display a one-line summary per channel-group.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If you do not specify a *channel-group*, all channel groups are displayed.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show etherchannel 1 detail** command:

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
               Ports in the group:
               -------------------
Port: Gi0/1
------------

Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Active      Gcchange = -
Port-channel  = Po1         GC   =   -         Pseudo port-channel = Po1
```

```
Port index    = 0           Load = 0x00        Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port     Port
Port      Flags   State     Priority      Key       Key     Number   State
Gi0/1     SA      bndl      32768         0x1       0x1     0x101    0x3D
Gi0/2      A      bndl      32768         0x0       0x1     0x0      0x3D

Age of the port in the current state: 01d:20h:06m:04s

               Port-channels in the group:
               ----------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 01d:20h:20m:26s
Logical slot/port   = 10/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi0/1 Active          0
  0     00     Gi0/2 Active          0

Time since last port bundled:    01d:20h:20m:20s    Gi0/2
```

This is an example of output from the **show etherchannel 1 summary** command:

```
Switch> show etherchannel 1 summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        u - unsuitable for bundling
        U - in use      f - failed to allocate aggregator
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SU)         LACP      Gi0/1(P)  Gi0/2(P)
```

This is an example of output from the **show etherchannel 1 port-channel** command:

```
Switch> show etherchannel 1 port-channel
               Port-channels in the group:
               ----------------------
Port-channel: Po1    (Primary Aggregator)

------------

Age of the Port-channel   = 01d:20h:24m:50s
Logical slot/port   = 10/1          Number of ports = 2
HotStandBy port = null
```

```
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi0/1    Active          0
  0     00     Gi0/2    Active          0

Time since last port bundled:    01d:20h:24m:44s    Gi0/2
```

This is an example of output from **show etherchannel protocol** command:

```
Switch# show etherchannel protocol
                Channel-group listing:
                -----------------------
Group: 1
----------
Protocol:  LACP

Group: 2
----------
Protocol:  PAgP
```

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
channel-protocol	Restricts the protocol used on a port to manage channeling.
interface port-channel	Accesses or creates the port channel.

show fallback profile

Use the **show fallback profile** privileged EXEC command to display the fallback profiles that are configured on a switch.

show fallback profile [**append** | **begin** | **exclude** | **include** | {[**redirect** | **tee**] *url*} *expression*]

Syntax Description

| append	(Optional) Append redirected output to a specified URL
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
| redirect	(Optional) Copy output to a specified URL.
| tee	(Optional) Copy output to a specified URL.
expression	Expression in the output to use as a reference point.
url	Specified URL where output is directed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **show fallback** profile privileged EXEC command to display profiles that are configured on the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show fallback profile** command:

```
switch# show fall profile
Profile Name: dot1x-www
-----------------------------------
Description       : NONE
IP Admission Rule : webauth-fallback
IP Access-Group IN: default-policy
Profile Name: dot1x-www-lpip
-----------------------------------
Description       : NONE
IP Admission Rule : web-lpip
IP Access-Group IN: default-policy
Profile Name: profile1
-----------------------------------
Description       : NONE
IP Admission Rule : NONE
IP Access-Group IN: NONE
```

Related Commands

Command	Description
flowcontrol	Create a web authentication fallback profile.
ip admission	Enable web authentication on a switch port
ip admission name proxy http	Enable web authentication globally on a switch

show flowcontrol

Use the **show flowcontrol** user EXEC command to display the flow control status and statistics.

show flowcontrol [**interface** *interface-id* | **module** *number*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Display the flow control status and statistics for a specific interface.
module *number*	(Optional) Display the flow control status and statistics for all interfaces on the switch. The only valid module number is 1. This option is not available if you have entered a specific interface ID.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use this command to display the flow control status and statistics on the switch or for a specific interface.

Use the **show flowcontrol** command to display information about all the switch interfaces. For a standalone switch, the output from the **show flowcontrol** command is the same as the output from the **show flowcontrol module** *number* command.

Use the **show flowcontrol interface** *interface-id* command to display information about a specific interface.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show flowcontrol** command.

```
Switch> show flowcontrol
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Gi0/1      Unsupp.  Unsupp.  off      off         0       0
Gi0/2      desired  off      off      off         0       0
Gi0/3      desired  off      off      off         0       0
<output truncated>
```

This is an example of output from the **show flowcontrol interface** *interface-id* command:

```
Switch> show flowcontrol gigabitethernet0/2
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Gi0/2      desired  off      off      off         0       0
```

Related Commands

Command	Description
flowcontrol	Sets the receive flow-control state for an interface.

show idprom

Use the **show idprom** user EXEC command to display the IDPROM information for the specified interface.

show idprom {**interface** *interface-id*} [**detail**] [**|** {**begin | exclude | include**} *expression*]

Syntax Description

interface *interface-id*	Display the IDPROM information for the specified interface.
detail	(Optional) Display detailed hexidecimal IDPROM information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This command applies only to 10-Gigabit Ethernet interfaces and to the SFP module interfaces.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show idprom interface tengigabitethernet0/1** command for the 10-Gigabit Ethernet interface.

```
Switch# show idprom interface tengigabitethernet0/1
X2 Serial EEPROM Contents:
Non-Volatile Register (NVR) Fields
 X2 MSA Version supported :0xA
 NVR Size in bytes :0x100
 Number of bytes used :0x100
 Basic Field Address :0xB
 Customer Field Address :0x77
 Vendor Field Address :0xA7
 Extended Vendor Field Address :0x100
 Reserved :0x0
 Transceiver type :0x2 =X2
 Optical connector type :0x0 =Unspecified
 Bit encoding :0x1 =NRZ
 Normal BitRate in multiple of 1M b/s :0x2848
 Protocol Type :0x1 =10GgE
```

```
Standards Compliance Codes :
 10GbE Code Byte 0 :0x0 =Unspecified
 10GbE Code Byte 1 :0x0
 SONET/SDH Code Byte 0 :0x0
 SONET/SDH Code Byte 1 :0x0
 SONET/SDH Code Byte 2 :0x0
 SONET/SDH Code Byte 3 :0x0
 10GFC Code Byte 0 :0x0
 10GFC Code Byte 1 :0x0
 10GFC Code Byte 2 :0x0
 10GFC Code Byte 3 :0x0
 Transmission range in 10m :0x0
Fibre Type :
 Fibre Type Byte 0 :0x0 =Unspecified
 Fibre Type Byte 1 :0x0 =Unspecified

Centre Optical Wavelength in 0.01nm steps - Channel 0 :0x0 0x0 0x0
Centre Optical Wavelength in 0.01nm steps - Channel 1 :0x0 0x0 0x0
Centre Optical Wavelength in 0.01nm steps - Channel 2 :0x0 0x0 0x0
Centre Optical Wavelength in 0.01nm steps - Channel 3 :0x0 0x0 0x0
Package Identifier OUI :0xC09802
Transceiver Vendor OUI :0x3400B01
Transceiver vendor name :CISCO-OPNEXT,INC
Part number provided by transceiver vendor :TRTC010EN-BMC
Revision level of part number provided by vendor :00
Vendor serial number :OSA093900JK
Vendor manufacturing date code :2005092800

Reserved1 : 01 01 20 04 00 01 00
Basic Field Checksum :0x63

Customer Writable Area :
 0x00: 58 32 2D 31 30 47 42 2D 43 58 34 20 20 20 20 20
 0x10: 20 56 30 31 20 4F 53 41 30 39 33 39 30 30 4A 4B
 0x20: 31 30 2D 32 31 30 35 2D 30 31 20 20 41 30 20 20
Vendor Specific :
 0x00: 1F 01 1C 02 00 00 00 00 00 00 00 00 00 00 00 00
 0x10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x30: 00 00 01 00 11 B3 39 9F 5A 51 52 C3 2B 93 E2 A3
 0x40: 19 81 34 33 16 00 00 00 00 00 00 00 00 00 AC 76
 0x50: 37 FF 00 00 00 00 00 00 00
 F8-FF-FB, 3F-0F, 01-00
```

Related Commands

Command	Description
show controllers ethernet-controller	Displays per-interface send and receive statistics read from the hardware, interface internal registers, or port ASIC information.

show interfaces

Use the **show interfaces** privileged EXEC command to display the administrative and operational status of all interfaces or a specified interface.

show interfaces [*interface-id* | **vlan** *vlan-id*] [**accounting** | **capabilities** [**module** *number*] | **counters** | **description** | **etherchannel** | **flowcontrol** | **pruning** | **stats** | **status** [**err-disabled**] | **switchport** [**module** *number*] | **tengigabitethernet** *interface-id* | **transceiver** [**detail** | **properties** | **dom-supported-list**] [**module** *number*] | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

Note Although visible in the command-line help, the **private-vlan mapping** keyword is not supported.

Syntax Description

interface-id	(Optional) Valid interfaces include physical ports (including type and port number) and port channels. The port-channel range is 1 to 48.
vlan *vlan-id*	(Optional) VLAN identification. The range is 1 to 4094.
accounting	(Optional) Display accounting information on the interface, including active protocols and input and output packets and octets. **Note** The display shows only packets processed in software; hardware-switched packets do not appear.
capabilities	(Optional) Display the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
module *number*	(Optional) Display **capabilities**, **switchport** configuration, or **transceiver** characteristics (depending on preceding keyword) of all interfaces on the switch. The only valid module number is 1. This option is not available if you entered a specific interface ID.
counters	(Optional) See the **show interfaces counters** command.
description	(Optional) Display the administrative status and description set for an interface.
etherchannel	(Optional) Display interface EtherChannel information.
flowcontrol	(Optional) Display interface flowcontrol information
pruning	(Optional) Display interface trunk VTP pruning information.
stats	(Optional) Display the input and output packets by switching path for the interface.
status	(Optional) Display the status of the interface. A status of *unsupported* in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.
err-disabled	(Optional) Display interfaces in error-disabled state.
switchport	(Optional) Display the administrative and operational status of a switching (nonrouting) port.
tengigabitethernet	Display the status of a connected ten-gigabit module.

transceiver [**detail** | **properties** | **dom-supported-list**]	(Optional) Display the physical properties of a coarse wavelength-division multiplexer (CWDM) or dense wavelength-division multiplexer (DWDM) small form-factor (SFP) module interface. The keywords have these meanings: • **detail**—(Optional) Display calibration properties, including high and low numbers and any alarm information. • **properties**—(Optional) Display speed and duplex settings on an interface. • **dom-supported-list**—(Optional) Display the supported Digital Optical Monitoring (DOM) SFP modules.
trunk	Display interface trunk information. If you do not specify an interface, only information for active trunking ports appears.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **random-detect**, **rate-limit**, and **shape** keywords are not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interface capabilities module 1** command to display the capabilities of all interfaces on the switch. Any other number is invalid.
- Use the **show interfaces** *interface-id* **capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces on the switch.
- Use the **show interface switchport module 1** to display the switch port characteristics of all interfaces on the switch. Any other number is invalid.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show interfaces** command:

```
Switch# show interfaces gigabitethernet0/21
GigabitEthernet0/1 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 0023.acd1.4c01 (bia 0023.acd1.4c01)
  Description: test
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

This is an example of output from the **show interfaces accounting** command.

```
Switch# show interfaces accounting
Vlan1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                      IP    1094395  131900022     559555   84077157
           Spanning Tree     283896   17033760         42       2520
                     ARP      63738    3825680        231      13860
Interface Vlan2 is disabled
Vlan7
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
Vlan31
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.

GigabitEthernet0/1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet0/2
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.

<output truncated>
```

This is an example of output from the **show interfaces capabilities** command for an interface.

```
Switch# show interfaces gigabitethernet0/1 capabilities
GigabitEthernet0/1
    Model:                 WS-C2360-48TD
  Type:                  10/100/1000BaseTX
  Speed:                 10,100,1000,auto
  Duplex:                half,full,auto
  Trunk encap. type:     802.1Q
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off,on,desired),tx-(none)
  Fast Start:            yes
  QoS scheduling:        rx-(not configurable on per port basis),
                         tx-(4q3t) (3t: Two configurable values and one fixed.)
  CoS rewrite:           yes
  ToS rewrite:           yes
  UDLD:                  yes
  Inline power:          no
  SPAN:                  source/destination
  PortSecure:            yes
  Dot1x:                 yes
```

This is an example of output from the **show interfaces** *interface* **description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command.

```
Switch# show interfaces gigabitethernet0/2 description
Interface Status         Protocol Description
Gi0/2     up             down     Connects to Marketing
```

This is an example of output from the **show interfaces etherchannel** command when port channels are configured on the switch:

```
Switch# show interfaces etherchannel
-----
Port-channel1:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/1           Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel2:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/2           Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel3:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/3           Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
```

This is an example of output from the **show interfaces** *interface-id* **pruning** command when pruning is enabled in the VTP domain:

```
Switch# show interfaces gigibitethernet0/2 pruning
Port    Vlans pruned for lack of request by neighbor
Gi0/2     3,4

Port    Vlans traffic requested of neighbor
Gi0/2     1-3
```

This is an example of output from the **show interfaces stats** command for a specified VLAN interface.

```
Switch# show interfaces vlan 1 stats
Switching path    Pkts In   Chars In   Pkts Out  Chars Out
        Processor    1165354  136205310     570800   91731594
      Route cache          0          0          0          0
            Total    1165354  136205310     570800   91731594
```

This is an example of partial output from the **show interfaces status** command. It displays the status of all interfaces.

```
Switch# show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/1                        connected    routed     a-half  a-100 10/100/1000BaseTX
Gi0/2                        notconnect   121,40       auto   auto 10/100/1000BaseTX
Gi0/3                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/4                        notconnect   18           auto   auto Not Present
Gi0/5                        connected    121        a-full a-1000 10/100/1000BaseTX
Gi0/6                        connected    122,11     a-full a-1000 10/100/1000BaseTX

<output truncated>
Gi0/1                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/2                        notconnect   1            auto   auto unsupported

<output truncated>
```

These are examples of output from the **show interfaces status** command for a specific interface.

```
Switch# show interfaces gigabitethernet0/2 status
Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/2     test2              notconnect   1            auto   auto 10/100/1000Ba
seTX
```

This is an example of output from the **show interfaces status err-disabled** command. It displays the status of interfaces in the error-disabled state.

```
Switch# show interfaces status err-disabled
Port      Name               Status        Reason
Gi0/2                        err-disabled gbic-invalid
Gi0/3                        err-disabled dtp-flap
```

This is an example of output from the **show interfaces switchport** command for a port. Table 2-9 describes the fields in the display.

```
Switch# show interfaces gigabitethernet0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
```

```
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: NONE
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Table 2-9 show interfaces switchport Field Descriptions

Field	Description
Name	Displays the port name.
Switchport	Displays the administrative and operational status of the port. In this display, the port is in switchport mode.
Administrative Mode Operational Mode	Displays the administrative and operational modes.
Administrative Trunking Encapsulation Operational Trunking Encapsulation Negotiation of Trunking	Displays the administrative and operational encapsulation method and whether trunking negotiation is enabled.
Access Mode VLAN	Displays the VLAN ID to which the port is configured.
Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active	Lists the VLAN ID of the trunk that is in native mode. Lists the allowed VLANs on the trunk. Lists the active VLANs on the trunk.
Pruning VLANs Enabled	Lists the VLANs that are pruning-eligible.
Protected	Not applicable on this switch.
Unknown unicast blocked Unknown multicast blocked	Displays whether or not unknown multicast and unknown unicast traffic is blocked on the interface.
Voice VLAN	Not applicable on this switch.
Administrative private-vlan host-association	Not applicable on this switch.
Administrative private-vlan mapping	Not applicable on this switch.
Operational private-vlan	Not applicable on this switch.
Appliance trust	Displays the class of service (CoS) setting of the data packets of the connected device.

This is an example of output from the **show interfaces** *interface-id* **pruning** command:

```
Switch# show interfaces gigibitethernet0/2 pruning
Port    Vlans pruned for lack of request by neighbor
```

This is an example of output from the **show interfaces** *interface-id* **trunk** command. It displays trunking information for the port.

```
Switch# show interfaces gigabitethernet0/1 trunk
Port          Mode         Encapsulation  Status        Native vlan
Gi0/1       auto         negotiate      trunking      1

Port          Vlans allowed on trunk
Gi0/1       1-4094

Port          Vlans allowed and active in management domain
Gi0/1       1-4

Port          Vlans in spanning tree forwarding state and not pruned
Gi0/1        1-4
```

This is an example of output from the **show interfaces** *interface-id* **transceiver properties** command:

```
Switch# show interfaces gigabitethernet0/1 transceiver properties
Name : Gi0/1
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: enable
Operational Duplex: auto
Administrative Auto-MDIX: off
Operational Auto-MDIX: off
```

This is an example of output from the **show interfaces** *interface-id* **transceiver detail** command:

```
Switch# show interfaces gigabitethernet0/3 transceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is externally calibrated.
mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
++:high alarm, +:high warning, -:low warning, -- :low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are uncalibrated.

                          High Alarm  High Warn  Low Warn   Low Alarm
        Temperature       Threshold   Threshold  Threshold  Threshold
Port     (Celsius)        (Celsius)   (Celsius)  (Celsius)  (Celsius)
------- ----------------  ----------  ---------  ---------  ---------
Gi0/3   41.5              110.0       103.0      -8.0       -12.0

                          High Alarm  High Warn  Low Warn   Low Alarm
         Voltage          Threshold   Threshold  Threshold  Threshold
Port     (Volts)          (Volts)     (Volts)    (Volts)    (Volts)
-------  ---------------  ----------  ---------  ---------  ---------
Gi0/3    3.20             4.00        3.70       3.00       2.95

                          High Alarm  High Warn  Low Warn   Low Alarm
         Current          Threshold   Threshold  Threshold  Threshold
Port     (milliamperes)   (mA)        (mA)       (mA)       (mA)
-------  ---------------  ----------  ---------  ---------  ---------
Gi0/3    31.0             84.0        70.0       4.0        2.0

         Optical          High Alarm  High Warn  Low Warn   Low Alarm
         Transmit Power   Threshold   Threshold  Threshold  Threshold
Port     (dBm)            (dBm)       (dBm)      (dBm)      (dBm)
-------  ---------------  ----------  ---------  ---------  ---------
Gi0/3    -0.0 ( -0.0)     -0.0        -0.0       -0.0       -0.0

         Optical          High Alarm  High Warn  Low Warn   Low Alarm
         Receive Power    Threshold   Threshold  Threshold  Threshold
```

```
Port     (dBm)              (dBm)       (dBm)       (dBm)       (dBm)
-------  -----------------  ----------  ----------  ----------  ----------
Gi0/3    N/A  ( -0.0) --    -0.0        -0.0        -0.0        -0.0
```

This is an example of output from the **show interfaces tengigabitethernet** *interface-id* **transceiver detail** command:

```
Switch# show interfaces tengigabitethernet0/1 transceiver detail
Transceiver monitoring is disabled for all interfaces.

ITU Channel not available (Wavelength not available),
Transceiver is internally calibrated.
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.
High Alarm High Warn Low Warn Low Alarm
Temperature Threshold Threshold Threshold Threshold
Port (Celsius) (Celsius) (Celsius) (Celsius) (Celsius)
--------- ------------------ ---------- --------- --------- ---------
Te0/1 26.8 70.0 60.0 5.0 0.0
High Alarm High Warn Low Warn Low Alarm
Voltage Threshold Threshold Threshold Threshold
Port (Volts) (Volts) (Volts) (Volts) (Volts)
--------- --------------- ---------- --------- --------- ---------
Te0/1 3.15 3.63 3.63 2.97 2.97
High Alarm High Warn Low Warn Low Alarm
Current Threshold Threshold Threshold Threshold
Port (milliamperes) (mA) (mA) (mA) (mA)
--------- ----------------- ---------- --------- --------- ---------
Te0/1 5.0 16.3 15.3 3.9 3.2
Optical High Alarm High Warn Low Warn Low Alarm
Transmit Power Threshold Threshold Threshold Threshold
Port (dBm) (dBm) (dBm) (dBm) (dBm)
--------- ----------------- ---------- --------- --------- ---------
Te0/1 -1.9 1.0 0.5 -8.2 -8.5
Optical High Alarm High Warn Low Warn Low Alarm
Receive Power Threshold Threshold Threshold Threshold
Port (dBm) (dBm) (dBm) (dBm) (dBm)
------- ----------------- ---------- --------- --------- ---------
Te0/1 -1.4 1.0 0.5 -14.1 -15.0
```

This is an example of output from the **show interfaces tengigabitethernet** *interface-id* **transceiver properties** command:

```
Switch# show interfaces tengigabitethernet0/1 transceiver properties
Transceiver monitoring is disabled for all interfaces.

ITU Channel not available (Wavelength not available),
Transceiver is internally calibrated.
Name : Te0/1
Administrative Speed: 10000
Administrative Duplex: full
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
Operational Speed: 10000
Operational Duplex: full
Operational Auto-MDIX: off
Media Type: 10GBase-LR
```

This is an example of output from the **show interfaces transceiver dom-supported-list** command:

```
Transceiver Type           Cisco p/n min version
                               supporting DOM
------------------       -------------------------

   DWDM GBIC                ALL
   DWDM SFP                 ALL
   RX only WDM GBIC         ALL
   DWDM XENPAK              ALL
   DWDM X2                  ALL
   DWDM XFP                 ALL
   CWDM GBIC                NONE
   CWDM X2                  ALL
   CWDM XFP                 ALL
   XENPAK ZR                ALL
   X2 ZR                    ALL
   XFP ZR                   ALL
   Rx_only_WDM_XENPAK       ALL
   XENPAK_ER                10-1888-03
   X2_ER                    ALL
   XFP_ER                   ALL
   XENPAK_LR                10-1838-04
   X2_LR                    ALL
   XFP_LR                   ALL
   XENPAK_LW                ALL
   X2_LW                    ALL
   XFP_LW                   NONE
   XENPAK SR                NONE
   X2 SR                    ALL
   XFP SR                   ALL
   XENPAK LX4               NONE
   X2 LX4                   NONE
   XFP LX4                  NONE
   XENPAK CX4               NONE
   X2 CX4                   NONE
   SX GBIC                  NONE
   LX GBIC                  NONE
   ZX GBIC                  NONE
   CWDM_SFP                 ALL
   Rx_only_WDM_SFP          NONE
   SX_SFP                   ALL
   LX_SFP                   ALL
   ZX_SFP                   ALL
   SX SFP                   NONE
   LX SFP                   NONE
   ZX SFP                   NONE
   GIgE BX U SFP            NONE
   GigE BX D SFP            ALL
```

Related CommandsT

Command	Description
switchport access	Configures a port as a static-access or a dynamic-access port.
switchport mode	Configures the VLAN membership mode of a port.
switchport trunk pruning	Configures the VLAN pruning-eligible list for ports in trunking mode.

show interfaces counters

Use the **show interfaces counters** privileged EXEC command to display various counters for the switch or for a specific interface.

show interfaces [*interface-id* | **vlan** *vlan-id*] **counters** [**errors** | **etherchannel** | **module** *module-number* | **protocol status** | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the physical interface, including type and port number.
errors	(Optional) Display error counters.
etherchannel	(Optional) Display EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.
module *number*	(Optional) On the Catalyst 2360 switch, the module number is always 1
protocol status	(Optional) Display status of protocols enabled on interfaces.
trunk	(Optional) Display trunk counters.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If you do not enter any keywords, all counters for all interfaces are included.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of partial output from the **show interfaces counters** command. It displays all counters for the switch.

```
Switch# show interfaces counters
Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Gi0/1                  0             0             0             0
Gi0/2                  0             0             0             0

<output truncated>
```

This is an example of partial output from the **show interfaces counters protocol status** command for all interfaces.

```
Switch# show interfaces counters protocol status
Protocols allocated:
 Vlan1: Other, IP
 Vlan20: Other, IP, ARP
 Vlan30: Other, IP, ARP
 Vlan40: Other, IP, ARP
 Vlan50: Other, IP, ARP
 Vlan60: Other, IP, ARP
 Vlan70: Other, IP, ARP
 Vlan80: Other, IP, ARP
 Vlan90: Other, IP, ARP
 Vlan900: Other, IP, ARP
 Vlan3000: Other, IP
 Vlan3500: Other, IP
 GigabitEthernet0/1: Other, IP, ARP, CDP
 GigabitEthernet0/2: Other, IP
 GigabitEthernet0/3: Other, IP
 GigabitEthernet0/4: Other, IP
 GigabitEthernet0/5: Other, IP
 GigabitEthernet0/6: Other, IP
 GigabitEthernet0/7: Other, IP
 GigabitEthernet0/8: Other, IP
 GigabitEthernet0/9: Other, IP
 GigabitEthernet0/10: Other, IP, CDP

<output truncated>
```

This is an example of output from the **show interfaces counters trunk** command. It displays trunk counters for all interfaces.

```
Switch# show interfaces counters trunk
Port        TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi0/1               0              0           0
Gi0/2               0              0           0
Gi0/3           80678           4155           0
Gi0/4           82320            126           0
Gi0/5               0              0           0

<output truncated>
```

Related Commands

Command	Description
show interfaces	Displays additional interface characteristics.

show interfaces transceivers

Use the **show interfaces transceivers** privileged EXEC command to display the physical properties of a small form-factor pluggable (SFP) module interface.

show interfaces [*interface-id]* **transceiver** [**detail | dom-supported-list | module** *number* **| properties | threshold-table**] [| {**begin | exclude | include**} *expression*]

Syntax Description

interface-id	(Optional) Display configuration and status for a specified physical interface.
detail	(Optional) Display calibration properties, including high and low numbers and any alarm information for any Digital Optical Monitoring (DoM)-capable transceiver if one is installed in the switch.
dom-supported-list	(Optional) List all supported DoM transceivers.
module *number*	(Optional) Limit display to interfaces on module on the switch. The range is 1 to 9. This option is not available if you entered a specific interface ID.
properties	(Optional) Display speed, and duplex settings on an interface.
threshold-table	(Optional) Display alarm and warning threshold table
| begin	(Optional) Display begins with the line that matches the *expression*
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show interfaces** *interface-id* **transceiver properties** command:

```
Switch# show interfaces gigabitethernet0/1 transceiver properties
Name : Gi0/1
Administrative Speed: auto
Administrative Duplex: auto
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
Operational Speed: auto
Operational Duplex: auto
Operational Auto-MDIX: on
Media Type: 10/100/1000BaseTX
```

This is an example of output from the **show interfaces** *interface-id* **transceiver detail** command:

```
Switch# show interfaces gigabitethernet0/3 transceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is externally calibrated.
mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
++:high alarm, +:high warning, -:low warning, -- :low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are uncalibrated.

                           High Alarm  High Warn  Low Warn   Low Alarm
        Temperature        Threshold   Threshold  Threshold  Threshold
Port     (Celsius)         (Celsius)   (Celsius)  (Celsius)  (Celsius)
------- ------------------  ----------  ---------  ---------  ---------
Gi0/3 41.5                110.0       103.0      -8.0       -12.0

                           High Alarm  High Warn  Low Warn   Low Alarm
         Voltage           Threshold   Threshold  Threshold  Threshold
Port     (Volts)           (Volts)     (Volts)    (Volts)    (Volts)
-------  ---------------    ----------  ---------  ---------  ---------
Gi0/3  3.20                4.00        3.70       3.00       2.95

                           High Alarm  High Warn  Low Warn   Low Alarm
         Current           Threshold   Threshold  Threshold  Threshold
Port     (milliamperes)    (mA)        (mA)       (mA)       (mA)
-------  -----------------  ----------  ---------  ---------  ---------
Gi0/3  31.0                84.0        70.0       4.0        2.0

         Optical           High Alarm  High Warn  Low Warn   Low Alarm
         Transmit Power    Threshold   Threshold  Threshold  Threshold
Port     (dBm)             (dBm)       (dBm)      (dBm)      (dBm)
-------  -----------------  ----------  ---------  ---------  ---------
Gi0/3  -0.0 ( -0.0)       -0.0        -0.0       -0.0       -0.0

         Optical           High Alarm  High Warn  Low Warn   Low Alarm
         Receive Power     Threshold   Threshold  Threshold  Threshold
Port     (dBm)             (dBm)       (dBm)      (dBm)      (dBm)
-------  -----------------  ----------  ---------  ---------  ---------
Gi0/3  N/A  ( -0.0) --    -0.0        -0.0       -0.0       -0.0
```

This is an example of output from the **show interfaces transceiver dom-supported-list** command:

```
Switch# show interfaces transceiver dom-supported-list
Transceiver Type           Cisco p/n min version
                               supporting DOM
------------------       -------------------------

   DWDM GBIC                ALL
   DWDM SFP                 ALL
   RX only WDM GBIC         ALL
   DWDM XENPAK              ALL
   DWDM X2                  ALL
   DWDM XFP                 ALL
   CWDM GBIC                NONE
   CWDM X2                  ALL
   CWDM XFP                 ALL
   XENPAK ZR                ALL
   X2 ZR                    ALL
   XFP ZR                   ALL
   Rx_only_WDM_XENPAK       ALL
   XENPAK_ER                10-1888-03
   X2_ER                    ALL
   XFP_ER                   ALL
   XENPAK_LR                10-1838-04
```

```
   X2_LR                    ALL
   XFP_LR                   ALL
   XENPAK_LW                ALL
   X2_LW                    ALL
   XFP_LW                   NONE
   XENPAK SR                NONE
   X2 SR                    ALL
   XFP SR                   ALL
   XENPAK LX4               NONE
   X2 LX4                   NONE
   XFP LX4                  NONE
   XENPAK CX4               NONE
   X2 CX4                   NONE
   SX GBIC                  NONE
   LX GBIC                  NONE
   ZX GBIC                  NONE
   CWDM_SFP                 ALL
   Rx_only_WDM_SFP          NONE
   SX_SFP                   ALL
   LX_SFP                   ALL
   ZX_SFP                   ALL
   SX SFP                   NONE
   LX SFP                   NONE
   ZX SFP                   NONE
   GIgE BX U SFP            NONE
   GigE BX D SFP            ALL
```

This is an example of output from the **show interfaces transceiver threshold-table** command:

```
Optical Tx     Optical Rx    Temp     Laser Bias    Voltage
                                                    current
             -------------  -------------  ------   ------------  ---------

 DWDM GBIC
Min1             -0.50        -28.50        0            N/A          4.50
Min2             -0.30        -28.29        5            N/A          4.75
Max2              3.29         -6.69        60           N/A          5.25
Max1              3.50          6.00        70           N/A          5.50
 DWDM SFP
Min1             -0.50        -28.50        0            N/A          3.00
Min2             -0.30        -28.29        5            N/A          3.09
Max2              4.30         -9.50        60           N/A          3.59
Max1              4.50          9.30        70           N/A          3.70
 RX only WDM GBIC
Min1              N/A         -28.50        0            N/A          4.50
Min2              N/A         -28.29        5            N/A          4.75
Max2              N/A          -6.69        60           N/A          5.25
Max1              N/A           6.00        70           N/A          5.50
 DWDM XENPAK
Min1             -1.50        -24.50        0            N/A          N/A
Min2             -1.29        -24.29        5            N/A          N/A
Max2              3.29         -6.69        60           N/A          N/A
Max1              3.50          4.00        70           N/A          N/A
 DWDM X2
Min1             -1.50        -24.50        0            N/A          N/A
Min2             -1.29        -24.29        5            N/A          N/A
Max2              3.29         -6.69        60           N/A          N/A
Max1              3.50          4.00        70           N/A          N/A
 DWDM XFP
Min1             -1.50        -24.50        0            N/A          N/A
Min2             -1.29        -24.29        5            N/A          N/A
Max2              3.29         -6.69        60           N/A          N/A
Max1              3.50          4.00        70           N/A          N/A
```

```
 CWDM X2
Min1                N/A             N/A             0               N/A             N/A
Min2                N/A             N/A             0               N/A             N/A
Max2                N/A             N/A             0               N/A             N/A
Max1                N/A             N/A             0               N/A             N/A
```

Related Commands

Command	Description
show interfaces	Displays additional interface characteristics.

show inventory

Use the **show inventory** user EXEC command to display product identification (PID) information for the hardware.

show inventory [*entity-name* | **raw**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

entity-name	(Optional) Display the specified entity. For example, enter the interface (such as gigabitethernet0/1) into which a small form-factor pluggable (SFP) module is installed.
raw	(Optional) Display every entity in the device.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The command is case sensitive. With no arguments, the **show inventory** command produces a compact dump of all identifiable entities that have a product identifier. The compact dump displays the entity location (slot identity), entity description, and the unique device identifier (UDI) (PID, VID, and SN) of that entity.

Note If there is no PID, no output appears when you enter the **show inventory** command.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is example output from the **show inventory** command:

```
Switch> show inventory
NAME: "5", DESCR: "WS-C2360-48TD-SD"
PID: WS-C2360-48TD-SD , VID: E0 , SN: CAT0749R204
```

show ip igmp profile

Use the **show ip igmp profile** privileged EXEC command to display all configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile.

show ip igmp profile [*profile number*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

profile number	(Optional) The IGMP profile number to be displayed. The range is 1 to 4294967295. If no profile number is entered, all IGMP profiles are displayed.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

These are examples of output from the **show ip igmp profile** privileged EXEC command, with and without specifying a profile number. If no profile number is entered, the display includes all profiles configured on the switch.

```
Switch# show ip igmp profile 40
IGMP Profile 40
    permit
    range 233.1.1.1 233.255.255.255

Switch# show ip igmp profile
IGMP Profile 3
    range 230.9.9.0 230.9.9.0
IGMP Profile 4
    permit
    range 229.9.9.0 229.255.255.255
```

Related Commands

Command	Description
ip igmp profile	Configures the specified IGMP profile number.

show ip igmp snooping

Use the **show ip igmp snooping** user EXEC command to display the Internet Group Management Protocol (IGMP) snooping configuration of the switch or the VLAN.

show ip igmp snooping [**detail** | **groups** | **mrouter** | **querier**] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

detail	(Optional) Display IGMP snooping operational state information.
groups	(Optional) See the **show ip igmp snooping groups** command.
mrouter	(Optional) See the **show ip igmp snooping mrouter** command.
querier	(Optional) See the **show ip igmp snooping querier** command.
vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094 (available only in privileged EXEC mode).
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use this command to display snooping configuration for the switch or for a specific VLAN.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN.

```
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             :Enabled
IGMPv3 snooping (minimal) :Enabled
Report suppression        :Enabled
TCN solicit query         :Disabled
TCN flood query count     :2
Last member query interval : 100
```

```
Vlan 1:
--------
IGMP snooping                          :Enabled
Immediate leave                        :Disabled
Multicast router learning mode         :pim-dvmrp
Source only learning age timer         :10
CGMP interoperability mode             :IGMP_ONLY
Last member query interval : 100
```

This is an example of output from the **show ip igmp snooping** command. It displays snooping characteristics for all VLANs on the switch.

```
Switch> show ip igmp snooping
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping               : Enabled
IGMPv3 snooping (minimal)   : Enabled
Report suppression          : Enabled
TCN solicit query           : Disabled
TCN flood query count       : 2
Last member query interval : 100

Vlan 1:
--------
IGMP snooping                          :Enabled
Immediate leave                        :Disabled
Multicast router learning mode         :pim-dvmrp
Source only learning age timer         :10
CGMP interoperability mode             :IGMP_ONLY
Last member query interval             : 100

Vlan 2:
--------
IGMP snooping                          :Enabled
Immediate leave                        :Disabled
Multicast router learning mode         :pim-dvmrp
Source only learning age timer         :10
CGMP interoperability mode             :IGMP_ONLY
Last member query interval             : 333

<output truncated>
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping last-member-query-interval	Enables the IGMP snooping configurable-leave timer.
ip igmp snooping querier	Enables the IGMP querier function in Layer 2 networks.
ip igmp snooping report-suppression	Enables IGMP report suppression.
ip igmp snooping tcn	Configures the IGMP topology change notification behavior.
ip igmp snooping tcn flood	Specifies multicast flooding as the IGMP spanning-tree topology change notification behavior.
ip igmp snooping vlan immediate-leave	Enables IGMP snooping immediate-leave processing on a VLAN.
ip igmp snooping vlan static	Adds a multicast router port or configures the multicast learning method.

Command	Description
ip igmp snooping vlan static	Statically adds a Layer 2 port as a member of a multicast group.
show ip igmp snooping groups	Displays the IGMP snooping multicast table for the switch.
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier configured on a switch.

show ip igmp snooping groups

Use the **show ip igmp snooping groups** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping multicast table for the switch or the multicast information. Use with the **vlan** keyword to display the multicast table for a specified multicast VLAN or specific multicast information.

show ip igmp snooping groups [**count** | **dynamic** [**count**] | **user** [**count**]] [| {**begin** | **exclude** | **include**} *expression*]

show ip igmp snooping groups vlan *vlan-id* [*ip_address* | **count** | **dynamic** [**count**] | **user** [**count**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

count	(Optional) Display the total number of entries for the specified command options instead of the actual entries.
dynamic	(Optional) Display entries learned by IGMP snooping.
user	Optional) Display only the user-configured multicast entries.
ip_address	(Optional) Display characteristics of the multicast group with the specified group IP address.
vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use this command to display multicast information or the multicast table.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the switch.

```
Switch# show ip igmp snooping groups
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
1         224.1.4.4       igmp                    Gi0/11
1         224.1.4.5       igmp                    Gi0/11
2         224.0.1.40      igmp        v2          Gi0/15
104       224.1.4.2       igmp        v2          Gi0/1, Gi0/2
104       224.1.4.3       igmp        v2          Gi0/1, Gi0/2
```

This is an example of output from the **show ip igmp snooping groups count** command. It displays the total number of multicast groups on the switch.

```
Switch# show ip igmp snooping groups count
Total number of multicast groups: 2
```

This is an example of output from the **show ip igmp snooping groups dynamic** command. It shows only the entries learned by IGMP snooping.

```
Switch# show ip igmp snooping groups vlan 1 dynamic
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1, Gi0/15
104       224.1.4.3       igmp        v2          Gi0/1, Gi0/15
```

This is an example of output from the **show ip igmp snooping groups vlan** *vlan-id ip-address* command. It shows the entries for the group with the specified IP address.

```
Switch# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1, Gi0/15
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping vlan static	Configures a multicast router port.
ip igmp snooping vlan static	Statically adds a Layer 2 port as a member of a multicast group.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

show ip igmp snooping mrouter

Use the **show ip igmp snooping mrouter** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the switch or for the specified multicast VLAN.

show ip igmp snooping mrouter [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use this command to display multicast router ports on the switch or for a specific VLAN.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

When multicast VLAN registration (MVR) is enabled, the **show ip igmp snooping mrouter** command displays MVR multicast router information and IGMP snooping information.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip igmp snooping mrouter** command. It shows how to display multicast router ports on the switch.

```
Switch# show ip igmp snooping mrouter
Vlan    ports
----    -----
   1    Gi0/1(dynamic)
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping vlan static	Adds a multicast router port.
ip igmp snooping vlan static	Statically adds a Layer 2 port as a member of a multicast group.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN
show ip igmp snooping groups	Displays IGMP snooping multicast information for the switch or for the specified parameter.

show ip igmp snooping querier

Use the **show ip igmp snooping querier detail** user EXEC command to display the configuration and operation information for the IGMP querier configured on a switch.

show ip igmp snooping querier [**detail** | **vlan** *vlan-id* [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

detail	Optional) Display detailed IGMP querier information.
vlan *vlan-id* [**detail**]	Optional) Display IGMP querier information for the specified VLAN. The range is 1 to 1001 and 1006 to 4094. Use the **detail** keyword to display detailed information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **show ip igmp snooping querier** command to display the IGMP version and the IP address of a detected device, also called a *querier*, that sends IGMP query messages. A subnet can have multiple multicast routers but has only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 switch.

The **show ip igmp snooping querier** command output also shows the VLAN and the interface on which the querier was detected. If the querier is the switch, the output shows the *Port* field as *Router.* If the querier is a router, the output shows the port number on which the querier is learned in the *Port* field.

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier** command displays only the device IP address most recently detected by the switch querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the switch querier and this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the switch querier (if any) that is configured in the VLAN

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip igmp snooping querier** command:

```
Switch> show ip igmp snooping querier
Vlan      IP Address      IGMP Version        Port
--------------------------------------------------
1         172.20.50.11    v3                  Gi0/1
2         172.20.40.20    v2                  Router
```

This is an example of output from the **show ip igmp snooping querier detail** command:

```
Switch> show ip igmp snooping querier detail
Vlan      IP Address      IGMP Version    Port
-----------------------------------------------------------
1         1.1.1.1         v2              Gi0/1

Global IGMP switch querier status
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 0.0.0.0
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10

Vlan 1:   IGMP switch querier status

-----------------------------------------------------------
elected querier is 1.1.1.1          on port Gi0/1
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping querier	Enables the IGMP querier function in Layer 2 networks.
show ip igmp snooping	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

show ipv6 mld snooping

Use the **show ipv6 mld snooping** user EXEC command to display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN.

show ipv6 mld snooping [**vlan** *vlan-id*] [**|** {**begin** | **exclude** | **include**} *expression*]

Note This command is available only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use this command to display MLD snooping configuration for the switch or for a specific VLAN.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ipv6 mld snooping vlan** command. It shows snooping characteristics for a specific VLAN.

```
Switch> show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
-----------------------------------------
MLD snooping                  : Enabled
MLDv2 snooping (minimal)      : Enabled
Listener message suppression  : Enabled
TCN solicit query             : Disabled
TCN flood query count         : 2
Robustness variable           : 3
Last listener query count     : 2
Last listener query interval  : 1000

Vlan 100:
--------
```

```
MLD snooping                          : Disabled
MLDv1 immediate leave                 : Disabled
Explicit host tracking                : Enabled
Multicast router learning mode        : pim-dvmrp
Robustness variable                   : 3
Last listener query count             : 2
Last listener query interval          : 1000
```

This is an example of output from the **show ipv6 mld snooping** command. It displays snooping characteristics for all VLANs on the switch.

```
Switch> show ipv6 mld snooping
Global MLD Snooping configuration:
-----------------------------------------
MLD snooping                  : Enabled
MLDv2 snooping (minimal)      : Enabled
Listener message suppression  : Enabled
TCN solicit query             : Disabled
TCN flood query count         : 2
Robustness variable           : 3
Last listener query count     : 2
Last listener query interval  : 1000

Vlan 1:
--------
MLD snooping                          : Disabled
MLDv1 immediate leave                 : Disabled
Explicit host tracking                : Enabled
Multicast router learning mode        : pim-dvmrp
Robustness variable                   : 1
Last listener query count             : 2
Last listener query interval          : 1000

<output truncated>

Vlan 951:
--------
MLD snooping                          : Disabled
MLDv1 immediate leave                 : Disabled
Explicit host tracking                : Enabled
Multicast router learning mode        : pim-dvmrp
Robustness variable                   : 3
Last listener query count             : 2
Last listener query interval          : 1000
```

Related Commands

Command	Description
ipv6 mld snooping	Enables and configures MLD snooping on the switch or on a VLAN.

show ipv6 mld snooping address

Use the **show ipv6 mld snooping address** user EXEC command to display all or specified IP Version 6 (IPv6) multicast address information maintained by Multicast Listener Discovery (MLD) snooping.

show ipv6 mld snooping address [[**vlan** *vlan-id*] [*ipv6 address*]] [**vlan** *vlan-id*] [**count** | **dynamic** | **user**] [| {**begin** | **exclude** | **include**} *expression*]

Note This command is available only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN about which to show MLD snooping multicast address information. The VLAN ID range is 1 to 1001 and 1006 to 4094.
ipv6-multicast-address	(Optional) Display information about the specified IPv6 multicast address. This keyword is only available when a VLAN ID is entered.
count	(Optional) Display the number of multicast groups on the switch or in the specified VLAN.
dynamic	(Optional) Display MLD snooping learned group information.
user	(Optional) Display MLD snooping user-configured group information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use this command to display IPv6 multicast address information.

You can enter an IPv6 multicast address only after you enter a VLAN ID.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Use the **dynamic** keyword to display information only about groups that are learned. Use the **user** keyword to display information only about groups that have been configured.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show snooping address** user EXEC command:

```
Switch> show ipv6 mld snooping address
Vlan Group   Type Version Port List
------------------------------------------------------------
2    FF12::3 user         Gi0/2, Gi0/2, Gi0/1,Gi0/3
```

This is an example of output from the **show snooping address count** user EXEC command:

```
Switch> show ipv6 mld snooping address count
Total number of multicast groups: 2
```

This is an example of output from the **show snooping address user** user EXEC command:

```
Switch> show ipv6 mld snooping address user
Vlan Group  Type Version Port List
------------------------------------------------------------
2    FF12::3 user  v2    Gi0/2, Gi0/2, Gi0/1,Gi0/3
```

Related Commands

Command	Description
ipv6 mld snooping vlan	Configures IPv6 MLD snooping on a VLAN.

show ipv6 mld snooping mrouter

Use the **show ipv6 mld snooping mrouter** user EXEC command to display dynamically learned and manually configured IP version 6 (IPv6) Multicast Listener Discovery (MLD) router ports for the switch or a VLAN.

show ipv6 mld snooping mrouter [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Note This command is available only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use this command to display MLD snooping router ports for the switch or for a specific VLAN.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ipv6 mld snooping mrouter** command. It displays snooping characteristics for all VLANs on the switch that are participating in MLD snooping.

```
Switch> show ipv6 mld snooping mrouter
Vlan    ports
----    -----
   2    Gi0/11(dynamic)
  72    Gi0/11(dynamic)
 200    Gi0/11(dynamic)
```

This is an example of output from the **show ipv6 mld snooping mrouter vlan** command. It shows multicast router ports for a specific VLAN.

```
Switch> show ipv6 mld snooping mrouter vlan 100
Vlan    ports
----    -----
```

```
2     Gi0/11(dynamic)
```

Related Commands

Command	Description
ipv6 mld snooping	Enables and configures MLD snooping on the switch or on a VLAN.
ipv6 mld snooping vlan mrouter interface *interface-id* | **static** *ipv6-multicast-address* **interface** *interface-id*]	Configures multicast router ports for a VLAN.

show ipv6 mld snooping querier

Use the **show ipv6 mld snooping querier** user EXEC command to display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping querier-related information most recently received by the switch or the VLAN.

show ipv6 mld snooping querier [**vlan** *vlan-id*] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

Note This command is available only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
detail	(Optional) Display MLD snooping detailed querier information for the switch or for the VLAN.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **show ipv6 mld snooping querier** command to display the MLD version and IPv6 address of a detected device that sends MLD query messages, which is also called a *querier*. A subnet can have multiple multicast routers but has only one MLD querier. The querier can be a Layer 3 switch.

The **show ipv6 mld snooping querier** command output also shows the VLAN and interface on which the querier was detected. If the querier is the switch, the output shows the *Port* field as *Router*. If the querier is a router, the output shows the port number on which the querier is learned in the *Port* field.

The output of the **show ipv6 mld snoop querier vlan** command displays the information received in response to a query message from an external or internal querier. It does not display user-configured VLAN values, such as the snooping robustness variable on the particular VLAN. This querier information is used only on the MASQ message that is sent by the switch. It does not override the user-configured robustness variable that is used for aging out a member that does not respond to query messages.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ipv6 mld snooping querier** command:

```
Switch> show ipv6 mld snooping querier
Vlan      IP Address               MLD Version Port
------------------------------------------------------------
2         FE80::201:C9FF:FE40:6000 v1          Gi0/1
```

This is an example of output from the **show ipv6 mld snooping querier detail** command:

```
Switch> show ipv6 mld snooping querier detail
Vlan      IP Address               MLD Version Port
------------------------------------------------------------
2        FE80::201:C9FF:FE40:6000 v1           Gi0/1
```

This is an example of output from the **show ipv6 mld snooping querier vlan** command:

```
Switch> show ipv6 mld snooping querier vlan 2
IP address : FE80::201:C9FF:FE40:6000
MLD version : v1
Port : Gi0/1
Max response time : 1000s
```

Related Commands

Command	Description
ipv6 mld snooping	Enables and configures IPv6 MLD snooping on the switch or on a VLAN.
ipv6 mld snooping last-listener-query-count	Configures the maximum number of queries that the switch sends before aging out an MLD client.
ipv6 mld snooping last-listener-query-interval	Configures the maximum response time after sending out a query that the switch waits before deleting a port from the multicast group.
ipv6 mld snooping robustness-variable	Configures the maximum number of queries that the switch sends before aging out a multicast address when there is no response.
ipv6 mld snooping	Enables and configures IPv6 MLD snooping on the switch or on a VLAN.

show lacp

Use the **show lacp** user EXEC command to display Link Aggregation Control Protocol (LACP) channel-group information.

show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor** | **sys-id**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 48.
counters	Display traffic information.
internal	Display internal information.
neighbor	Display neighbor information.
sys-id	Display the system identifier that is being used by LACP. The system identifier is made up of the LACP system priority and the switch MAC address.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can enter any **show lacp** command to display the active channel-group information. To display specific channel information, enter the **show lacp** command with a channel-group number.

If you do not specify a channel group, information for all channel groups appears.

You can enter the *channel-group-number* option to specify a channel group for all keywords except **sys-id**.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show lacp counters** user EXEC command. Table 2-10 describes the fields in the display.

```
Switch> show lacp counters
               LACPDUs          Marker      Marker Response    LACPDUs
Port          Sent    Recv     Sent    Recv     Sent    Recv      Pkts Err
--------------------------------------------------------------------------
Channel group:1
Gi0/1         19      10       0       0        0       0         0
Gi0/2         14      6        0       0        0       0         0
```

Table 2-10 show lacp counters Field Descriptions

Field	Description
LACPDUs Sent and Recv	The number of LACP packets sent and received by a port.
Marker Sent and Recv	The number of LACP marker packets sent and received by a port.
Marker Response Sent and Recv	The number of LACP marker response packets sent and received by a port.
LACPDUs Pkts and Err	The number of unknown and illegal packets received by LACP for a port.

This is an example of output from the **show lacp internal** command:

```
Switch> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                              LACP port     Admin     Oper    Port     Port
Port        Flags   State     Priority      Key       Key     Number   State
Gi0/1       SA      bndl      32768         0x3       0x3     0x4      0x3D
Gi0/2       SA      bndl      32768         0x3       0x3     0x5      0x3D
```

Table 2-11 describes the fields in the display:

Table 2-11 show lacp internal Field Descriptions

Field	Description
State	State of the specific port. These are the allowed values: • – —Port is in an unknown state. • **bndl**—Port is attached to an aggregator and bundled with other ports. • **susp**—Port is in a suspended state; it is not attached to any aggregator. • **hot-sby**—Port is in a hot-standby state. • **indiv**—Port is incapable of bundling with any other port. • **indep**—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port). • **down**—Port is down.
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports s in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
Admin Key	Administrative key assigned to this port. LACP automatically generates an administrative key value as a hexadecimal number. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by the port physical characteristics (for example, data rate and duplex capability) and configuration restrictions that you establish.
Oper Key	Runtime operational key that is being used by this port. LACP automatically generates this value as a hexadecimal number.
Port Number	Port number.
Port State	State variables for the port, encoded as individual bits within a single octet with these meanings: • bit0: LACP_Activity • bit1: LACP_Timeout • bit2: Aggregation • bit3: Synchronization • bit4: Collecting • bit5: Distributing • bit6: Defaulted • bit7: Expired **Note** In the list above, bit7 is the MSB and bit0 is the LSB.

This is an example of output from the **show lacp neighbor** command:

```
Switch> show lacp neighbor
Flags:  S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 3 neighbors

Partner's information:

          Partner               Partner                   Partner
Port      System ID             Port Number     Age       Flags
Gi0/1    32768,0007.eb49.5e80  0xC             19s       SP

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          32768                 0x3             0x3C

Partner's information:

          Partner               Partner                   Partner
Port      System ID             Port Number     Age       Flags
Gi0/2    32768,0007.eb49.5e80  0xD             15s       SP

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          32768                 0x3             0x3C
```

This is an example of output from the **show lacp sys-id** command:

```
Switch> show lacp sys-id
32765,0002.4b29.3a00
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

Related Commands

Command	Description
clear lacp	Clears the LACP channel-group information.
lacp port-priority	Configures the LACP port priority.
lacp system-priority	Configures the LACP system priority.

show link state group

Use the **show link state group** privileged EXEC command to display the link-state group information.

show link state group [*number*] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

number	(Optional) Number of the link-state group.
detail	(Optional) Specify that detailed information appears.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **show link state group** command to display the link-state group information. Enter this command without keywords to display information about all link-state groups. Enter the group number to display information specific to the group.

Enter the **detail** keyword to display detailed information about the group. The output for the **show link state group detail** command displays only those link-state groups that have link-state tracking enabled or that have upstream or downstream interfaces (or both) configured. If there is no link-state configuration for a group, the group is not shown as enabled or disabled.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show link state group 1** command:

```
Switch> show link state group 1
Link State Group: 1      Status: Enabled, Down
```

This is an example of output from the **show link state group detail** command:

```
Switch> show link state group detail
(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi0/15(Dwn) Gi0/16(Dwn)
Downstream Interfaces : Gi0/11(Dis) Gi0/12(Dis) Gi0/13(Dis) Gi0/14(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi0/15(Dwn) Gi0/16(Dwn) Gi0/17(Dwn)
Downstream Interfaces : Gi0/11(Dis) Gi0/12(Dis) Gi0/13(Dis) Gi0/14(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

Related Commands

Command	Description
link state group	Configures an interface as a member of a link-state group.
link state track	Enables a link-state group.
show running-config	Displays the operating configuration.

show location

Use the **show location** user EXEC command to display location information for an endpoint.

show location admin-tag | [| {**begin** | **exclude** | **include**} *expression*]

show location civic-location {**identifier** *id number* | **interface** *interface-id* | **static** } | {**begin** | **exclude** | **include**} *expression*]

show location elin-location {**identifier** *id number* | **interface** *interface-id* | **static**} | {**begin** | **exclude** | **include**} *expression*]

Syntax Description

admin-tag	Display administrative tag or site information.
civic-location	Display civic location information.
elin-location	Display emergency location information (ELIN).
identifier *id*	Specify the ID for the civic location or the elin location. The id range is 1 to 4095.
interface *interface-id*	Display location information for the specified interface or all interfaces. Valid interfaces include physical ports.
static	Display static configuration information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **show location** command to display location information for an endpoint.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show location civic-location** command that displays location information for an interface:

```
Switch> show location civic interface gigabitethernet0/1
Civic location information
--------------------------
Identifier              : 1
County                  : Santa Clara
Street number           : 3550
Building                : 19
Room                    : C6
Primary road name       : Cisco Way
City                    : San Jose
State                   : CA
Country                 : US
```

This is an example of output from the **show location civic-location** command that displays all the civic location information:

```
Switch> show location civic-location static
Civic location information
--------------------------
Identifier              : 1
County                  : Santa Clara
Street number           : 3550
Building                : 19
Room                    : C6
Primary road name       : Cisco Way
City                    : San Jose
State                   : CA
Country                 : US
Ports                   : Gi0/1
--------------------------
Identifier              : 2
Street number           : 24568
Street number suffix    : West
Landmark                : Golden Gate Bridge
Primary road name       : 19th Ave
City                    : San Francisco
Country                 : US
--------------------------
```

This is an example of output from the **show location elin-location** command that displays the emergency location information:

```
Switch> show location elin-location identifier 1
Elin location information
--------------------------
Identifier : 1
Elin       : 14085553881
Ports      : Gi0/2
```

This is an example of output from the **show location elin static** command that displays all emergency location information:

```
Switch> show location elin static
Elin location information
--------------------------
Identifier : 1
Elin       : 14085553881
Ports      : Gi0/2
--------------------------
Identifier : 2
Elin       : 18002228999
--------------------------
```

Related Commands

Command	Description
location (global configuration)	Configures the global location information for an endpoint.
location (interface configuration)	Configures the location information for an interface.

show mac address-table

Use the **show mac address-table** user EXEC command to display a specific MAC address table static and dynamic entry or the MAC address table static and dynamic entries on a specific interface or VLAN.

show mac address-table [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table** command:

```
Switch> show mac address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type       Ports
----    -----------       ----       -----
 All    0000.0000.0001    STATIC     CPU
 All    0000.0000.0002    STATIC     CPU
 All    0000.0000.0003    STATIC     CPU
 All    0000.0000.0009    STATIC     CPU
 All    0000.0000.0012    STATIC     CPU
 All    0180.c200.000b    STATIC     CPU
 All    0180.c200.000c    STATIC     CPU
 All    0180.c200.000d    STATIC     CPU
 All    0180.c200.000e    STATIC     CPU
 All    0180.c200.000f    STATIC     CPU
 All    0180.c200.0010    STATIC     CPU
   1    0030.9441.6327    DYNAMIC    Gi0/4
Total Mac Addresses for this criterion: 12
```

Related Commands

Command	Description
clear mac address-table dynamic	Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table address

Use the **show mac address-table address** user EXEC command to display MAC address table information for the specified MAC address.

show mac address-table address *mac-address* [**interface** *interface-id*] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

mac-address	Specify the 48-bit MAC address; the valid format is H.H.H.
interface *interface-id*	(Optional) Display information for a specific interface. Valid interfaces include physical ports and port channels.
vlan *vlan-id*	(Optional) Display entries for the specific VLAN only. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table address** command:

```
Switch# show mac address-table address 0002.4b28.c482
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
 All    0002.4b28.c482  STATIC  CPU
Total Mac Addresses for this criterion: 1
```

Related Commands

Command	Description
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table aging-time

Use the **show mac address-table aging-time** user EXEC command to display the aging time of a specific address table instance, all address table instances on a specified VLAN or, if a specific VLAN is not specified, on all VLANs.

show mac address-table aging-time [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan *vlan-id*	(Optional) Display aging time information for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If no VLAN number is specified, the aging time for all VLANs appears.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table aging-time** command:

```
Switch> show mac address-table aging-time
Vlan    Aging Time
----    ----------
   1     300
```

This is an example of output from the **show mac address-table aging-time vlan 10** command:

```
Switch> show mac address-table aging-time vlan 10
Vlan    Aging Time
----    ----------
  10     300
```

Related Commands

Command	Description
mac address-table aging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table count

Use the **show mac address-table count** user EXEC command to display the number of addresses present in all VLANs or the specified VLAN.

show mac address-table count [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan *vlan-id*	(Optional) Display the number of addresses for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If no VLAN number is specified, the address count for all VLANs appears.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table count** command:

```
Switch# show mac address-table count
Mac Entries for Vlan   : 1
---------------------------
Dynamic Address Count  : 2
Static  Address Count  : 0
Total Mac Addresses    : 2
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table dynamic

Use the **show mac address-table dynamic** user EXEC command to display only dynamic MAC address table entries.

show mac address-table dynamic [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

address *mac-address*	(Optional) Specify a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
interface *interface-id*	(Optional) Specify an interface to match; valid *interfaces* include physical ports and port channels.
vlan *vlan-id*	(Optional) Display entries for a specific VLAN; the range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table dynamic** command:

```
Switch> show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0030.b635.7862  DYNAMIC Gi0/2
   1    00b0.6496.2741  DYNAMIC Gi0/2
Total Mac Addresses for this criterion: 2
```

Related Commands

Command	Description
clear mac address-table dynamic	Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table interface

Use the **show mac address-table interface** user command to display the MAC address table information for the specified interface in the specified VLAN.

show mac address-table interface *interface-id* [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	Specify an interface type; valid interfaces include physical ports and port channels.
vlan *vlan-id*	(Optional) Display entries for a specific VLAN; the range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table interface** command:

```
Switch> show mac address-table interface gigabitethernet0/2
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0030.b635.7862  DYNAMIC Gi0/2
   1    00b0.6496.2741  DYNAMIC Gi0/2
Total Mac Addresses for this criterion: 2
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table static

Use the **show mac address-table static** user EXEC command to display only static MAC address table entries.

show mac address-table static [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

address *mac-address*	(Optional) Specify a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
interface *interface-id*	(Optional) Specify an interface to match; valid *interfaces* include physical ports and port channels.
vlan *vlan-id*	(Optional) Display addresses for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table static** command:

```
Switch> show mac address-table static
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
 All    0100.0ccc.cccc  STATIC  CPU
 All    0180.c200.0000  STATIC  CPU
 All    0100.0ccc.cccd  STATIC  CPU
 All    0180.c200.0001  STATIC  CPU
 All    0180.c200.0004  STATIC  CPU
 All    0180.c200.0005  STATIC  CPU
   4    0001.0002.0004  STATIC  Drop
   6    0001.0002.0007  STATIC  Drop
Total Mac Addresses for this criterion: 8
```

Related Commands

Command	Description
mac address-table static	Adds static addresses to the MAC address table.
mac address-table static drop	Enables unicast MAC address filtering and configures the switch to drop traffic with a specific source or destination MAC address.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table vlan

Use the **show mac address-table vlan** user EXEC command to display the MAC address table information for the specified VLAN.

show mac address-table vlan *vlan-id* [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan-id	(Optional) Display addresses for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table vlan 1** command:

```
Switch> show mac address-table vlan 1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0100.0ccc.cccc  STATIC  CPU
   1    0180.c200.0000  STATIC  CPU
   1    0100.0ccc.cccd  STATIC  CPU
   1    0180.c200.0001  STATIC  CPU
   1    0180.c200.0002  STATIC  CPU
   1    0180.c200.0003  STATIC  CPU
   1    0180.c200.0005  STATIC  CPU
   1    0180.c200.0006  STATIC  CPU
   1    0180.c200.0007  STATIC  CPU
Total Mac Addresses for this criterion: 9
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table static	Displays static MAC address table entries only.

show mls qos

Use the **show mls qos** user EXEC command to display global quality of service (QoS) configuration information.

show mls qos [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mls qos** command when QoS is enabled and Differentiated Services Code Point (DSCP) transparency is disabled:

```
Switch> show mls qos
QoS is enabled
QoS ip packet dscp rewrite is disabled
```

This is an example of output from the **show mls qos** command when QoS is enabled and DSCP transparency is enabled:

```
Switch> show mls qos
QoS is enabled
QoS ip packet dscp rewrite is enabled
```

Related Commands

Command	Description
mls qos	Enables QoS for the entire switch.

show mls qos interface

Use the **show mls qos interface** user EXEC command to display quality of service (QoS) information at the port level.

show mls qos interface [*interface-id*] [**buffers** | **queueing** | **statistics**]
[| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Display QoS information for the specified port. Valid interfaces include physical ports.
buffers	(Optional) Display the buffer allocation among the queues.
queueing	(Optional) Display the queueing strategy (shared or shaped) and the weights corresponding to the queues.
statistics	(Optional) Display statistics for sent and received Differentiated Services Code Points (DSCPs) and class of service (CoS) values, the number of packets enqueued or dropped per egress queue, and the number of in-profile and out-of-profile packets for each policer.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help string, the **policers** keyword is not supported.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mls qos interface** *interface-id* command when VLAN-based QoS is enabled:

```
Switch> show mls qos interface gigabitethernet0/1
GigabitEthernet0/1
trust state:not trusted
trust mode:not trusted
trust enabled flag:ena
COS override:dis
default COS:0
```

```
DSCP Mutation Map:Default DSCP Mutation Map
Trust device:none
qos mode:vlan-based
```

This is an example of output from the **show mls qos interface** *interface-id* command when VLAN-based QoS is disabled:

```
Switch> show mls qos interface gigabitethernet0/2
GigabitEthernet0/2
trust state:not trusted
trust mode:not trusted
trust enabled flag:ena
COS override:dis
default COS:0
DSCP Mutation Map:Default DSCP Mutation Map
Trust device:none
qos mode:port-based
```

This is an example of output from the **show mls qos interface** *interface-id* **buffers** command:

```
Switch> show mls qos interface gigabitethernet0/2 buffers
GigabitEthernet0/2
The port is mapped to qset : 1
The allocations between the queues are : 25 25 25 25
```

This is an example of output from the **show mls qos interface** *interface-id* **queueing** command. The egress expedite queue overrides the configured shaped round robin (SRR) weights.

```
Switch> show mls qos interface gigabitethernet0/2 queueing
GigabitEthernet0/2
Egress Priority Queue :enabled
Shaped queue weights (absolute) :  25 0 0 0
Shared queue weights  :  25 25 25 25
The port bandwidth limit : 100  (Operational Bandwidth:100.0)
The port is mapped to qset : 1
```

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to a queue-set.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
mls qos trust	Configures the port trust state.
radius-server dead-criteria	Maps a port to a queue-set.

show mls qos maps

Use the **show mls qos maps** user EXEC command to display quality of service (QoS) mapping information. During classification, QoS uses the mapping tables to represent the priority of the traffic and to derive a corresponding class of service (CoS) or Differentiated Services Code Point (DSCP) value from the received CoS, DSCP, or IP precedence value.

show mls qos maps [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-mutation** *dscp-mutation-name* | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

cos-dscp	(Optional) Display class of service (CoS)-to-DSCP map.
cos-input-q	(Optional) Display the CoS input queue threshold map.
cos-output-q	(Optional) Display the CoS output queue threshold map.
dscp-cos	(Optional) Display DSCP-to-CoS map.
dscp-input-q	(Optional) Display the DSCP input queue threshold map.
dscp-mutation *dscp-mutation-name*	(Optional) Display the specified DSCP-to-DSCP-mutation map.
dscp-output-q	(Optional) Display the DSCP output queue threshold map.
ip-prec-dscp	(Optional) Display the IP-precedence-to-DSCP map.
policed-dscp	(Optional) Display the policed-DSCP map.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

The policed-DSCP, DSCP-to-CoS, and the DSCP-to-DSCP-mutation maps appear as a matrix. The d1 column specifies the most-significant digit in the DSCP. The d2 row specifies the least-significant digit in the DSCP. The intersection of the d1 and d2 values provides the policed-DSCP, the CoS, or the mutated-DSCP value. For example, in the DSCP-to-CoS map, a DSCP value of 43 corresponds to a CoS value of 5.

The DSCP input queue threshold and the DSCP output queue threshold maps appear as a matrix. The d1 column specifies the most-significant digit of the DSCP number. The d2 row specifies the least-significant digit in the DSCP number. The intersection of the d1 and the d2 values provides the queue ID and threshold ID. For example, in the DSCP input queue threshold map, a DSCP value of 43 corresponds to queue 2 and threshold 1 (02-01).

The CoS input queue threshold and the CoS output queue threshold maps show the CoS value in the top row and the corresponding queue ID and threshold ID in the second row. For example, in the CoS input queue threshold map, a CoS value of 5 corresponds to queue 2 and threshold 1 (2-1).

Examples

This is an example of output from the **show mls qos maps** command:

```
Switch> show mls qos maps
Policed-dscp map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63

Dscp-cos map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07

Cos-dscp map:
     cos:   0  1  2  3  4  5  6  7
  --------------------------------
    dscp:   0  8 16 24 32 40 48 56

IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   0  8 16 24 32 40 48 56

Dscp-outputq-threshold map:
  d1 :d2    0     1     2     3     4     5     6     7     8     9
  ------------------------------------------------------------------------
   0 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
   1 :    02-01 02-01 02-01 02-01 02-01 02-01 03-01 03-01 03-01 03-01
   2 :    03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01
   3 :    03-01 03-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
   4 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 04-01 04-01
   5 :    04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
   6 :    04-01 04-01 04-01 04-01
```

```
Dscp-inputq-threshold map:
    d1 :d2    0     1     2     3     4     5     6     7     8     9
    ------------------------------------------------------------------
     0 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     1 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     2 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     3 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     4 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 01-01 01-01
     5 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     6 :    01-01 01-01 01-01 01-01

Cos-outputq-threshold map:
              cos:  0   1   2   3   4   5   6   7
              ------------------------------------
  queue-threshold: 2-1 2-1 3-1 3-1 4-1 1-1 4-1 4-1

   Cos-inputq-threshold map:
              cos:  0   1   2   3   4   5   6   7
              ------------------------------------
  queue-threshold: 1-1 1-1 1-1 1-1 1-1 2-1 1-1 1-1

Dscp-dscp mutation map:
   Default DSCP Mutation Map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
```

Related Commands

Command	Description
mls qos queue-set output buffers	Defines the CoS-to-DSCP map, DSCP-to-CoS map, DSCP-to-DSCP-mutation map, IP-precedence-to-DSCP map, and the policed-DSCP map.
mls qos trust	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.

show mls qos queue-set

Use the **show mls qos queue-set** user EXEC command to display quality of service (QoS) settings for the egress queues.

show mls qos queue-set [*qset-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

qset-id	(Optional) ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.nway

Examples

This is an example of output from the **show mls qos queue-set** command:

```
Switch> show mls qos queue-set
Queueset: 1
Queue   :        1       2       3       4
----------------------------------------------
buffers   :      25      25      25      25
threshold1:      100     200     100     100
threshold2:      100     200     100     100
reserved  :      50      50      50      50
maximum   :      400     400     400     400
Queueset: 2
Queue   :        1       2       3       4
----------------------------------------------
buffers   :      25      25      25      25
threshold1:      100     200     100     100
threshold2:      100     200     100     100
reserved  :      50      50      50      50
maximum   :      400     400     400     400
```

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to the queue-set.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation of the queue-set.

show monitor

Use the **show monitor** user EXEC command to display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions on the switch. Use the command with keywords to show a specific session, all sessions, all local sessions, or all remote sessions.

show monitor [**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

session	(Optional) Display information about specified SPAN sessions.
session_number	Specify the number of the SPAN or RSPAN session. The range is 1 to 66.
all	Display all SPAN sessions.
local	Display only local SPAN sessions.
range *list*	Display a range of SPAN sessions, where *list* is the range of valid sessions, either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges. **Note** This keyword is available only in privileged EXEC mode.
remote	Display only remote SPAN sessions.
detail	(Optional) Display detailed information about the specified sessions.
| begin	Display begins with the line that matches the *expression*.
| exclude	Display excludes lines that match the *expression*.
| include	Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

The output is the same for the **show monitor** command and the **show monitor session all** command.

Examples

This is an example of output for the **show monitor** user EXEC command on a switch:

```
Switch# show monitor
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi0/1
Both : Gi0/2-3,Gi0/5-6
Destination Ports : Gi0/20
Encapsulation : Replicate
Ingress : Disabled

Session 2
---------
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

This is an example of output for the **show monitor** user EXEC command for local SPAN source session 1:

```
Switch# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi0/1
Both : Gi0/2-3,Gi0/5-6
Destination Ports : Gi0/20
Encapsulation : Replicate
Ingress : Disabled
```

This is an example of output for the **show monitor session all** user EXEC command when ingress traffic forwarding is enabled:

```
Switch# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi0/2
Destination Ports : Gi0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q

Session 2
---------
Type : Local Session
Source Ports :
Both : Gi0/8
Destination Ports : Gi0/12
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

Related Commands

Command	Description
monitor session	Starts or modifies a SPAN or RSPAN session.

show pagp

Use the **show pagp** user EXEC command to display Port Aggregation Protocol (PAgP) channel-group information.

show pagp [*channel-group-number*] {**counters** | **dual-active** | **internal** | **neighbor**} [| {**begin** | **exclude** | **include**} *expression*]]

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 48.
counters	Display traffic information.
dual-active	Display the dual-active status.
internal	Display internal information.
neighbor	Display neighbor information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can enter any **show pagp** command to display the active channel-group information. To display the nonactive information, enter the **show pagp** command with a channel-group number.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* are appear.

Examples

This is an example of output from the **show pagp 1 counters** command:

```
Switch> show pagp 1 counters
             Information        Flush
Port         Sent   Recv     Sent   Recv
---------------------------------------
Channel group: 1
  Gi0/1    45     42       0      0
  Gi0/2    45     41       0      0
```

This is an example of output from the **show pagp dual-active** command:

```
Switch> show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1
```

```
Channel group 1
          Dual-Active     Partner              Partner   Partner
Port      Detect Capable  Name                 Port      Version
Gi0/1   No              Switch               Gi0/3   N/A
Gi0/2   No              Switch               Gi0/4   N/A

<output truncated>
```

This is an example of output from the **show pagp 1 internal** command:

```
Switch> show pagp 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Channel group 1
                                Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi0/1     SC    U6/S7   H       30s      1        128        Any      16
Gi0/2     SC    U6/S7   H       30s      1        128        Any      16
```

This is an example of output from the **show pagp 1 neighbor** command:

```
Switch> show pagp 1 neighbor
   Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
           A - Device is in Auto mode.        P - Device learns on physical port.

   Channel group 1 neighbors
               Partner              Partner          Partner           Partner Group
   Port        Name                 Device ID        Port         Age  Flags   Cap.
   Gi0/1     switch-p2            0002.4b29.4600   Gi0/1        9s SC      10001
   Gi0/2     switch-p2            0002.4b29.4600   Gi0/2       24s SC      10001
```

Related Commands

Command	Description
clear pagp	Clears PAgP channel-group information.

show setup express

Use the **show setup express** privileged EXEC command to display if Express Setup mode is active on the switch.

show setup express [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Examples

This is an example of output from the **show setup express co**mmand:

```
Switch# show setup express
express setup mode is active
```

Related Commands

Command	Description
setup express	Enables Express Setup mode.

show spanning-tree

Use the **show spanning-tree** user EXEC command to display spanning-tree state information.

show spanning-tree [*bridge-group* | **active** [**detail**] | **backbonefast** | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **mst** | **pathcost method** | **root** | **summary** [**totals**] | **uplinkfast** | **vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree *bridge-group* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree vlan *vlan-id* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree {**vlan** *vlan-id* | *bridge-group*} **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree {**vlan** *vlan-id* | *bridge-group*} **root** [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree interface *interface-id* [**active** [**detail**] | **cost** | **detail** [**active**] | **inconsistency** | **portfast** | **priority** | **rootcost** | **state**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree mst [**configuration** [digest]] | [*instance-id* [**detail** | **interface** *interface-id* [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

bridge-group	(Optional) Specify the bridge group number. The range is 1 to 255.
active [**detail**]	(Optional) Display spanning-tree information only on active interfaces (available only in privileged EXEC mode).
backbonefast	(Optional) Display spanning-tree BackboneFast status.
blockedports	(Optional) Display blocked port information (available only in privileged EXEC mode).
bridge [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]	(Optional) Display status and configuration of this switch (optional keywords available only in privileged EXEC mode).
detail [**active**]	(Optional) Display a detailed summary of interface information (**active** keyword available only in privileged EXEC mode).
inconsistentports	(Optional) Display inconsistent port information (available only in privileged EXEC mode).
interface *interface-id* [**active** [**detail**] | **cost** | **detail** [**active**] | **inconsistency** | **portfast** | **priority** | **rootcost** | **state**]	(Optional) Display spanning-tree information for the specified interface (all options except **portfast** and **state** available only in privileged EXEC mode). Enter each interface separated by a space. Ranges are not supported. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48.

mst [**configuration** [**digest**]] [*instance-id* [**detail** | **interface** *interface-id* [**detail**]]	(Optional) Display the multiple spanning-tree (MST) region configuration and status (available only in privileged EXEC mode). The keywords have these meanings: • **digest**—(Optional) Display the MD5 digest included in the current MST configuration identifier (MSTCI). Two separate digests, one for standard and one for prestandard switches, appear (available only in privileged EXEC mode). The terminology was updated for the implementation of the IEEE standard, and the *txholdcoun*t field was added. The new master role appears for boundary ports. The word *pre-standard* or *Pre-STD* appears when an IEEE standard bridge sends prestandard BPDUs on a port. The word *pre-standard (config)* or *Pre-STD-Cf* appears when a port has been configured to transmit prestandard BPDUs and no prestandard BPDU has been received on that port. The word *pre-standard (rcvd)* or *Pre-STD-Rx* appears when a prestandard BPDU has been received on a port that has not been configured to transmit prestandard BPDUs. A *dispute* flag appears when a designated port receives inferior designated information until the port returns to the forwarding state or ceases to be designated. • *instance-id*—You can specify a single instance ID, a range of IDs separated by a hyphen, or a series of IDs separated by a comma. The range is 1 to 4094. The display shows the number of currently configured instances. • **interface** *interface-id*—(Optional) Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48. • **detail**—(Optional) Display detailed information for the instance or interface.
pathcost method	(Optional) Display the default path cost method (available only in privileged EXEC mode).
root [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**]]	(Optional) Display root switch status and configuration (all keywords available only in privileged EXEC mode).
summary [**totals**]	(Optional) Display a summary of port states or the total lines of the spanning-tree state section. The words *IEEE Standard* identify the MST version running on a switch.
uplinkfast	(Optional) Display spanning-tree UplinkFast status.
vlan *vlan-id* [**active** [**detail**] | **backbonefast** | **blockedports** | **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]	(Optional) Display spanning-tree information for the specified VLAN (some keywords available only in privileged EXEC mode). You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

user EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If the *vlan-id* variable is omitted, the command applies to the spanning-tree instance for all VLANs.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show spanning-tree active** command:

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0001.42e2.cdd0
             Cost        3038
             Port        24 (GigabitEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    49153  (priority 49152 sys-id-ext 1)
             Address     0003.fd63.9580
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
  Uplinkfast enabled

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1          Root FWD 3019      128.24   P2p
<output truncated>
```

This is an example of output from the **show spanning-tree detail** command:

```
Switch# show spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 49152, sysid 1, address 0003.fd63.9580
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0001.42e2.cdd0
  Root port is 24 (GigabitEthernet0/1), cost of root path is 3038
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 1d16h ago
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
  Uplinkfast enabled
```

```
 Port 1 (GigabitEthernet0/1) of VLAN0001 is forwarding
   Port path cost 3019, Port priority 128, Port Identifier 128.24.
   Designated root has priority 32768, address 0001.42e2.cdd0
   Designated bridge has priority 32768, address 00d0.bbf5.c680
   Designated port id is 128.25, designated path cost 19
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 0, received 72364
<output truncated>
```

This is an example of output from the **show spanning-tree interface** *interface-id* command:

```
Switch# show spanning-tree interface gigabitethernet0/1
Vlan             Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Root FWD 3019      128.24   P2p

Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID   is enabled
Portfast             is disabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard            is disabled by default
UplinkFast           is enabled
BackboneFast         is enabled
Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                  1        0         0        11         12
VLAN0002                  3        0         0        1          4
VLAN0004                  3        0         0        1          4
VLAN0006                  3        0         0        1          4
VLAN0031                  3        0         0        1          4
VLAN0032                  3        0         0        1          4
<output truncated>
---------------------- -------- --------- -------- ---------- ----------
37 vlans                  109      0         0        47         156
Station update rate set to 150 packets/sec.

UplinkFast statistics
-----------------------
Number of transitions via uplinkFast (all VLANs)            : 0
Number of proxy multicast addresses transmitted (all VLANs) : 0

BackboneFast statistics
-----------------------
Number of transition via backboneFast (all VLANs)           : 0
Number of inferior BPDUs received (all VLANs)               : 0
Number of RLQ request PDUs received (all VLANs)             : 0
Number of RLQ response PDUs received (all VLANs)            : 0
Number of RLQ request PDUs sent (all VLANs)                 : 0
Number of RLQ response PDUs sent (all VLANs)                : 0
```

This is an example of output from the **show spanning-tree mst configuration** command:

```
Switch# show spanning-tree mst configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ------------------
0         1-9,21-4094
1         10-20
----------------------------
```

This is an example of output from the **show spanning-tree mst interface** *interface-id* command:

```
Switch# show spanning-tree mst interface gigabitethernet0/1
GigabitEthernet0/1 of MST00 is root forwarding
Edge port: no             (default)        port guard : none        (default)
Link type: point-to-point (auto)           bpdu filter: disable     (default)
Boundary : boundary       (STP)            bpdu guard : disable     (default)
Bpdus sent 5, received 74

Instance role state cost      prio vlans mapped
0        root FWD   200000    128  1,12,14-4094
```

This is an example of output from the **show spanning-tree mst 0** command:

```
Switch# show spanning-tree mst 0
###### MST00        vlans mapped: 1-9,21-4094
Bridge      address 0002.4b29.7a00  priority  32768 (32768 sysid 0)
Root        address 0001.4297.e000  priority  32768 (32768 sysid 0)
            port    Gi0/1          path cost 200038
IST master *this switch
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured  hello time 2, forward delay 15, max age 20, max hops 20

Interface              role state cost      prio type
--------------------   ---- ----- --------- ---- --------------------------------
GigabitEthernet0/1    root FWD   200000    128  P2P bound(STP)
GigabitEthernet0/2    desg FWD   200000    128  P2P bound(STP)
Port-channel1          desg FWD   200000    128  P2P bound(STP)
```

Related Commands

Command	Description
clear spanning-tree counters	Clears the spanning-tree counters.
clear spanning-tree detected-protocols	Restarts the protocol migration process.
spanning-tree backbonefast	Enables the BackboneFast feature.
spanning-tree bpdufilter	Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts an interface in the error-disabled state when it receives a BPDU.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree extend system-id	Enables the extended system ID feature.
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree link-type	Overrides the default link-type setting for rapid spanning-tree transitions to the forwarding state.

Command	Description
spanning-tree loopguard default	Prevents alternate or root ports from becoming the designated port because of a failure that leads to a unidirectional link.
spanning-tree mst configuration	Enters multiple spanning-tree (MST) configuration mode through which the MST region configuration occurs.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in an MST region before the BPDU is discarded and the information held for an interface is aged.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree port-priority	Configures an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.
spanning-tree uplinkfast	Accelerates the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself.
spanning-tree vlan	Configures spanning tree on a per-VLAN basis.

show system mtu

Use the **show system mtu** privileged EXEC command to display the global maximum transmission unit (MTU) or maximum packet size set for the switch.

show system mtu [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If you have used the **system mtu** or **system mtu jumbo** global configuration command to change the MTU setting, the new setting does not take effect until you reset the switch.

For information about the MTU values and the configurations that affect the MTU values, see the **system mtu** command.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show system mtu** command:

```
Switch# show system mtu
System MTU size is 1500 bytes
System Jumbo MTU size is 1550 bytes
Routing MTU size is 1500 bytes.
```

Related Commands

Command	Description
system mtu	Sets the MTU size for the Gigabit Ethernet or 10-Gigabit Ethernet ports.

show udld

Use the **show udld** user EXEC command to display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port.

show udld [*interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the interface and port number. Valid interfaces include physical ports and VLANs. The VLAN range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If you do not enter an *interface-id*, administrative and operational UDLD status for all interfaces appear.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show udld** *interface-id* command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. Table 2-12 describes the fields in this display.

```
Switch> show udld gigabitethernet0/1
Interface gi0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
    Entry 1
    Expiration time: 146
    Device ID: 1
    Current neighbor state: Bidirectional
    Device name: Switch-A
    Port ID: Gi0/1
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Gi0/2
    Message interval: 5
    CDP Device name: Switch-A
```

Table 2-12 show udld Field Descriptions

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state appears if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state appears if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring.
Current operational state	The current phase of the UDLD state machine. For a normal bidirectional link, the state machine is most often in the Advertisement phase.
Message interval	How often advertisement messages are sent from the local device. Measured in seconds.
Time out interval	The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window.
Entry 1	Information from the first cache entry, which contains a copy of echo information received from the neighbor.
Expiration time	The amount of time in seconds remaining before this cache entry is aged out.
Device ID	The neighbor device identification.
Current neighbor state	The neighbor's current state. If both the local and neighbor devices are running UDLD normally, the neighbor state and local state should be bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries appear.
Device name	The device name or the system serial number of the neighbor. The system serial number appears if the device name is not set or is set to the default (Switch).
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The device name of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP device name	The CDP device name or the system serial number. The system serial number appears if the device name is not set or is set to the default (Switch).

Related Commands

Command	Description
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.
udld reset	Resets all interfaces shutdown by UDLD and permits traffic to begin passing through them again.

show version

Use the **show version** user EXEC command to display version information for the hardware and firmware and software license information.

show version [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show version** command that shows the software licenses installed on the switch:

Note Though visible in the **show version** output, the *configuration register* information is not supported on the switch.

```
Switch> show version
Cisco IOS Software, C2360 Software (c2360-universalk9-mz), Version 12.2(53)EY, RELE
ASE SOFTWARE (fc1)
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Fri 23-Jan-09 15:45 by myl
Image text-base: 0x00003000, data-base: 0x01800000

ROM: Bootstrap program is C2350 boot loader
BOOTLDR: C3560E Boot Loader (C3560E-HBOOT-M), Version 12.2 [lqian-v122_44_se_thr
ottle 106]

switch uptime is 1 week, 4 days, 23 hours, 5 minutes
System returned to ROM by power-on
System restarted at 16:41:14 PST Fri Jan 23 2009
System image file is "flash:/c2360-universalk9-mz.122-53.EY/c2360-universalk9-mz.122
-53.EY.bin"
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.


cisco WS-C2360-48TD (PowerPC405) processor with 126976K/4088K bytes of memory.
Processor board ID FDO1245R0LE
Last reset from power-on
2 Virtual Ethernet interfaces
1 FastEthernet interface
52 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:23:AC:D1:4C:00
Motherboard assembly number     : 73-12369-01
Motherboard serial number       : FDO124506LX
Motherboard revision number     : 02
Model number                    : WS-C2360-48TD-S
Daughterboard assembly number   : 800-29737-01
Daughterboard serial number     : FDO1245017W
System serial number            : FDO1245R0LE
Top Assembly Part Number        : 800-32281-01
Top Assembly Revision Number    : 01
Hardware Board Revision Number  : 0x00


Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 54    WS-C2360-48TD      12.2(53)EY            c2360-UNIVERSALK9-MZ


Configuration register is 0xF
```

show vlan

Use the **show vlan** user EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch.

show vlan [**access-map** *name* | **brief** | **id** *vlan-id* | **internal usage** | **mtu** | **name** *vlan-name* | **remote-span** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

access-map *name*	(Optional) Display information about a particular VLAN access-map or all VLAN access-maps.
brief	(Optional) Display one line for each VLAN with the VLAN name, status, and its ports.
id *vlan-id*	(Optional) Display information about a single VLAN identified by VLAN ID number. For *vlan-id*, the range is 1 to 4094.
internal usage	(Optional) Display a list of VLANs being used internally by the switch. These VLANs are always from the extended range (VLAN IDs 1006 to 4094), and you cannot create VLANs with these IDS by using the **vlan** global configuration command until you remove them from internal use.
mtu	(Optional) Display a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.
name *vlan-name*	(Optional) Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
remote-span	(Optional) Display information about Remote SPAN (RSPAN) VLANs.
summary	(Optional) Display VLAN summary information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help string, the **ifindex** keyword is not supported.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

In the **show vlan mtu** command output, the MTU_Mismatch column shows whether all the ports in the VLAN have the same MTU. When *yes* appears in this column, it means that the VLAN has ports with different MTUs, and packets that are switched from a port with a larger MTU to a port with a smaller MTU might be dropped. If the VLAN does not have an SVI, the hyphen (-) symbol appears in the SVI_MTU column. If the MTU-Mismatch column displays *yes*, the names of the port with the MinMTU and the port with the MaxMTU appear.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show vlan** command. Table 2-13 describes the fields in the display.

```
Switch> show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                                Gi0/5, Gi0/6, Gi0/7, Gi0/8
                                                Gi0/9, Gi0/10, Gi0/11, Gi0/12
                                                Gi0/13, Gi0/14, Gi0/15, Gi0/16
                                                Gi0/17, Gi0/18, Gi0/19, Gi0/20
                                                Gi0/21, Gi0/22, Gi0/23, Gi0/24
                                                Gi0/25, Gi0/26, Gi0/27, Gi0/28
                                                Gi0/29, Gi0/30, Gi0/31, Gi0/32
                                                Gi0/33, Gi0/34, Gi0/35, Gi0/36
                                                Gi0/37, Gi0/38, Gi0/39, Gi0/40
                                                Gi0/41, Gi0/42, Gi0/43, Gi0/44
                                                Gi0/45, Gi0/46, Gi0/47, Te0/1
                                                Te0/2
<output truncated>

2    VLAN0002                         active
3    VLAN0003                         active

<output truncated>

1000 VLAN1000                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0

<output truncated>

1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

```
Primary Secondary Type Ports
------- --------- ----------------- ------------------------------------------
20      25     isolated  Gi0/1,Gi0/3
20      30     community Gi0/1, Gi0/3
20      35     community Gi0/1, Gi0/3

<output truncated>
```

Table 2-13 show vlan Command Output Fields

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.
Trans1	Translation bridge 1.
Trans2	Translation bridge 2.
Remote SPAN VLANs	Identifies any RSPAN VLANs that have been configured.

This is an example of output from the **show vlan dot1q tag native** command:

```
Switch> show vlan dot1q tag native
dot1q native vlan tagging is disabled
```

This is an example of output from the **show vlan summary** command:

```
Switch> show vlan summary
Number of existing VLANs           : 45
 Number of existing VTP VLANs      : 45
 Number of existing extended VLANs : 0
```

This is an example of output from the **show vlan id** command.

```
Switch# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    VLAN0200                         active    Gi0/7, Gi0/8
2    VLAN0200                         active    Gi0/1, Gi0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled
```

Related Commands

Command	Description
switchport mode	Configures the VLAN membership mode of a port.
vlan (global configuration)	Enables VLAN configuration mode where you can configure VLANs 1 to 4094.

show vtp

Use the **show vtp** user EXEC command to display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters.

show vtp {**counters** | **password** | **status**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

counters	Display the VTP statistics for the switch.
password	Display the configured VTP password.
status	Display general information about the VTP management domain status.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show vtp counters** command. Table 2-14 describes each field in the display.

```
Switch> show vtp counters
VTP statistics:
Summary advertisements received    : 0
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 0
Subset advertisements transmitted  : 0
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0
```

```
VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- --------------------------
Gi0/47             0                0                0
Gi0/48             0                0                0
Gi0/1              0                0                0
Gi0/2              0                0                0
```

Table 2-14 show vtp counters Field Descriptions

Field	Description
Summary advertisements received	Number of summary advertisements received by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements received	Number of advertisement requests received by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Summary advertisements transmitted	Number of summary advertisements sent by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements transmitted	Number of advertisement requests sent by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Number of configuration revision errors	Number of revision errors. Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the switch increments. Revision errors increment whenever the switch receives an advertisement whose revision number matches the revision number of the switch, but the MD5 digest values do not match. This error means that the VTP password in the two switches is different or that the switches have different configurations. These errors means that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.

Table 2-14 show vtp counters Field Descriptions (continued)

Field	Description
Number of configuration digest errors	Number of MD5 digest errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually means that the VTP password in the two switches is different. To solve this problem, make sure the VTP password on all switches is the same. These errors mean that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of V1 summary errors	Number of Version 1 errors. Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP Version 1 frame. These errors mean that at least one neighboring switch is either running VTP Version 1 or VTP Version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.
Join Transmitted	Number of VTP pruning messages sent on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

This is an example of output from the **show vtp status** command. Table 2-15 describes each field in the display.

```
Switch> show vtp status
VTP Version                     : running VTP2
Configuration Revision          : 579
Maximum VLANs supported locally : 128
Number of existing VLANs        : 63
VTP Operating Mode              : Server
VTP Domain Name                 : lsi1
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Enabled
MD5 digest                      : 0xDD 0x0A 0xFB 0x19 0xB9 0xDC 0x2B 0xF9
```

Table 2-15 show vtp status Field Descriptions

Field	Description
VTP Version	Displays the VTP version operating on the switch. By default, the switch implements Version 1 but can be set to Version 2.
Configuration Revision	Current configuration revision number on this switch.
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.

Table 2-15 show vtp status Field Descriptions (continued)

Field	Description
VTP Operating Mode	Displays the VTP operating mode, which can be server, client, or transparent. Server: a switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all the VLAN information in the current VTP database from NVRAM after reboot. By default, every switch is a VTP server. **Note** The switch automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM and cannot return to server mode until the NVRAM is functioning. Client: a switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database. Transparent: a switch in VTP transparent mode is disabled for VTP, does not send or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.
VTP Domain Name	Name that identifies the administrative domain for the switch.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
VTP V2 Mode	Displays if VTP Version 2 mode is enabled. All VTP Version 2 switches operate in Version 1 mode by default. Each VTP switch automatically detects the capabilities of all the other VTP devices. A network of VTP devices should be configured to Version 2 only if all VTP switches in the network can operate in Version 2 mode.
VTP Traps Generation	Displays whether VTP traps are sent to a network management station.
MD5 Digest	A 16-byte checksum of the VTP configuration.
Configuration Last Modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.

Related Commands

Command	Description
clear vtp counters	Clears the VTP and pruning counters.
vtp (global configuration)	Configures the VTP filename, interface name, domain name, and mode.
vtp (VLAN configuration)	Configures the VTP domain name, password, pruning, and mode.

shutdown

Use the **shutdown** interface configuration command to disable an interface. Use the **no** form of this command to restart a disabled interface.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

The port is enabled (not shut down).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **shutdown** command causes a port to stop forwarding. You can enable the port with the **no shutdown** command.

The **no shutdown** command has no effect if the port is a static-access port assigned to a VLAN that has been deleted, suspended, or shut down. The port must first be a member of an active VLAN before it can be re-enabled.

The **shutdown** command disables all functions on the specified interface.

This command also marks the interface as unavailable. To see if an interface is disabled, use the **show interfaces** privileged EXEC command. An interface that has been shut down is shown as administratively down in the display.

Examples

These examples show how to disable and re-enable a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# shutdown

Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no shutdown
```

You can verify your settings by entering the **show interfaces** privileged EXEC command.

Related Commands

Command	Description
show interfaces	Displays the statistical information specific to all interfaces or to a specific interface.

shutdown vlan

Use the **shutdown vlan** global configuration command to shut down (suspend) local traffic on the specified VLAN. Use the **no** form of this command to restart local traffic on the VLAN.

shutdown vlan *vlan-id*

no shutdown vlan *vlan-id*

Syntax Description

vlan-id	ID of the VLAN to be locally shut down. The range is 2 to 1001. VLANs defined as default VLANs under the VLAN Trunking Protocol (VTP), as well as extended-range VLANs (greater than 1005) cannot be shut down. The default VLANs are 1 and 1002 to 1005.

Defaults

No default is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **shutdown vlan** command does not change the VLAN information in the VTP database. The command shuts down local traffic, but the switch still advertises VTP information.

Examples

This example shows how to shut down traffic on VLAN 2:

```
Switch(config)# shutdown vlan 2
```

You can verify your setting by entering the **show vlan** privileged EXEC command.

Related Commands

Command	Description
shutdown (config-vlan mode)	Shuts down local traffic on the VLAN when in config-VLAN mode (accessed by the **vlan** *vlan-id* global configuration command).

small-frame violation rate

Use the **small-frame violation rate** *pps* interface configuration command to configure the rate (threshold) for an interface to be error disabled when it receives VLAN-tagged packets that are small frames (67 bytes or less) at the specified rate. Use the **no** form of this command to return to the default setting.

small-frame violation rate *pps*

no small-frame violation rate *pps*

Syntax Description

pps	Specify the threshhold at which an interface receiving small frames will be error disabled. The range is 1 to 10,000 packets per second (pps).

Defaults

This feature is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This command enables the rate (threshold) for a port to be error disabled when it receives small frames. Small frames are considered packets that are 67 frames or less.

Use the **errdisable detect cause small-frame** global configuration command to globally enable the small-frames threshold for each port.

You can configure the port to be automatically re-enabled by using the **errdisable recovery cause small-frame** global configuration command. You configure the recovery time by using the **errdisable recovery interval** *interval global configuration command.*

Examples

This example shows how to enable the small-frame arrival rate feature so that the port is error disabled if incoming small frames arrived at 10,000 pps.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# small-frame violation rate 10000
```

You can verify your setting by entering the privileged EXEC command.

Related Commands

Command	Description
errdisable detect cause small-frame	Allows any switch port to be put into the error-disabled state if an incoming frame is smaller than the minimum size and arrives at the specified rate (threshold).
errdisable recovery cause small-frame	**Enables the recovery timer.**
show interfaces	Displays the interface settings on the switch, including input and output flow control.

snmp-server enable traps

Use the **snmp-server enable traps** global configuration command to enable the switch to send Simple Network Management Protocol (SNMP) notifications for various traps or inform requests to the network management system (NMS). Use the **no** form of this command to return to the default setting.

snmp-server enable traps [**bridge** [**newroot**] [**topologychange**] | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **flash** [**insertion** | **removal**] | **fru-ctrl** | **rep** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vtp**]

no snmp-server enable traps [**bridge** [**newroot**] [**topologychange**] | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **flash** [**insertion** | **removal**] | **fru-ctrl** | **rep** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vtp**]

Syntax Description

bridge [**newroot**] [**topologychange**]	(Optional) Generate STP bridge MIB traps. The keywords have these meanings: • **newroot**—(Optional) Enable SNMP STP Bridge MIB new root traps. • **topologychange**—(Optional) Enable SNMP STP Bridge MIB topology change traps.
cluster	(Optional) Enable cluster traps.
config	(Optional) Enable SNMP configuration traps.
config-copy	Optional) Enable SNMP configuration-copy traps
config-ctid	Optional) Enable SNMP configuration change tracking identification (config-ctid) traps
copy-config	(Optional) Enable SNMP copy-configuration traps.
entity	(Optional) Enable SNMP entity traps.
envmon [**fan** | **shutdown** | **status** | **supply** | **temperature**]	Optional) Enable SNMP environmental traps. The keywords have these meanings: • **fan**—(Optional) Enable fan traps. • **shutdown**—(Optional) Enable environmental monitor shutdown traps. • **status**—(Optional) Enable SNMP environmental status-change traps. • **supply**—(Optional) Enable environmental monitor power-supply traps. • **temperature**—(Optional) Enable environmental monitor temperature traps.

flash [**insertion** | **removal**]	(Optional) Enable SNMP FLASH notifications. The keywords have these meanings: **insertion**—(Optional) Generate a trap when a switch (flash) is inserted into a stack, either physically or because of a power cycle or reload. **removal**—(Optional) Generate a trap when a switch (flash) is removed from a stack, either physically or because of a power cycle or reload.
fru-ctrl	(Optional) Enable SNMP entity FRU control traps.
rep	(Optional) Enable SNMP Resilient Ethernet Protocol traps.
snmp [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]	(Optional) Enable SNMP traps. The keywords have these meanings: • **authentication**—(Optional) Enable authentication trap. • **coldstart**—(Optional) Enable cold start trap. • **linkdown**—(Optional) Enable linkdown trap. • **linkup**—(Optional) Enable linkup trap. • **warmstart**—(Optional) Enable warmstart trap.
storm-control trap-rate *value*	(Optional) Enable storm-control traps. Use the **trap-rat**e keyword to set the maximum number of storm-control traps sent per minute. The range is 0 to 1000; the default is 0 (no limit is imposed; a trap is sent at every occurrence).
stpx	(Optional) Enable SNMP STPX MIB traps. The keywords have these meanings: • **inconsistency**—(Optional) Enable SNMP STPX MIB Inconsistency Update traps. • **root-inconsistency**—(Optional) Enable SNMP STPX MIB Root Inconsistency Update traps. • **loop-inconsistency**—(Optional) Enable SNMP STPX MIB Loop Inconsistency Update traps.
syslog	(Optional) Enable SNMP syslog traps.
transceiver	(Optional) Enable SNMP transceiver traps.
tty	(Optional) Send TCP connection traps. This is enabled by default.
vlan-membership	(Optional) Enable SNMP VLAN membership traps.
vlancreate	(Optional) Enable SNMP VLAN-created traps.
vlandelete	(Optional) Enable SNMP VLAN-deleted traps.
vtp	(Optional) Enable VLAN Trunking Protocol (VTP) traps.

Note Though visible in the command-line help strings, the **cpu** [**threshold**] keyword is not supported.

The **snmp-server enable informs** global configuration command is not supported. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** global configuration command combined with the **snmp-server host** *host-addr* **informs** global configuration command.

Defaults

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

When supported, use the **snmp-server enable traps** command to enable sending of traps or informs.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to send VTP traps to the NMS:

```
Switch(config)# snmp-server enable traps vtp
```

You can verify your setting by entering the **show vtp status** or the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.
snmp-server host	Specifies the host that receives SNMP traps.

snmp-server host

Use the **snmp-server host** global configuration command to specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation. Use the **no** form of this command to remove the specified host.

snmp-server host *host-addr* [**informs | traps**] [**version** {**1 | 2c | 3** {**auth | noauth| priv**}] [**vrf** *vrf-instance*] {*community-string* [*notification-type*]}

no snmp-server host *host-addr* [**informs | traps**] [**version** {**1 | 2c | 3** {**auth | noauth | priv**}] [**vrf** *vrf-instance*] *community-string*

Syntax Description

host-addr	Name or Internet address of the host (the targeted recipient).
udp-port *port*	(Optional) Configure the User Datagram Protocol (UDP) port number of the host to receive the traps. The range is 0 to 65535.
**informs	traps**	(Optional) Send SNMP traps or informs to this host.
**version 1	2c	3**	(Optional) Version of the SNMP used to send the traps. These keywords are supported: **1**—SNMPv1. This option is not available with informs. **2c**—SNMPv2C. **3**—SNMPv3. These optional keywords can follow the Version 3 keyword: • **auth** (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. • **noauth** (Default). The noAuthNoPriv security level. This is the default if the [**auth	noauth	priv**] keyword choice is not specified. • **priv** (Optional). Enables Data Encryption Standard (DES) packet encryption (also called *privacy*). **Note** The **priv** keyword is available only when the cryptographic (encrypted) software image is installed.
vrf *vrf-instance*	(Optional) Virtual private network (VPN) routing instance and name for this host.
community-string	Password-like community string sent with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** global configuration command before using the **snmp-server host** command. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the these keywords: • **bridge**—Send SNMP Spanning Tree Protocol (STP) bridge MIB traps. • **cluster**—Send cluster member status traps. • **config**—Send SNMP configuration traps. • **copy-config**—Send SNMP copy configuration traps. • **entity**— Send SNMP entity traps. • **envmon**—Send environmental monitor traps. • **flash**—Send SNMP FLASH notifications. • **fru-ctrl**—Send entity FRU control traps. • **snmp—**Send SNMP-type traps. • **storm-control—**Send SNMP storm-control traps. • **stpx—**Send SNMP STP extended MIB traps. • **syslog—**Send SNMP syslog traps. • **tty—**Send TCP connection traps. • **udp-port** *port***—**Configure the User Datagram Protocol (UDP) port number of the host to receive the traps. The range is from 0 to 65535. • **vlan-membership—** Send SNMP VLAN membership traps. • **vlancreate—**Send SNMP VLAN-created traps. • **vlandelete—**Send SNMP VLAN-deleted traps. • **vtp—**Send SNMP VLAN Trunking Protocol (VTP) traps.

Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is Version 1.

If Version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

If a local user is not associated with a remote host, the switch does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

Examples

This example shows how to configure a unique SNMP community string named *comaccess* for traps and prevent SNMP polling access with this string through access-list 10:

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name *myhost.cisco.com*. The community string is defined as *comaccess*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the switch to send all traps to the host *myhost.cisco.com* by using the community string *public*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.
snmp-server enable traps	Enables SNMP notification for various trap types or inform requests.

snmp trap mac-notification

Use the **snmp trap mac-notification** interface configuration command to enable the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific Layer 2 interface. Use the **no** form of this command to return to the default setting.

snmp trap mac-notification {**added | removed**}

no snmp trap mac-notification {**added | removed**}

Syntax Description

added	Enable the MAC notification trap whenever a MAC address is added on this interface.
removed	Enable the MAC notification trap whenever a MAC address is removed from this interface.

Defaults

By default, the traps for both address addition and address removal are disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Even though you enable the notification trap for a specific interface by using the **snmp trap mac-notification** command, the trap is generated only when you enable the **snmp-server enable traps mac-notification** and the **mac address-table notification** global configuration commands.

Examples

This example shows how to enable the MAC notification trap when a MAC address is added to a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# snmp trap mac-notification added
```

You can verify your settings by entering the **show mac address-table notification interface** privileged EXEC command.

Related Commands

Command	Description
snmp-server enable traps	Sends the SNMP MAC notification traps when the **mac-notification** keyword is appended.

spanning-tree backbonefast

Use the **spanning-tree backbonefast** global configuration command to enable the BackboneFast feature. Use the **no** form of the command to return to the default setting.

spanning-tree backbonefast

no spanning-tree backbonefast

Syntax Description

This command has no arguments or keywords.

Defaults

BackboneFast is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can configure the BackboneFast feature for rapid PVST+ or for multiple spanning-tree (MST) mode, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.

BackboneFast starts when a root port or blocked port on a switch receives inferior BPDUs from its designated switch. An inferior BPDU identifies a switch that declares itself as both the root bridge and the designated switch. When a switch receives an inferior BPDU, it means that a link to which the switch is not directly connected (an *indirect* link) has failed (that is, the designated switch has lost its connection to the root switch. If there are alternate paths to the root switch, BackboneFast causes the maximum aging time on the interfaces on which it received the inferior BPDU to expire and allows a blocked port to move immediately to the listening state. BackboneFast then transitions the interface to the forwarding state. For more information, see the software configuration guide for this release.

Enable BackboneFast on all supported switches to allow the detection of indirect link failures and to start the spanning-tree reconfiguration sooner.

Examples

This example shows how to enable BackboneFast on the switch:

```
Switch(config)# spanning-tree backbonefast
```

You can verify your setting by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree summary	Displays a summary of the spanning-tree interface states.

spanning-tree bpdufilter

Use the **spanning-tree bpdufilter** interface configuration command to prevent an interface from sending or receiving bridge protocol data units (BPDUs). Use the **no** form of this command to return to the default setting.

spanning-tree bpdufilter {**disable** | **enable**}

no spanning-tree bpdufilter

Syntax Description

disable	Disable BPDU filtering on the specified interface.
enable	Enable BPDU filtering on the specified interface.

Defaults

BPDU filtering is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can enable the BPDU filtering feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

Caution Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can globally enable BPDU filtering on all Port Fast-enabled interfaces by using the **spanning-tree portfast bpdufilter default** global configuration command.

You can use the **spanning-tree bpdufilter** interface configuration command to override the setting of the **spanning-tree portfast bpdufilter default** global configuration command.

Examples

This example shows how to enable the BPDU filtering feature on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpdufilter enable
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interface or enables the Port Fast feature on all nontrunking interfaces.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.

spanning-tree bpduguard

Use the **spanning-tree bpduguard** interface configuration command to put an interface in the error-disabled state when it receives a bridge protocol data unit (BPDU). Use the **no** form of this command to return to the default setting.

spanning-tree bpduguard {**disable** | **enable**}

no spanning-tree bpduguard

Syntax Description

disable	Disable BPDU guard on the specified interface.
enable	Enable BPDU guard on the specified interface.

Defaults

BPDU guard is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU guard feature in a service-provider network to prevent an interface from being included in the spanning-tree topology.

You can enable the BPDU guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

You can globally enable BPDU guard on all Port Fast-enabled interfaces by using the **spanning-tree portfast bpduguard default** global configuration command.

You can use the **spanning-tree bpduguard** interface configuration command to override the setting of the **spanning-tree portfast bpduguard default** global configuration command.

Examples

This example shows how to enable the BPDU guard feature on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpduguard enable
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.

spanning-tree cost

Use the **spanning-tree cost** interface configuration command to set the path cost for spanning-tree calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to place in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree [**vlan** *vlan-id*] **cost** *cost*

no spanning-tree [**vlan** *vlan-id*] **cost**

Syntax Description

vlan *vlan-id*	(Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
cost	Path cost. The range is 1 to 200000000, with higher values meaning higher costs.

Defaults

The default path cost is computed from the interface bandwidth setting. These are the IEEE default path cost values:

- 1000 Mb/s—4
- 100 Mb/s—19
- 10 Mb/s—100

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When you configure the cost, higher values represent higher costs.

If you configure an interface with both the **spanning-tree vlan** *vlan-id* **cost** *cost* command and the **spanning-tree cost** *cost* command, the **spanning-tree vlan** *vlan-id* **cost** *cost* command takes effect.

Examples

This example shows how to set the path cost to 250 on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree cost 250
```

This example shows how to set a path cost to 300 for VLANs 10, 12 to 15, and 20:

```
Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

You can verify your settings by entering the **show spanning-tree interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
show spanning-tree interface *interface-id*	Displays spanning-tree information for the specified interface.
spanning-tree port-priority	Configures an interface priority.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree etherchannel guard misconfig

Use the **spanning-tree etherchannel guard misconfig** global configuration command to display an error message when the switch detects an EtherChannel misconfiguration. Use the **no** form of this command to disable the feature.

spanning-tree etherchannel guard misconfig

no spanning-tree etherchannel guard misconfig

Syntax Description

This command has no arguments or keywords.

Defaults

EtherChannel guard is enabled on the switch.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When the switch detects an EtherChannel misconfiguration, this error message appears:

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in
err-disable state.
```

To show switch ports that are in the misconfigured EtherChannel, use the **show interfaces status err-disabled** privileged EXEC command. To verify the EtherChannel configuration on a remote device, use the **show etherchannel summary** privileged EXEC command on the remote device.

When a port is in the error-disabled state because of an EtherChannel misconfiguration, you can bring it out of this state by entering the **errdisable recovery cause channel-misconfig** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

Examples

This example shows how to enable the EtherChannel guard misconfiguration feature:

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

You can verify your settings by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands

Command	Description
errdisable recovery cause channel-misconfig	Enables the timer to recover from the EtherChannel misconfiguration error-disabled state.
show etherchannel summary	Displays EtherChannel information for a channel as a one-line summary per channel-group.
show interfaces status err-disabled	Displays the interfaces in the error-disabled state.

spanning-tree extend system-id

Use the **spanning-tree extend system-id** global configuration command to enable the extended system ID feature.

spanning-tree extend system-id

Note Though visible in the command-line help strings, the **no** version of this command is not supported. You cannot disable the extended system ID feature.

Syntax Description

This command has no arguments or keywords.

Defaults

The extended system ID is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The switch supports the IEEE 802.1t spanning-tree extensions. Some of the bits previously used for the switch priority are now used for the extended system ID (VLAN identifier for the per-VLAN spanning-tree plus [PVST+] and rapid PVST+ or as an instance identifier for the multiple spanning tree [MST]).

The spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN or multiple spanning-tree instance.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For more information, see the "spanning-tree mst root" and the "spanning-tree vlan" sections.

If your network consists of switches that do not support the extended system ID and switches that do support it, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches.

Related Commands

Command	Description
show spanning-tree summary	Displays a summary of spanning-tree interface states.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree guard

Use the **spanning-tree guard** interface configuration command to enable root guard or loop guard on all the VLANs associated with the selected interface. Root guard restricts which interface is allowed to be the spanning-tree root port or the path-to-the root for the switch. Loop guard prevents alternate or root ports from becoming designated ports when a failure creates a unidirectional link. Use the **no** form of this command to return to the default setting.

spanning-tree guard {**loop** | **none** | **root**}

no spanning-tree guard

Syntax Description

loop	Enable loop guard.
none	Disable root guard or loop guard.
root	Enable root guard.

Defaults

Root guard is disabled.

Loop guard is configured according to the **spanning-tree loopguard default** global configuration command (globally disabled).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can enable root guard or loop guard when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

When root guard is enabled, if spanning-tree calculations cause an interface to be selected as the root port, the interface transitions to the root-inconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root. The root port provides the best path from the switch to the root switch.

When the **no spanning-tree guard** or the **no spanning-tree guard none** command is entered, root guard is disabled for all VLANs on the selected interface. If this interface is in the root-inconsistent (blocked) state, it automatically transitions to the listening state.

Do not enable root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state. The UplinkFast feature is not available when the switch is operating in the rapid-PVST+ or MST mode.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

To disable root guard or loop guard, use the **spanning-tree guard none** interface configuration command. You cannot enable both root guard and loop guard at the same time.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

Examples

This example shows how to enable root guard on all the VLANs associated with the specified port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard root
```

This example shows how to enable loop guard on all the VLANs associated with the specified port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard loop
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree loopguard default	Prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link.
spanning-tree mst cost	Configures the path cost for MST calculations.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree port-priority	Configures an interface priority.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree link-type

Use the **spanning-tree link-type** interface configuration command to override the default link-type setting, which is determined by the duplex mode of the interface, and to enable rapid spanning-tree transitions to the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree link-type {**point-to-point** | **shared**}

no spanning-tree link-type

Syntax Description

point-to-point	Specify that the link type of an interface is point-to-point.
shared	Specify that the link type of an interface is shared.

Defaults

The switch derives the link type of an interface from the duplex mode. A full-duplex interface is considered a point-to-point link, and a half-duplex interface is considered a shared link.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can override the default setting of the link type by using the **spanning-tree link-type** command. For example, a half-duplex link can be physically connected point-to-point to a single interface on a remote switch running the Multiple Spanning Tree Protocol (MSTP) or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol and be enabled for rapid transitions.

Examples

This example shows how to specify the link type as shared (regardless of the duplex setting) and to prevent rapid transitions to the forwarding state:

```
Switch(config-if)# spanning-tree link-type shared
```

You can verify your setting by entering the **show spanning-tree mst interface** *interface-id* or the show **spanning-tree interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
clear spanning-tree detected-protocols	Restarts the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.
show spanning-tree interface *interface-id*	Displays spanning-tree state information for the specified interface.
show spanning-tree mst interface *interface-id*	Displays MST information for the specified interface.

spanning-tree loopguard default

Use the **spanning-tree loopguard default** global configuration command to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. Use the **no** form of this command to return to the default setting.

spanning-tree loopguard default

no spanning-tree loopguard default

Syntax Description

This command has no arguments or keywords.

Defaults

Loop guard is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can enable the loop guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

Loop guard operates only on interfaces that the spanning tree identifies as point-to-point.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

Examples

This example shows how to globally enable loop guard:

```
Switch(config)# spanning-tree loopguard default
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree guard loop	Enables the loop guard feature on all the VLANs associated with the specified interface.

spanning-tree mode

Use the **spanning-tree mode** global configuration command to enable per-VLAN spanning-tree plus (PVST+), rapid PVST+, or multiple spanning tree (MST) on your switch. Use the **no** form of this command to return to the default setting.

spanning-tree mode {**mst** | **pvst** | **rapid-pvst**}

no spanning-tree mode

Syntax Description

mst	Enable MST and Rapid Spanning Tree Protocol (RSTP) (based on IEEE 802.1s and IEEE 802.1w).
pvst	Enable PVST+ (based on IEEE 802.1D).
rapid-pvst	Enable rapid PVST+ (based on IEEE 802.1w).

Defaults

The default mode is PVST+.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The switch supports PVST+, rapid PVST+, and MSTP, but only one version can be active at any time: All VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.

When you enable the MST mode, RSTP is automatically enabled.

Caution Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode.

Examples

This example shows to enable MST and RSTP on the switch:

```
Switch(config)# spanning-tree mode mst
```

This example shows to enable rapid PVST+ on the switch:

```
Switch(config)# spanning-tree mode rapid-pvst
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.

spanning-tree mst configuration

Use the **spanning-tree mst configuration** global configuration command to enter multiple spanning-tree (MST) configuration mode through which you configure the MST region. Use the **no** form of this command to return to the default settings.

spanning-tree mst configuration

no spanning-tree mst configuration

Syntax Description

This command has no arguments or keywords.

Defaults

The default mapping is that all VLANs are mapped to the common and internal spanning-tree (CIST) instance (instance 0).

The default name is an empty string.

The revision number is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **spanning-tree mst configuration** command enables the MST configuration mode. These configuration commands are available:

- **abort**: exits the MST region configuration mode without applying configuration changes.
- **exit**: exits the MST region configuration mode and applies all configuration changes.
- **instance** *instance-id* **vlan** *vlan-range*: maps VLANs to an MST instance. The range for the *instance-id* is 1 to 4094. The range for *vlan-range* is 1 to 4094. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.
- **name** *name*: sets the configuration name. The *name* string has a maximum length of 32 characters and is case sensitive.
- **no**: negates the **instance**, **name**, and **revision** commands or sets them to their defaults.
- **private-vlan**: Though visible in the command-line help strings, this command is not supported.
- **revision** *version*: sets the configuration revision number. The range is 0 to 65535.
- **show** [**current** | **pending**]: displays the current or pending MST region configuration.

In MST mode, the switch supports up to 65 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

When you map VLANs to an MST instance, the mapping is incremental, and VLANs specified in the command are added to or removed from the VLANs that were previously mapped. To specify a range, use a hyphen; for example, **instance 1 vlan 1-63** maps VLANs 1 to 63 to MST instance 1. To specify a series, use a comma; for example, **instance 1 vlan 10, 20, 30** maps VLANs 10, 20, and 30 to MST instance 1.

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST by using the **no** form of the command.

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Examples

This example shows how to enter MST configuration mode, map VLANs 10 to 20 to MST instance 1, name the region *region1*, set the configuration revision to 1, display the pending configuration, apply the changes, and return to global configuration mode:

```
Switch# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------

Switch(config-mst)# exit
Switch(config)#
```

This example shows how to add VLANs 1 to 100 to the ones already mapped (if any) to instance 2, to move VLANs 40 to 60 that were previously mapped to instance 2 to the CIST instance, to add VLAN 10 to instance 10, and to remove all the VLANs mapped to instance 2 and map them to the CIST instance:

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

You can verify your settings by entering the **show pending** MST configuration command.

Related Commands

Command	Description
show spanning-tree mst configuration	Displays the MST region configuration.

spanning-tree mst cost

Use the **spanning-tree mst cost** interface configuration command to set the path cost for multiple spanning-tree (MST) calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

Syntax Description

instance-id	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
cost	Path cost is 1 to 200000000, with higher values meaning higher costs.

Defaults

The default path cost is computed from the interface bandwidth setting. These are the IEEE default path cost values:

- 1000 Mb/s—20000
- 100 Mb/s—200000
- 10 Mb/s—2000000

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When you configure the cost, higher values represent higher costs.

Examples

This example shows how to set a path cost of 250 on a port associated with instances 2 and 4:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst interface *interface-id*	Displays MST information for the specified interface.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.

spanning-tree mst forward-time

Use the **spanning-tree mst forward-time** global configuration command to set the forward-delay time for all multiple spanning-tree (MST) instances. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. Use the **no** form of this command to return to the default setting.

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

Syntax Description

seconds	Length of the listening and learning states. The range is 4 to 30 seconds.

Defaults

The default is 15 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Changing the **spanning-tree mst forward-time** command affects all spanning-tree instances.

Examples

This example shows how to set the spanning-tree forwarding time to 18 seconds for all MST instances:

```
Switch(config)# spanning-tree mst forward-time 18
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst hello-time	Sets the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst hello-time

Use the **spanning-tree mst hello-time** global configuration command to set the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages. Use the **no** form of this command to return to the default setting.

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

Syntax Description

seconds	Interval between hello BPDUs sent by root switch configuration messages. The range is 1 to 10 seconds.

Defaults

The default is 2 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(46)EY	This command was introduced.

Usage Guidelines

After you set the **spanning-tree mst max-age** *seconds* global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

Changing the **spanning-tree mst hello-time** command affects all spanning-tree instances.

Examples

This example shows how to set the spanning-tree hello time to 3 seconds for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst hello-time 3
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst max-age

Use the **spanning-tree mst max-age** global configuration command to set the interval between messages that the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputes the spanning-tree topology. Use the **no** form of this command to return to the default setting.

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

Syntax Description

seconds	Interval between messages the spanning tree receives from the root switch. The range is 6 to 40 seconds.

Defaults

The default is 20 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

After you set the **spanning-tree mst max-age** *seconds* global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

Changing the **spanning-tree mst max-age** command affects all spanning-tree instances.

Examples

This example shows how to set the spanning-tree max-age to 30 seconds for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst max-age 30
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst max-hops

Use the **spanning-tree mst max-hops** global configuration command to set the number of hops in a region before the bridge protocol data unit (BPDU) is discarded and the information held for an interface is aged. Use the **no** form of this command to return to the default setting.

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

Syntax Description

hop-count	Number of hops in a region before the BPDU is discarded. The range is 1 to 255 hops.

Defaults

The default is 20 hops.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates the decremented count as the remaining hop count in the generated M-records. A switch discards the BPDU and ages the information held for the interface when the count reaches 0.

Changing the **spanning-tree mst max-hops** command affects all spanning-tree instances.

Examples

This example shows how to set the spanning-tree max-hops to 10 for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst max-hops 10
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.

spanning-tree mst port-priority

Use the **spanning-tree mst port-priority** interface configuration command to configure an interface priority. If a loop occurs, the Multiple Spanning Tree Protocol (MSTP) can find the interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

Syntax Description

instance-id	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
priority	The range is 0 to 240 in increments of 16. Valid priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.

Defaults

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, the multiple spanning tree (MST) puts the interface with the lowest interface number in the forwarding state and blocks other interfaces.

Examples

This example shows how to increase the likelihood that the interface associated with spanning-tree instances 20 and 22 is placed into the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 20,22 port-priority 0
```

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst interface *interface-id*	Displays MST information for the specified interface.

Command	Description
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree mst pre-standard

Use the **spanning-tree mst pre-standard** interface configuration command to configure a port to send only prestandard bridge protocol data units (BPDUs).

spanning-tree mst pre-standard

no spanning-tree mst pre-standard

Syntax Description

This command has no arguments or keywords.

Command Default

The default state is automatic detection of prestandard neighbors.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The port can accept both prestandard and standard BPDUs. If the neighbor types are mismatched, only the common and internal spanning tree (CIST) runs on this interface.

Note If a switch port is connected to a switch running prestandard Cisco IOS software, you *must* use the **spanning-tree mst pre-standard** interface configuration command on the port. If you do not configure the port to send only prestandard BPDUs, the Multiple STP (MSTP) performance might diminish.

When the port is configured to automatically detect prestandard neighbors, the *prestandard* flag always appears in the **show spanning-tree mst** commands.

Examples

This example shows how to configure a port to send only prestandard BPDUs:

```
Switch(config-if)# spanning-tree mst pre-standard
```

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst *instance-id*	Displays multiple spanning-tree (MST) information, including the *prestandard* flag, for the specified interface.

spanning-tree mst priority

Use the **spanning-tree mst priority** global configuration command to set the switch priority for the specified spanning-tree instance. Use the **no** form of this command to return to the default setting.

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

Syntax Description

instance-id	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
priority	Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. The range is 0 to 61440 in increments of 4096. Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

Defaults

The default is 32768.

Command Modes

Global configuration

Command History

Release	Modification
12.2(46)EY	This command was introduced.

Examples

This example shows how to set the spanning-tree priority to 8192 for multiple spanning-tree instances (MST) 20 to 21:

```
Switch(config)# spanning-tree mst 20-21 priority 8192
```

You can verify your settings by entering the **show spanning-tree mst** *instance-id* privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst *instance-id*	Displays MST information for the specified interface.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst port-priority	Configures an interface priority.

spanning-tree mst root

Use the **spanning-tree mst root** global configuration command to configure the multiple spanning-tree (MST) root switch priority and timers based on the network diameter. Use the **no** form of this command to return to the default settings.

spanning-tree mst *instance-id* **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]

no spanning-tree mst *instance-id* **root**

Syntax Description

instance-id	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
root primary	Force this switch to be the root switch.
root secondary	Set this switch to be the root switch should the primary root switch fail.
diameter *net-diameter*	(Optional) Set the maximum number of switches between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0.
hello-time *seconds*	(Optional) Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds. This keyword is available only for MST instance 0.

Defaults

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

The hello time is 2 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **spanning-tree mst** *instance-id* **root** command only on backbone switches.

When you enter the **spanning-tree mst** *instance-id* **root** command, the software tries to set a high enough priority to make this switch the root of the spanning-tree instance. Because of the extended system ID support, the switch sets the switch priority for the instance to 24576 if this value will cause this switch to become the root for the specified instance. If any root switch for the specified instance has a switch priority lower than 24576, the switch sets its own priority to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree mst** *instance-id* **root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch fails, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768 and are therefore unlikely to become the root switch).

Examples

This example shows how to configure the switch as the root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree mst** *instance-id* privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst *instance-id*	Displays MST information for the specified instance.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree port-priority

Use the **spanning-tree port-priority** interface configuration command to configure an interface priority. If a loop occurs, spanning tree can find the interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree [**vlan** *vlan-id*] **port-priority** *priority*

no spanning-tree [**vlan** *vlan-id*] **port-priority**

Syntax Description

vlan *vlan-id*	(Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
priority	Number from 0 to 240, in increments of 16. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.

Defaults

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If the variable *vlan-id* is omitted, the command applies to the spanning-tree instance associated with VLAN 1.

You can set the priority on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign the interface to the VLAN.

If you configure an interface with both the **spanning-tree vlan** *vlan-id* **port-priority** *priority* command and the **spanning-tree port-priority** *priority* command, the **spanning-tree vlan** *vlan-id* **port-priority** *priority* command takes effect.

Examples

This example shows how to increase the likelihood that a port will be put in the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

This example shows how to set the port-priority value on VLANs 20 to 25:

```
Switch(config-if)# spanning-tree vlan 20-25 port-priority 0
```

You can verify your settings by entering the **show spanning-tree interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
show spanning-tree interface *interface-id*	Displays spanning-tree information for the specified interface.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree portfast (global configuration)

Use the **spanning-tree portfast** global configuration command to globally enable bridge protocol data unit (BPDU) filtering on Port Fast-enabled interfaces, the BPDU guard feature on Port Fast-enabled interfaces, or the Port Fast feature on all nontrunking interfaces. The BPDU filtering feature prevents the switch interface from sending or receiving BPDUs. The BPDU guard feature puts Port Fast-enabled interfaces that receive BPDUs in an error-disabled state. Use the **no** form of this command to return to the default settings.

spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

no spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

Syntax Description

bpdufilter default	Globally enable BPDU filtering on Port Fast-enabled interfaces and prevent the switch interface connected to end stations from sending or receiving BPDUs.
bpduguard default	Globally enable the BPDU guard feature on Port Fast-enabled interfaces and place the interfaces that receive BPDUs in an error-disabled state.
default	Globally enable the Port Fast feature on all nontrunking interfaces. When the Port Fast feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes.

Defaults

The BPDU filtering, the BPDU guard, and the Port Fast features are disabled on all interfaces unless they are individually configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can enable these features when the switch is operating in the per-VLAN spanning-tree plus (PVST+) rapid-PVST+, or the multiple spanning-tree (MST) mode.

Use the **spanning-tree portfast bpdufilter default** global configuration command to globally enable BPDU filtering on interfaces that are Port Fast-enabled (the interfaces are in a Port Fast-operational state). The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to switch interfaces do not receive BPDUs. If a BPDU is received on a Port Fast-enabled interface, the interface loses its Port Fast-operational status and BPDU filtering is disabled.

You can override the **spanning-tree portfast bpdufilter default** global configuration command by using the **spanning-tree bdpufilter** interface configuration command.

Caution Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on interfaces that are in a Port Fast-operational state. In a valid configuration, Port Fast-enabled interfaces do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled interface signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the interface in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You can override the **spanning-tree portfast bpduguard default** global configuration command by using the **spanning-tree bdpuguard** interface configuration command.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking interfaces. Configure Port Fast only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A Port Fast-enabled interface moves directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-delay time.

You can override the **spanning-tree portfast default** global configuration command by using the **spanning-tree portfast** interface configuration command. You can use the **no spanning-tree portfast default** global configuration command to disable Port Fast on all interfaces unless they are individually configured with the **spanning-tree portfast** interface configuration command.

Examples

This example shows how to globally enable the BPDU filtering feature:

```
Switch(config)# spanning-tree portfast bpdufilter default
```

This example shows how to globally enable the BPDU guard feature:

```
Switch(config)# spanning-tree portfast bpduguard default
```

This example shows how to globally enable the Port Fast feature on all nontrunking interfaces:

```
Switch(config)# spanning-tree portfast default
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree bpdufilter	Prevents an interface from sending or receiving BPDUs.
spanning-tree bpduguard	Puts an interface in the error-disabled state when it receives a BPDU.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface in all its associated VLANs.

spanning-tree portfast (interface configuration)

Use the **spanning-tree portfast** interface configuration command to enable the Port Fast feature on an interface in all its associated VLANs. When the Port Fast feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes. Use the **no** form of this command to return to the default setting.

spanning-tree portfast [**disable** | **trunk**]

no spanning-tree portfast

Syntax Description

disable	(Optional) Disable the Port Fast feature on the specified interface.
trunk	(Optional) Enable the Port Fast feature on a trunking interface.

Defaults

The Port Fast feature is disabled on all interfaces; however, it is automatically enabled on dynamic-access ports.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use this feature only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.

To enable Port Fast on trunk ports, you must use the **spanning-tree portfast trunk** interface configuration command. The **spanning-tree portfast** command is not supported on trunk ports.

You can enable this feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

This feature affects all VLANs on the interface.

An interface with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without the standard forward-time delay.

You can use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking interfaces. However, the **spanning-tree portfast** interface configuration command can override the global setting.

If you configure the **spanning-tree portfast default** global configuration command, you can disable Port Fast on an interface that is not a trunk interface by using the **spanning-tree portfast disable** interface configuration command.

Examples

This example shows how to enable the Port Fast feature on a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree portfast
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree bpdufilter	Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts an interface in the error-disabled state when it receives a BPDU.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.

spanning-tree transmit hold-count

Use the **spanning-tree transmit hold-count** global configuration command to configure the number of bridge protocol data units (BPDUs) sent every second. Use the **no** form of this command to return to the default setting.

spanning-tree transmit hold-count [*value*]

no spanning-tree transmit hold-count [*value*]

Syntax Description

value	(Optional) Number of BPDUs sent every second. The range is 1 to 20.

Defaults

The default is 6.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Increasing the transmit hold-count value can have a significant impact on CPU utilization when the switch is in rapid-per-VLAN spanning-tree plus (rapid-PVST+) mode. Decreasing this value might slow down convergence. We recommend using the default setting.

Examples

This example shows how to set the transmit hold count to 8:

```
Switch(config)# spanning-tree transmit hold-count 8
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst	Displays the multiple spanning-tree (MST) region configuration and status, including the transmit hold count.

spanning-tree uplinkfast

Use the **spanning-tree uplinkfast** global configuration command to accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. Use the **no** form of this command to return to the default setting.

spanning-tree uplinkfast [**max-update-rate** *pkts-per-second*]

no spanning-tree uplinkfast [**max-update-rate**]

Syntax Description

max-update-rate *pkts-per-second*	(Optional) The number of packets per second at which update packets are sent. The range is 0 to 32000.

Defaults

UplinkFast is disabled.

The update rate is 150 packets per second.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use this command only on access switches.

You can configure the UplinkFast feature for rapid PVST+ or for multiple spanning-tree (MST) mode, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.

When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs.

When UplinkFast is enabled, the switch priority of all VLANs is set to 49152. If you change the path cost to a value less than 3000 and you enable UplinkFast or UplinkFast is already enabled, the path cost of all interfaces and VLAN trunks is increased by 3000 (if you change the path cost to 3000 or above, the path cost is not altered). The changes to the switch priority and the path cost reduces the chance that a switch will become the root switch.

When UplinkFast is disabled, the switch priorities of all VLANs and path costs of all interfaces are set to default values if you did not modify them from their defaults.

When spanning tree detects that the root port has failed, UplinkFast immediately changes to an alternate root port, changing the new root port directly to forwarding state. During this time, a topology change notification is sent.

Do not enable the root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state.

If you set the max-update-rate to 0, station-learning frames are not generated, so the spanning-tree topology converges more slowly after a loss of connectivity.

Examples

This example shows how to enable UplinkFast:

```
Switch(config)# spanning-tree uplinkfast
```

You can verify your setting by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree summary	Displays a summary of the spanning-tree interface states.
spanning-tree vlan root primary	Forces this switch to be the root switch.

spanning-tree vlan

Use the **spanning-tree vlan** global configuration command to configure spanning tree on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

spanning-tree vlan *vlan-id* [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]]

no spanning-tree vlan *vlan-id* [**forward-time** | **hello-time** | **max-age** | **priority** | **root**]

Syntax Description

vlan-id	VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
forward-time *seconds*	(Optional) Set the forward-delay time for the specified spanning-tree instance. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds.
hello-time *seconds*	(Optional) Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds.
max-age *seconds*	(Optional) Set the interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds.
priority *priority*	(Optional) Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. The range is 0 to 61440 in increments of 4096. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
root primary	(Optional) Force this switch to be the root switch.
root secondary	(Optional) Set this switch to be the root switch should the primary root switch fail.
diameter *net-diameter*	(Optional) Set the maximum number of switches between any two end stations. The range is 2 to 7.

Defaults

Spanning tree is enabled on all VLANs.

The forward-delay time is 15 seconds.

The hello time is 2 seconds.

The max-age is 20 seconds.

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

Command Modes Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. Interfaces that are administratively down remain down. Received BPDUs are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.

You can disable the STP on a VLAN that is not currently active and verify the change by using the **show running-config** or the **show spanning-tree vlan** *vlan-id* privileged EXEC command. The setting takes effect when the VLAN is activated.

When disabling or re-enabling the STP, you can specify a range of VLANs that you want to disable or enable.

When a VLAN is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign interfaces to it.

When setting the **max-age** *seconds,* if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

The **spanning-tree vlan** *vlan-id* **root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan** *vlan-id* **root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan** *vlan-id* **root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

Examples This example shows how to disable the STP on VLAN 5:

```
Switch(config)# no spanning-tree vlan 5
```

You can verify your setting by entering the **show spanning-tree** privileged EXEC command. In this instance, VLAN 5 does not appear in the list.

This example shows how to set the spanning-tree forwarding time to 18 seconds for VLANs 20 and 25:

```
Switch(config)# spanning-tree vlan 20,25 forward-time 18
```

This example shows how to set the spanning-tree hello-delay time to 3 seconds for VLANs 20 to 24:

```
Switch(config)# spanning-tree vlan 20-24 hello-time 3
```

This example shows how to set spanning-tree max-age to 30 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 max-age 30
```

This example shows how to reset the **max-age** parameter to the default value for spanning-tree instance 100 and 105 to 108:

```
Switch(config)# no spanning-tree vlan 100, 105-108 max-age
```

This example shows how to set the spanning-tree priority to 8192 for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

This example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree vlan** *vlan-id* privileged EXEC command.

Related Commands

Command	Description
show spanning-tree vlan	Displays spanning-tree information.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree port-priority	Sets an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface in all its associated VLANs.
spanning-tree uplinkfast	Enables the UplinkFast feature, which accelerates the choice of a new root port.

speed

Use the **speed** interface configuration command to specify the speed of a 10/100 Mb/s or 10/100/1000 Mb/s port. Use the **no** or **default** form of this command to return the port to its default value.

speed {**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**] | **nonegotiate**}

no speed

Syntax Description

10	Port runs at 10 Mb/s.
100	Port runs at 100 Mb/s.
1000	Port runs at 1000 Mb/s. This option is valid and visible only on 10/100/1000 Mb/s-ports.
auto	Port automatically detects the speed it should run at based on the port at the other end of the link. If you use the **10**, **100**, or **1000** keywords with the **auto** keyword, the port only autonegotiates at the specified speeds.
nonegotiate	Autonegotiation is disabled, and the port runs at 1000 Mb/s.

Defaults

The default is **auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You cannot configure speed on the 10-Gigabit Ethernet ports.

Except for the 1000BASE-T small form-factor pluggable (SFP) modules, you can configure the speed to not negotiate (**nonegotiate**) when an SFP module port is connected to a device that does not support autonegotiation.

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

If both ends of the line support autonegotiation, we highly recommend the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, do use the **auto** setting on the supported side, but set the duplex and speed on the other side.

Caution Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

For guidelines on setting the switch speed and duplex parameters, see the "Configuring Interface Characteristics" chapter in the software configuration guide for this release.

Examples

This example shows how to set speed on a port to 100 Mb/s:

```
Switch(config)# interface gigabitethernet0/17
Switch(config-if)# speed 100
```

This example shows how to set a port to autonegotiate at only 10 Mb/s:

```
Switch(config)# interface gigabitethernet0/18
Switch(config-if)# speed auto 10
```

This example shows how to set a port to autonegotiate at only 10 or 100 Mb/s:

```
Switch(config)# interface gigabitethernet0/17
Switch(config-if)# speed auto 10 100
```

You can verify your settings by entering the **show interfaces** privileged EXEC command.

Related Commands

Command	Description
duplex	Specifies the duplex mode of operation.
show interfaces	Displays the statistical information specific to all interfaces or to a specific interface.

srr-queue bandwidth limit

Use the **srr-queue bandwidth limit** interface configuration command to limit the maximum output on a port. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth limit *weight1*

no srr-queue bandwidth limit

Syntax Description

weight1	Percentage of the port speed to which the port should be limited. The range is 10 to 90.

Defaults

The port is not rate limited and is set to 100 percent.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If you configure this command to 80 percent, the port is idle 20 percent of the time. The line rate drops to 80 percent of the connected speed. These values are not exact because the hardware adjusts the line rate in increments of six.

Note The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your quality of service (QoS) solution.

Examples

This example shows how to limit a port to 800 Mb/s:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **queueing** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to the queue-set.
mls qos srr-queue output cos-map	Maps class of service (CoS) values to egress queue or maps CoS values to a queue and to a threshold ID.
mls qos trust	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation for the queue-set.
radius-server dead-criteria	Maps a port to a queue-set.
show mls qos interface queueing	Displays QoS information.
srr-queue bandwidth shape	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
srr-queue bandwidth share	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

srr-queue bandwidth shape

Use the **srr-queue bandwidth shape** interface configuration command to assign the shaped weights and to enable bandwidth shaping on the four egress queues mapped to a port. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth shape *weight1 weight2 weight3 weight4*

no srr-queue bandwidth shape

Syntax Description

weight1 weight2 weight3 weight4	Specify the weights to specify the percentage of the port that is shaped. The inverse ratio (1/*weight*) specifies the shaping bandwidth for this queue. Separate each value with a space. The range is 0 to 65535.

Defaults

Weight1 is set to 25. Weight2, weight3, and weight4 are set to 0, and these queues are in shared mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

In shaped mode, the queues are guaranteed a percentage of the bandwidth, and they are rate-limited to that amount. Shaped traffic does not use more than the allocated bandwidth even if the link is idle. Use shaping to smooth bursty traffic or to provide a smoother output over time.

The shaped mode overrides the shared mode.

If you configure a shaped queue weight to 0 by using the **srr-queue bandwidth shape** interface configuration command, this queue participates in shared mode. The weight specified with the **srr-queue bandwidth shape** command is ignored, and the weights specified with the **srr-queue bandwidth share** interface configuration command for a queue come into effect.

When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.

Note The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Examples

This example shows how to configure the queues for the same port for both shaping and sharing. Because the weight ratios for queues 2, 3, and 4 are set to 0, these queues operate in shared mode. The bandwidth weight for queue 1 is 1/8, which is 12.5 percent. Queue 1 is guaranteed this bandwidth and limited to it; it does not extend its slot to the other queues even if the other queues have no traffic and are idle. Queues 2, 3, and 4 are in shared mode, and the setting for queue 1 is ignored. The bandwidth ratio allocated for the queues in shared mode is 4/(4+4+4), which is 33 percent:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
Switch(config-if)# srr-queue bandwidth share 4 4 4 4
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **queueing** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to a queue-set.
mls qos srr-queue output cos-map	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos trust	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
priority-queue	Enables the egress expedite queue on a port.
radius-server dead-criteria	Maps a port to a queue-set.
show mls qos interface queueing	Displays quality of service (QoS) information.
srr-queue bandwidth share	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

srr-queue bandwidth share

Use the **srr-queue bandwidth share** interface configuration command to assign the shared weights and to enable bandwidth sharing on the four egress queues mapped to a port. The ratio of the weights is the ratio of frequency in which the shaped round robin (SRR) scheduler dequeues packets from each queue. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth share *weight1 weight2 weight3 weight4*

no srr-queue bandwidth share

Syntax Description

weight1 weight2 weight3 weight4	The ratios of *weight1*, *weight2*, *weight3*, and *weight4* specify the ratio of the frequency in which the SRR scheduler dequeues packets. Separate each value with a space. The range is 1 to 255.

Defaults

Weight1, weight2, weight3, and weight4 are 25 (1/4 of the bandwidth is allocated to each queue).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The absolute value of each weight is meaningless, and only the ratio of parameters is used.

In shared mode, the queues share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it. For example, if a queue empties and does not require a share of the link, the remaining queues can expand into the unused bandwidth and share it among themselves.

If you configure a shaped queue weight to 0 by using the **srr-queue bandwidth shape** interface configuration command, this queue participates in SRR shared mode. The weight specified with the **srr-queue bandwidth shape** command is ignored, and the weights specified with the **srr-queue bandwidth share** interface configuration command for a queue take effect.

When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.

Note The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Examples

This example shows how to configure the weight ratio of the SRR scheduler running on an egress port. Four queues are used. The bandwidth ratio allocated for each queue in shared mode is 1/(1+2+3+4), 2/(1+2+3+4), 3/(1+2+3+4), and 4/(1+2+3+4), which is 10 percent, 20 percent, 30 percent, and 40 percent for queues 1, 2, 3, and 4. This means that queue 4 has four times the bandwidth of queue 1, twice the bandwidth of queue 2, and one-and-a-third times the bandwidth of queue 3.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **queueing** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to a queue-set.
mls qos srr-queue output cos-map	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos trust	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
priority-queue	Enables the egress expedite queue on a port.
radius-server dead-criteria	Maps a port to a queue-set.
show mls qos interface queueing	Displays quality of service (QoS) information.
srr-queue bandwidth shape	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.

switchport access

Use the **switchport access** interface configuration command to configure a port as a static-access port. If the switchport mode is set to **access**, the port operates as a member of the specified VLAN.

switchport access vlan *vlan-id*

no switchport access vlan

Syntax Description

vlan *vlan-id*	Configure the interface as a static access port with the VLAN ID of the access mode VLAN; the range is 1 to 4094.

Defaults

The default access VLAN and trunk interface native VLAN is a default VLAN corresponding to the platform or interface hardware.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **no switchport access** command resets the access mode VLAN to the appropriate default VLAN for the device.

The port must be in access mode before the **switchport access vlan** command can take effect.

An access port can be assigned to only one VLAN.

Examples

This example shows how to change a switched port interface that is operating in access mode to operate in VLAN 2 instead of the default VLAN:

```
Switch(config-if)# switchport access vlan 2
```

You can verify your setting by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

switchport autostate exclude

Use the **switchport autostate exclude** interface configuration command to exclude an interface from the VLAN interface (switch virtual interface) line-state up or down calculation. Use the **no** form of this command to return to the default setting.

switchport autostate exclude

no switchport autostate exclude

Syntax Description

This command has no arguments or keywords.

Defaults

All ports in the VLAN are included in the VLAN interface link-up calculation.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Enter the **switchport autostate exclude** command on a Layer 2 access or trunk port belonging to an SVI.

A VLAN interface (SVI) is up if ports are forwarding traffic in the associated VLAN. When all ports on a VLAN are down or blocking, the SVI is down. For the SVI to be up, at least one port in the VLAN must be up and forwarding. You can use the **switchport autostate exclude** command to exclude a port from the SVI interface line-state up-or-down calculation. For example, you might exclude a monitoring port from the calculations so that the VLAN is not considered up when only the monitoring port is active.

When you enter the **switchport autostate exclude** command on a port, the command applies to all VLANs that are enabled on the port.

You can verify the autostate mode of an interface by entering the **show interface** *interface-id* **switchport** privileged EXEC command. If the mode has not been set, the autostate mode does not appear.

Examples

This example shows how to configure autostate exclude on an interface and to verify the configuration:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport autostate exclude
Switch(config-if)# end
Switch# show interface gigabitethernet0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
```

```
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Autostate mode exclude
```

Related Commands

Command	Description
show interfaces [*interface-id*] **switchport**	Displays the administrative and operational status of a switching (nonrouting) port, including autostate mode, if set.
show running-config	Displays the current operating configuration.

switchport host

Use the **switchport host** interface configuration command to optimize a Layer 2 port for a host connection. The **no** form of this command has no affect on the system.

switchport host

Syntax Description

This command has no arguments or keywords.

Defaults

The default is for the port to not be optimized for a host connection.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

To optimize the port for a host connection, the **switchport host** command sets switch port mode to access, enables spanning tree Port Fast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning tree Port Fast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other switches, hubs, concentrators, or bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

Examples

This example shows how to optimize the port configuration for a host connection:

```
Switch(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Switch(config-if)#
```

You can verify your setting by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including switchport mode.

switchport mode

Use the **switchport mode** interface configuration command to configure the VLAN membership mode of a port. Use the **no** form of this command to reset the mode to the appropriate default for the device.

switchport mode {**access** | **dynamic** {**auto** | **desirable**} | **trunk**}

no switchport mode {**access** | **dynamic** | **trunk**}

Syntax Description

access	Set the port to access mode (either static-access or dynamic-access depending on the setting of the **switchport access vlan** interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN.
dynamic auto	Set the interface trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link. This is the default switchport mode.
dynamic desirable	Set the interface trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
trunk	Set the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.

Defaults

The default mode is **dynamic auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

A configuration that uses the **access** or **trunk** keywords takes effect only when you configure the port in the appropriate mode by using the **switchport mode** command. The static-access and trunk configuration are saved, but only one configuration is active at a time.

When you enter **access** mode, the interface changes to permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

When you enter **trunk** mode, the interface changes to permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change.

When you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

When you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

To autonegotiate trunking, the interfaces must be in the same VLAN Trunking Protocol (VTP) domain. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations. To avoid this, you should configure interfaces connected to devices that do not support DTP to not forward DTP frames, which turns off DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Access ports and trunk ports-are mutually exclusive.

Examples

This example shows how to configure a port for access mode:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
```

This example shows how set the port to dynamic desirable mode:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode dynamic desirable
```

This example shows how to configure a port for trunk mode:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode trunk
```

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport access	Configures a port as a static-access or dynamic-access port.
switchport trunk	Configures the trunk characteristics when an interface is in trunking mode.

switchport nonegotiate

Use the **switchport nonegotiate** interface configuration command to specify that Dynamic Trunking Protocol (DTP) negotiation packets are not sent on the Layer 2 interface. The switch does not engage in DTP negotiation on this interface. Use the **no** form of this command to return to the default setting.

switchport nonegotiate

no switchport nonegotiate

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to use DTP negotiation to learn the trunking status.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **no** form of the **switchport nonegotiate** command removes **nonegotiate** status.

This command is valid only when the interface switchport mode is access or trunk (configured by using the **switchport mode access** or the **switchport mode trunk** interface configuration command). This command returns an error if you attempt to execute it in **dynamic** (**auto** or **desirable**) mode.

Internetworking devices that do not support DTP might forward DTP frames improperly and cause misconfigurations. To avoid this, you should turn off DTP by using the **switchport no negotiate** command to configure the interfaces connected to devices that do not support DTP to not forward DTP frames.

When you enter the **switchport nonegotiate** command, DTP negotiation packets are not sent on the interface. The device does or does not trunk according to the **mode** parameter: **access** or **trunk**.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking on a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Examples

This example shows how to cause a port to refrain from negotiating trunking mode and to act as a trunk or access port (depending on the mode set):

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport nonegotiate
```

You can verify your setting by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

switchport trunk

Use the **switchport trunk** interface configuration command to set the trunk characteristics when the interface is in trunking mode. Use the **no** form of this command to reset a trunking characteristic to the default.

switchport trunk {**allowed vlan** *vlan-list* |**native vlan** *vlan-id* | **pruning vlan** *vlan-list*}

no switchport trunk {**allowed vlan** | **native vlan** | **pruning vlan**}

Syntax Description

allowed vlan *vlan-list*	Set the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the following *vlan-list* format. The **none** keyword is not valid. The default is **all**.
native vlan *vlan-id*	Set the native VLAN for sending and receiving untagged traffic when the interface is in IEEE 802.1Q trunking mode. The range is 1 to 4094.
pruning vlan *vlan-list*	Set the list of VLANs that are eligible for VTP pruning when in trunking mode. The **all** keyword is not valid.

The *vlan-list* format is **all** | **none** | [**add** | **remove** | **except**] *vlan-atom* [,*vlan-atom*...] where:

- **all** specifies all VLANs from 1 to 4094. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** means an empty list. This keyword is not allowed on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLANs (VLAN IDs greater than 1005) are valid in some cases.

  Note You can add extended-range VLANs to the allowed VLAN list, but not to the pruning-eligible VLAN list.

  Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLAN IDs are valid in some cases.

  Note You can remove extended-range VLANs from the allowed VLAN list, but you cannot remove them from the pruning-eligible list.

  Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.) Valid IDs are from 1 to 1005. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- *vlan-atom* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

Defaults

The default encapsulation is negotiate.

VLAN 1 is the default native VLAN ID on the port.

The default for all VLAN lists is to include all VLANs.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Native VLANs:

- All untagged traffic received on an IEEE 802.1Q trunk port is forwarded with the native VLAN configured for the port.
- If a packet has a VLAN ID that is the same as the sending-port native VLAN ID, the packet is sent without a tag; otherwise, the switch sends the packet with a tag.
- The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

Allowed VLAN:

- To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), Dynamic Trunking Protocol (DTP), and VLAN Trunking Protocol (VTP) in VLAN 1.
- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

Trunk pruning:

- The pruning-eligible list applies only to trunk ports.
- Each trunk port has its own eligibility list.
- If you do not want a VLAN to be pruned, remove it from the pruning-eligible list. VLANs that are pruning-ineligible receive flooded traffic.
- VLAN 1, VLANs 1002 to 1005, and extended-range VLANs (VLANs 1006 to 4094) cannot be pruned.

Examples

This example shows how to configure VLAN 3 as the default for the port to send all untagged traffic:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk native vlan 3
```

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

This example shows how to remove VLANs 3 and 10 to 15 from the pruning-eligible list:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

system env temperature threshold yellow

Use the **system env temperature threshold yellow** global configuration command to configure the difference between the yellow and red temperature thresholds that determines the value of yellow threshold. Use the **no** form of this command to return to the default value.

system env temperature threshold yellow *value*

no system env temperature threshold yellow *value*

Syntax Description

value	Specify the difference between the yellow and red threshold values (in Celsius). The range is 10 to 25. The default value is 10.

Defaults

Difference between Yellow and Red threshold values:

Red threshold value:

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You cannot configure the green and red thresholds but can configure the yellow threshold.

Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red thresholds and to configure the yellow threshold. For example, if the red threshold is 66 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 15** command.

Note The internal temperature sensor in the switch measures the internal system temperature and might vary ±5 degrees C.

Examples

This example sets 15 as the difference between the yellow and red thresholds:

```
Switch(config)# system env temperature threshold yellow 15
Switch(config)#
```

Related Commands

Command	Description
show env temperature status	Displays the temperature status and threshold levels.

system mtu

Use the **system mtu** global configuration command to set the maximum packet size or maximum transmission unit (MTU) size for Gigabit Ethernet (10/100/1000) ports, or for 10-Gigabit ports, or for routed ports. Use the **no** form of this command to restore the global MTU value to its default value

system mtu {*bytes* | **jumbo** *bytes*}

no system mtu [**jumbo**]

Syntax Description

bytes	Change the MTU size for all Fast Ethernet interfaces.
jumbo *bytes*	Set the system MTU for Gigabit Ethernet ports and 10-Gigabit Ethernet ports. The system jumbo MTU is the maximum MTU received at the Gigabit Ethernet and 10-Gigabit Ethernet ports. The range is from 1500 to 9198 bytes.

Defaults

The default MTU size for all ports is 1500 bytes.

The default value for the system routing MTU is the system MTU value.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The switch does not support the MTU on a per-interface basis.

If you enter the **system mtu** *bytes* global configuration command or the **system mtu routing** command on the switch, the commands have no effect.

When you use the **system mtu jumbo** *bytes* command to change the system jumbo MTU size, you must reset the switch before the new configuration takes effect.

The system MTU setting is saved in the switch environmental variable in NVRAM and becomes effective when the switch reloads. The MTU settings that you enter with the **system mtu jumbo** command are not saved in the switch Cisco IOS configuration file, even if you enter the **copy running-config startup-config** privileged EXEC command. Therefore, if you use TFTP to configure a new switch by using a backup configuration file and want the system MTU to be other than the default, you must explicitly configure the **system mtu jumbo** settings on the new switch and then reload the switch.

Examples

This example shows how to set the maximum jumbo packet size for Gigabit Ethernet ports to 6000 bytes:

```
Switch(config)# system mtu jumbo 6000
Switch(config)# exit
Switch# reload
```

You can verify your setting by entering the **show system mtu** privileged EXEC command.

Related Commands

Command	Description
show system mtu	Displays the packet size set for Gigabit Ethernet and 10-Gigabit Ethernet ports.

traceroute mac

Use the **traceroute mac** privileged EXEC command to display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

traceroute mac [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

Syntax Description

interface *interface-id*	(Optional) Specify an interface on the source or destination switch.
source-mac-address	Specify the MAC address of the source switch in hexadecimal format.
destination-mac-address	Specify the MAC address of the destination switch in hexadecimal format.
vlan *vlan-id*	(Optional) Specify the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch. Valid VLAN IDs are 1 to 4094.
detail	(Optional) Specify that detailed information appears.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2360-48TD-SD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201 detail

Source 0000.0201.0601 found on con6[WS-C2360-48TD-SD] (2.2.6.6)
con6 / WS-C2360-48TD-SD / 2.2.6.6 :
        Gi0/2 [auto, auto] => Gi0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2360-48TD-SD] (2.2.6.6)
con6 (2.2.6.6) :Gi00/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi00/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows the Layer 2 path when the switch is not connected to the source switch:

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[WS-C2360-48TD-SD] (2.2.5.5)
con5 / WS-C2360-48TD-SD / 2.2.5.5 :
        Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows the Layer 2 path when the switch cannot find the destination port for the source MAC address:

```
Switch# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

This example shows the Layer 2 path when source and destination switches belong to multiple VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

Related Commands

Command	Description
traceroute mac ip	Displays the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

traceroute mac ip

Use the **traceroute mac ip** privileged EXEC command to display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

traceroute mac ip {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

Syntax Description

source-ip-address	Specify the IP address of the source switch as a 32-bit quantity in dotted-decimal format.
destination-ip-address	Specify the IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
source-hostname	Specify the IP hostname of the source switch.
destination-hostname	Specify the IP hostname of the destination switch.
detail	(Optional) Specify that detailed information appears.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects an device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C3750E-24TD / 2.2.6.6 :
        Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Switch# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

Related Commands

Command	Description
traceroute mac	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

udld

Use the **udld** global configuration command to enable aggressive or normal mode in the UniDirectional Link Detection (UDLD) and to set the configurable message timer time. Use the **no** form of the command to disable aggressive or normal mode UDLD on all fiber-optic ports.

udld {**aggressive** | **enable** | **message time** *message-timer-interval*}

no udld {**aggressive** | **enable** | **message**}

Syntax Description

aggressive	Enable UDLD in aggressive mode on all fiber-optic interfaces.
enable	Enable UDLD in normal mode on all fiber-optic interfaces.
message time *message-timer-interval*	Configure the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is 1 to 90 seconds.

Defaults

UDLD is disabled on all interfaces.

The message timer is set at 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the “Understanding UDLD” section in the software configuration guide for this release.

If you change the message time between probe packets, you are making a trade-off between the detection speed and the CPU load. By decreasing the time, you can make the detection-response faster but increase the load on the CPU.

This command affects fiber-optic interfaces only. Use the **udld** interface configuration command to enable UDLD on other interface types.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD
- The **shutdown** and **no shutdown** interface configuration commands
- The **no udld enable** global configuration command followed by the **udld** {**aggressive** | **enable**} global configuration command to re-enable UDLD globally

- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to re-enable UDLD on the specified interface
- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands to automatically recover from the UDLD error-disabled state

Examples

This example shows how to enable UDLD on all fiber-optic interfaces:

```
Switch(config)# udld enable
```

You can verify your setting by entering the **show udld** privileged EXEC **command**.

Related Commands

Command	Description
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

udld port

Use the **udld port** interface configuration command to enable the UniDirectional Link Detection (UDLD) on an individual interface or prevent a fiber-optic interface from being enabled by the **udld** global configuration command. Use the **no** form of this command to return to the **udld** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port.

udld port [**aggressive**]

no udld port [**aggressive**]

Syntax Description

aggressive	Enable UDLD in aggressive mode on the specified interface.

Defaults

On fiber-optic interfaces, UDLD is not enabled, not in aggressive mode, and not disabled. For this reason, fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the “Configuring UDLD” chapter in the software configuration guide for this release.

To enable UDLD in normal mode, use the **udld port** interface configuration command. To enable UDLD in aggressive mode, use the **udld port aggressive** interface configuration command.

Use the **no udld port** command on fiber-optic ports to return control of UDLD to the **udld enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **udld port aggressive** command on fiber-optic ports to override the setting of the **udld enable** or **udld aggressive** global configuration command. Use the **no** form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the **udld** global configuration command or to disable UDLD on nonfiber-optic ports.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD
- The **shutdown** and **no shutdown** interface configuration commands
- The **no udld enable** global configuration command followed by the **udld** {**aggressive** | **enable**} global configuration command to re-enable UDLD globally
- The **no udld port** interface configuration command followed by the **udld port or udld port aggressive** interface configuration command to re-enable UDLD on the specified interface
- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands to automatically recover from the UDLD error-disabled state

Examples

This example shows how to enable UDLD on an port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# udld port
```

This example shows how to disable UDLD on a fiber-optic interface despite the setting of the **udld** global configuration command:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no udld port
```

You can verify your settings by entering the **show running-config** or the **show udld** *interface* privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

udld reset

Use the **udld reset** privileged EXEC command to reset all interfaces disabled by the UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again (though other features, such as spanning tree, Port Aggregation Protocol (PAgP), and Dynamic Trunking Protocol (DTP) still have their normal effects, if enabled).

udld reset

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected.

Examples

This example shows how to reset all interfaces disabled by UDLD:

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

You can verify your setting by entering the **show udld** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the operating configuration.
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.

usb-inactivity-timeout

To configure an inactivity timeout on the USB console, use the **usb-inactivity-timeout** command in console line configuration mode. To remove the inactivity timeout use the **no** form of this command.

usb-inactivity-timeout *minutes*

no usb-inactivity-timeout *minutes*

Syntax Description

minutes	Time, in minutes, before the console port changes to the RJ-45 port due to inactivity on the USB console. The range is 1 to 240. The default is no timeout.

Defaults

Inactivity timeout is not configured.

Command Modes

Line configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The switch has a configurable timeout inactivity that activates the RJ-45 console if the USB console has been activated but no input activity has occurred on the USB console for a specified time period. When the USB console is deactivated due to an inactivity timeout, you can restore its operation by disconnecting and reconnecting the USB cable.

Examples

This example shows how to configure the inactivity timeout:

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# usb-inactivity-timeout 60
```

If there is no input on the USB console for 60 minutes, the console changes to RJ-45, and a system message log appears showing the inactivity timeout.

Related Commands

Command	Description
no media-type rj45	Resets the console port as the USB port if it has been manually set to the RJ-45 port.

vlan (global configuration)

Use the **vlan** global configuration command to add a VLAN and to enter the config-vlan mode. Use the **no** form of this command to delete the VLAN. Configuration information for normal-range VLANs (VLAN IDs 1 to 1005) is always saved in the VLAN database. When VLAN Trunking Protocol (VTP) mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005), and the VTP mode, domain name, and the VLAN configuration are saved in the switch running configuration file. You can save configurations in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command.

vlan *vlan-id*

no vlan vlan-*id*

Syntax Description

vlan-id	ID of the VLAN to be added and configured. For *vlan-id*, the range is 1 to 4094. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You must use the **vlan** *vlan-id* global configuration command to add extended-range VLANs (VLAN IDs 1006 to 4094). Before configuring VLANs in the extended range, you must use the **vtp transparent** global configuration or VLAN configuration command to put the switch in VTP transparent mode. Extended-range VLANs are not learned by VTP and are not added to the VLAN database, but when VTP mode is transparent, VTP mode and domain name and all VLAN configurations are saved in the running configuration, and you can save them in the switch startup configuration file.

When you save the VLAN and VTP configurations in the startup configuration file and reboot the switch, the configuration is selected in these ways:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode is server, or if the startup VTP mode or domain names do not match the VLAN database, the VTP mode and the VLAN configuration for the first 1005 VLANs use the VLAN database information.

If you try to create an extended-range VLAN when the switch is not in VTP transparent mode, the VLAN is rejected, and you receive an error message.

If you enter an invalid VLAN ID, you receive an error message and do not enter config-vlan mode.

Entering the **vlan** command with a VLAN ID enables config-vlan mode. When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit the config-vlan mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.

These configuration commands are available in config-vlan mode. The **no** form of each command returns the characteristic to its default state.

Note Although all commands are visible, the only VLAN configuration commands that are supported on extended-range VLANs are **mtu** *mtu-size*, **private-vlan**, and **remote-span**. For extended-range VLANs, all other characteristics must remain at the default state.

- **are** *are-number*: defines the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs.The range is 0 to 13. The default is 7. If no value is entered, 0 is assumed to be the maximum.
- **backupcrf**: specifies the backup CRF mode. This keyword applies only to TrCRF VLANs.
  - **enable** backup CRF mode for this VLAN.
  - **disable** backup CRF mode for this VLAN (the default).
- **bridge** {*bridge-number*| **type**}: specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings having this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs. The **type** keyword applies only to TrCRF VLANs and is one of these:
  - **srb** (source-route bridging)
  - **srt** (source-route transparent) bridging VLAN
- **exit**: applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits config-vlan mode.
- **media**: defines the VLAN media type. See Table 2-16 for valid commands and syntax for different media types.

  Note The switch supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other switches. These VLANs are locally suspended.

  - **ethernet** is Ethernet media type (the default).
  - **fddi** is FDDI media type.
  - **fd-net** is FDDI network entity title (NET) media type.
  - **tokenring** is Token Ring media type if the VTP v2 mode is disabled, or TrCRF if the VTP Version 2 (v) mode is enabled.
  - **tr-net** is Token Ring network entity title (NET) media type if the VTP v2 mode is disabled or TrBRF media type if the VTP v2 mode is enabled.
- **mtu** *mtu-size*: specifies the maximum transmission unit (MTU) (packet size in bytes). The range is 1500 to 18190. The default is 1500 bytes.

- **name** *vlan-name*: names the VLAN with an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The default is *VLANxxxx* where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.
- **no**: negates a command or returns it to the default setting.
- **parent** *parent-vlan-id*: specifies the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF. The range is 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For both Token Ring and TrCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TrBRF VLAN.
- **remote-span**: configure the VLAN as a Remote SPAN (RSPAN) VLAN. When the RSPAN feature is added to an existing VLAN, the VLAN is first deleted and is then recreated with the RSPAN feature. Any access ports are deactivated until the RSPAN feature is removed. If VTP is enabled, the new RSPAN VLAN is propagated by VTP for VLAN-IDs that are lower than 1024. Learning is disabled on the VLAN. .
- **ring** *ring-number*: defines the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095. The default for Token Ring VLANs is 0. For FDDI VLANs, there is no default.
- **said** *said-value*: specifies the security association identifier (SAID) as documented in IEEE 802.10. The range is 1 to 4294967294, and the number must be unique within the administrative domain. The default value is 100000 plus the VLAN ID number.
- **shutdown**: shuts down VLAN switching on the VLAN. This command takes effect immediately. Other commands take effect when you exit config-vlan mode.
- **state**: specifies the VLAN state:
  - **active** means the VLAN is operational (the default).
  - **suspend** means the VLAN is suspended. Suspended VLANs do not pass packets.
- **ste** *ste-number*: defines the maximum number of spanning-tree explorer (STE) hops. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7.
- **stp type**: defines the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLANs. For FDDI-NET VLANs, the default STP type is **ieee**. For Token Ring-NET VLANs, the default STP type is **ibm**. For FDDI and Token Ring VLANs, the default is no type specified.
  - **ieee** for IEEE Ethernet STP running source-route transparent (SRT) bridging.
  - **ibm** for IBM STP running source-route bridging (SRB).
  - **auto** for STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).
- **tb-vlan1** *tb-vlan1-id* and **tb-vlan2** *tb-vlan2-id*: specifies the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. The range is 0 to 1005. If no value is specified, 0 (no transitional bridging) is assumed.

Table 2-16 Valid Commands and Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	**name** *vlan-name*, **media ethernet, state** {**suspend** | **active**}, **said** *said-value*, **mtu** *mtu-size*, **remote-span**, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
FDDI	**name** *vlan-name*, **media fddi, state** {**suspend** | **active**}, **said** *said-value*, **mtu** *mtu-size*, **ring** *ring-number*, **parent** *parent-vlan-id*, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*

Table 2-16 Valid Commands and Syntax for Different Media Types (continued)

Media Type	Valid Syntax
FDDI-NET	**name** *vlan-name*, **media fd-net, state** {**suspend** | **active**}, **said** *said-value*, **mtu** *mtu-size*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm** | **auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id* If VTP v2 mode is disabled, do not set the **stp type** to **auto**.
Token Ring	VTP v1 mode is enabled. **name** *vlan-name*, **media tokenring, state** {**suspend** | **active**}, **said** *said-value*, **mtu** *mtu-size*, **ring** *ring-number*, **parent** *parent-vlan-id*, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. **name** *vlan-name*, **media tokenring, state** {**suspend** | **active**}, **said** *said-value*, **mtu** *mtu-size*, **ring** *ring-number*, **parent** *parent-vlan-id*, **bridge type** {**srb** | **srt**}, **are** *are-number*, **ste** *ste-number*, **backupcrf** {**enable** | **disable**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
Token Ring-NET	VTP v1 mode is enabled. **name** *vlan-name*, **media tr-net, state** {**suspend** | **active**}, **said** *said-value*, **mtu** *mtu-size*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. **name** *vlan-name*, **media tr-net, state** {**suspend** | **active**}, **said** *said-value*, **mtu** *mtu-size*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm** | **auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*

Table 2-17 describes the rules for configuring VLANs.

Table 2-17 VLAN Configuration Rules

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.	Specify a parent VLAN ID of a TrBRF that already exists in the database. Specify a ring number. Do not leave this field blank. Specify unique ring numbers when TrCRF VLANs have the same parent VLAN ID. Only one backup concentrator relay function (CRF) can be enabled.
VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.	Do not specify a backup CRF.
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.

Table 2-17 VLAN Configuration Rules (continued)

Configuration	Rule
VTP v1 mode is enabled.	No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

Examples

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of *VLANxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default **media** option is **ethernet**; the **state** option is **active**. The default *said-value* variable is 100000 plus the VLAN ID; the *mtu-size* variable is 1500; the **stp-type** option is **ieee**. When you enter the **exit** config-vlan configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

This example shows how to create a new VLAN with all default characteristics and enter config-vlan mode:

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
Switch(config)#
```

This example shows how to create a new extended-range VLAN with all the default characteristics, to enter config-vlan mode, and to save the new VLAN in the switch startup configuration file:

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

You can verify your setting by entering the **show vlan** privileged EXEC command.

Related Commands

Command	Description
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.

vtp (global configuration)

Use the **vtp** global configuration command to set or modify the VLAN Trunking Protocol (VTP) configuration characteristics. Use the **no** form of this command to remove the settings or to return to the default settings.

vtp {**domain** *domain-name* | **file** *filename* | **interface** *name* [**only**] | **mode** {**client** | **server** | **transparent**} | **password** *password* | **pruning** | **version** *number*}

no vtp {**file** | **interface** | **mode** | **password** | **pruning** | **version**}

Syntax Description

domain *domain-name*	Specify the VTP domain name, an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
file *filename*	Specify the Cisco IOS file system file where the VTP VLAN configuration is stored.
interface *name*	Specify the name of the interface providing the VTP ID updated for this device.
only	(Optional) Use only the IP address of this interface as the VTP IP updater.
mode	Specify the VTP device mode as client, server, or transparent.
client	Place the switch in VTP client mode. A switch in VTP client mode is enabled for VTP, and can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on the switch. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
server	Place the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the switch. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	Place the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. When VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save them in the switch startup configuration file by entering the **copy running-config startup config** privileged EXEC command.
password *password*	Set the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
pruning	Enable VTP pruning on the switch.
version *number*	Set VTP version to Version 1 or Version 2.

Defaults

The default filename is *flash:vlan.dat*.

The default mode is server mode.

No domain name or password is defined.

No password is configured.

Pruning is disabled.

The default version is Version 1.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When you save VTP mode, domain name, and VLAN configurations in the switch startup configuration file and reboot the switch, the VTP and VLAN configurations are selected by these conditions:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the startup VTP mode is server mode, or the startup VTP mode or domain names do not match the VLAN database, VTP mode and VLAN configuration for the first 1005 VLANs are selected by VLAN database information, and VLANs greater than 1005 are configured from the switch configuration file.

The **vtp file** *filename* cannot be used to load a new database; it renames only the file in which the existing database is stored.

Follow these guidelines when configuring a VTP domain name:

- The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after it receives the first VTP summary packet on any port that is trunking or after you configure a domain name by using the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to 0. After the switch leaves the no-management-domain state, it can no be configured to re-enter it until you clear the NVRAM and reload the software.
- Domain names are case-sensitive.
- After you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

Follow these guidelines when setting VTP mode:

- The **no vtp mode** command returns the switch to VTP server mode.
- The **vtp mode server** command is the same as **no vtp mode** except that it does not return an error if the switch is not in client or transparent mode.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, be sure to make all VTP or VLAN configuration changes on a switch in server mode. If the receiving switch is in server mode or transparent mode, the switch 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 other switches in the network.
- If you change the VTP or VLAN configuration on a switch that is in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the switch.
- The VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file.
- If extended-range VLANs are configured on the switch and you attempt to set the VTP mode to server or client, you receive an error message, and the configuration is not allowed.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When you use the **no vtp password** form of the command, the switch returns to the no-password state.

Follow these guidelines when setting VTP pruning:

- VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.
- If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.
- Only VLANs in the pruning-eligible list can be pruned.
- Pruning is supported with VTP Version 1 and Version 2.

Follow these guidelines when setting the VTP version:

- Toggling the Version 2 (v2) mode state modifies parameters of certain default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use Version 2, all VTP switches in the network must support Version 2; otherwise, you must configure them to operate in VTP Version 1 mode.
- If all switches in a domain are VTP Version 2-capable, you need only to configure Version 2 on one switch; the version number is then propagated to the other Version-2 capable switches in the VTP domain.
- If you are using VTP in a Token Ring environment, VTP Version 2 must be enabled.

- If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use Version 2.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use Version 1.

You cannot save password, pruning, and version configurations in the switch configuration file.

Examples

This example shows how to rename the filename for VTP configuration storage to *vtpfilename*:

```
Switch(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Switch(config)# no vtp file vtpconfig
Clearing device storage filename.
```

This example shows how to specify the name of the interface providing the VTP updater ID for this device:

```
Switch(config)# vtp interface gigabitethernet
```

This example shows how to set the administrative domain for the switch:

```
Switch(config)# vtp domain OurDomainName
```

This example shows how to place the switch in VTP transparent mode:

```
Switch(config)# vtp mode transparent
```

This example shows how to configure the VTP domain password:

```
Switch(config)# vtp password ThisIsOurDomain'sPassword
```

This example shows how to enable pruning in the VLAN database:

```
Switch(config)# vtp pruning
Pruning switched ON
```

This example shows how to enable Version 2 mode in the VLAN database:

```
Switch(config)# vtp version 2
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

Related Commands

Command	Description
show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
vtp (VLAN configuration)	Configures VTP domain-name, password, pruning, version, and mode.

vtp (VLAN configuration)

Use the **vtp** VLAN configuration command to configure VLAN Trunking Protocol (VTP) characteristics. You access VLAN configuration mode by entering the vlan database privileged EXEC command. Use the **no** form of this command to return to the default settings, disable the characteristic, or remove the password.

vtp {**domain** *domain-name* | **password** *password* | **pruning** | **v2-mode** | {**server** | **client** | **transparent**}}

no vtp {**client** | **password** | **pruning** | **transparent** | **v2-mode**}

Syntax Description

domain *domain-name*	Set the VTP domain name by entering an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
password *password*	Set the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
pruning	Enable pruning in the VTP administrative 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.
v2-mode	Enable VLAN Trunking Protocol (VTP) Version 2 in the administrative domains.
client	Place the switch in VTP client mode. A switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
server	Place the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	Place the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.

Defaults

The default mode is server mode.

No domain name is defined.

No password is configured.

Pruning is disabled.

VTP Version 2 (v2 mode) is disabled.

Command Modes VLAN configuration

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines If the VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save the configuration in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Follow these guidelines when setting the VTP mode:

- The **no vtp client** and **no vtp transparent** forms of the command return the switch to VTP server mode.
- The **vtp server** command is the same as **no vtp client** or **no vtp transparent** except that it does not return an error if the switch is not in client or transparent mode.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, make sure to make all VTP or VLAN configuration changes on a switch in server mode. If the receiving switch is in server mode or transparent mode, the switch 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 other switches in the network.
- If you make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp transparent** command disables VTP from the domain but does not remove the domain from the switch.
- The VTP mode must be transparent for you to add extended-range VLANs or for the VTP and the VLAN configurations to be saved in the running configuration file.
- If extended-range VLANs are configured on the switch and you attempt to set the VTP mode to server or client, you receive an error message and the configuration is not allowed.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

Note VTP configuration in VLAN configuration mode is saved in the VLAN database when applied.

Follow these guidelines when configuring a VTP domain name:

- The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after receiving the first VTP summary packet on any port that is currently trunking or after configuring a domain name with the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to zero. After the switch leaves the no-management-domain state, it can never be configured to reenter it until you clear the NVRAM and reload the software.
- Domain names are case sensitive.
- After you configure a domain name, it cannot be removed. You can reassign it only to a different domain.

Follow these guidelines when configuring a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When the **no vtp password** form of the command is used, the switch returns to the no-password state.

Follow these guidelines when enabling VTP pruning:

- If you enable pruning on the VTP server, it is enabled for the entire management domain.
- Only VLANs included in the pruning-eligible list can be pruned.
- Pruning is supported with VTP Version 1 and Version 2.

Follow these guidelines when enabling VTP Version 2 (v2-mode):

- Toggling the version (v2-mode) state modifies certain parameters of certain default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use VTP Version 2, all VTP switches in the network must support Version 2; otherwise, you must configure them to operate in VTP Version 1 (**no vtp v2-mode**).
- If all switches in a domain are VTP Version 2-capable, you need only to enable VTP Version 2 on one switch; the version number is then propagated to the other Version-2 capable switches in the VTP domain.
- If you are using VTP in a Token Ring environment or configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, VTP Version 2 (**v2-mode**) must be enabled.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use VTP Version 1.

Examples

This example shows how to place the switch in VTP transparent mode:

```
Switch(vlan)# vtp transparent
Setting device to VTP TRANSPARENT mode.
```

This example shows how to set the administrative domain for the switch:

```
Switch(vlan)# vtp domain OurDomainName
Changing VTP domain name from cisco to OurDomainName
```

This example shows how to configure the VTP domain password:

```
Switch(vlan)# vtp password private
Setting device VLAN database password to private.
```

This example shows how to enable pruning in the proposed new VLAN database:

```
Switch(vlan)# vtp pruning
Pruning switched ON
```

This example shows how to enable v2 mode in the proposed new VLAN database:

```
Switch(vlan)# vtp v2-mode
V2 mode enabled.
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

Related Commands

Command	Description
show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
switchport trunk pruning	Configures the VLAN pruning-eligible list for ports in trunking mode.
vtp (global configuration)	Configures the VTP filename, interface, domain name, and mode.

APPENDIX A

Catalyst 2360 Switch Boot Loader Commands

This appendix describes the boot loader commands on the Catalyst 2360 switch.

During normal boot loader operation, you are not presented with the boot loader command-line prompt. You gain access to the boot loader command line if the switch is set to manually boot, if an error occurs during power-on self test (POST) DRAM testing, or if an error occurs while loading the operating system (a corrupted Cisco IOS image). You can also access the boot loader if you have lost or forgotten the switch password.

Note The default switch configuration allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process while the switch is powering up and then entering a new password. The password recovery disable feature allows the system administrator to protect access to the switch password by disabling part of this functionality and allowing the user to interrupt the boot process only by agreeing to set the system back to the default configuration. With password recovery disabled, the user can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted. For more information, see the software configuration guide for this release.

You can access the boot loader through a switch console connection at 9600 b/s. Unplug the switch power cord, and press the switch **Mode** button while reconnecting the power cord. You can release the **Mode** button a second or two after the LED above port 1X goes off. You should then see the boot loader *Switch:* prompt. The boot loader performs low-level CPU initialization, performs POST, and loads a default operating system image into memory.

arp

Use the **arp** boot loader command to display the contents the Address Resolution Protocol (ARP) table.

arp [*ip_address*]

Syntax Description

ip_address	(Optional) Show the ARP table or the mapping for a specific IP address.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The ARP table has the IP-address-to-MAC-address mappings.

Examples

This example shows how to display the ARP table:

```
switch: arp 172.20.136.8
arp'ing 172.20.136.8...
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

boot

Use the **boot** boot loader command to load and boot an executable image and to enter the command-line interface.

boot [**-post** | **-n** | **-p** | *flag*] *filesystem:/file-url ...*

Syntax Description

-post	(Optional) Run the loaded image with an extended or comprehensive power-on self-test (POST). Using this keyword causes POST to take longer to complete.
-n	(Optional) Pause for the Cisco IOS debugger immediately after starting.
-p	(Optional) Pause for the JTAG debugger right after loading the image.
*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	(Optional) Path (directory) and name of a bootable image. Separate image names with a semicolon.

Defaults

The switch attempts to automatically boot the system by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

When you enter the **boot** command without any arguments, the switch attempts to automatically boot the system by using the information in the BOOT environment variable, if any. If you supply an image name for the *file-url* variable, the **boot** command attempts to boot the specified image.

When you set boot loader **boot** command options, they are executed immediately and apply only to the current boot loader session. These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

Examples

This example shows how to boot the switch using the *new-image.bin* image:

```
switch: boot flash:/new-images/new-image.bin
```

After entering this command, you are prompted to start the setup program.

Related Commands

Command	Description
set	Sets the BOOT environment variable to boot a specific image when the **BOOT** keyword is appended to the command.

cat

Use the **cat** boot loader command to display the contents of one or more files.

cat *filesystem*:*/file-url* ...

Syntax Description

filesystem:	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	Path (directory) and name of the files to display. Separate each filename with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of a file:

```
switch: cat flash:c2360-universalk9-mz/info
version_suffix: universalk9-mz
version_directory: c2360-universalk9-mz
image_system_type_id: 0x00000002
image_name: c2360-universalk9-mz.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: c2360
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

Related Commands

Command	Description
more	Displays the contents of one or more files.
type	Displays the contents of one or more files.

copy

Use the **copy** boot loader command to copy a file from a source to a destination.

copy [**-b** *block-size*] *filesystem***:/***source-file-url filesystem***:/***destination-file-url*

Syntax Description

-b *block-size*	(Optional) This option is used only for internal development and testing.
*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*source-file-url*	Path (directory) and filename (source) to be copied.
/*destination-file-url*	Path (directory) and filename of the destination.

Defaults

The default block size is 4 KB.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

If you are copying a file to a new directory, the directory must already exist.

Examples

This example show how to copy a file at the root:

```
switch: copy flash:test1.text flash:test4.text
.
File "flash:test1.text" successfully copied to "flash:test4.text"
```

You can verify that the file was copied by entering the **dir** *filesystem***:** boot loader command.

Related Commands

Command	Description
delete	Deletes one or more files from the specified file system.

delete

Use the **delete** boot loader command to delete one or more files from the specified file system.

delete *filesystem***:/***file-url* ...

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*file-url*	Path (directory) and filename to delete. Separate each filename with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

The switch prompts you for confirmation before deleting each file.

Examples

This example shows how to delete two files:

```
switch: delete flash:test2.text flash:test5.text
Are you sure you want to delete "flash:test2.text" (y/n)?y
File "flash:test2.text" deleted
Are you sure you want to delete "flash:test5.text" (y/n)?y
File "flash:test2.text" deleted
```

You can verify that the files were deleted by entering the **dir flash:** boot loader command.

Related Commands

Command	Description
copy	Copies a file from a source to a destination.

dir

Use the **dir** boot loader command to display a list of files and directories on the specified file system.

dir *filesystem***:***/file-url* ...

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	(Optional) Path (directory) and directory name whose contents you want to display. Separate each directory name with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Examples

This example shows how to display the files in flash memory:

```
switch: dir flash:
Directory of flash:/
    3  -rwx        1839   Feb 01 2002 00:48:15  config.text
   11  -rwx        1140   Feb 01 2002 04:18:48  vlan.dat
   21  -rwx          26   Feb 01 2002 00:01:39  env_vars
    9  drwx         768   Feb 01 2002 23:11:42  html
   16  -rwx        1037   Feb 01 2002 00:01:11  config.text
   14  -rwx        1099   Feb 01 2002 01:14:05  homepage.htm
   22  -rwx          96   Feb 01 2002 00:01:39  system_env_vars
   17  drwx        192    Feb 06 2002 23:22:03  c2360-universalk9-mz
15998976 bytes total (6397440 bytes free)
```

Table A-1 describes the fields in the display.

Table A-1 dir Field Descriptions

Field	Description
2	Index number of the file.
-rwx	File permission, which can be any or all of the following: • d—directory • r—readable • w—writable • x—executable
1644045	Size of the file.

Table A-1 dir Field Descriptions (continued)

Field	Description
<date>	Last modification date.
env_vars	Filename.

Related Commands

Command	Description
mkdir	Creates one or more directories.
rmdir	Removes one or more directories.

flash_init

Use the **flash_init** boot loader command to initialize the flash file system.

flash_init

Syntax Description

This command has no arguments or keywords.

Defaults

The flash file system is automatically initialized during normal system operation.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

During the normal boot process, the flash file system is automatically initialized.

Use this command to manually initialize the flash file system. For example, you use this command during the recovery procedure for a lost or forgotten password.

format

Use the **format** boot loader command to format the specified file system and destroy all data in that file system.

format *filesystem***:**

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Caution Use this command with care; it destroys all data on the file system and renders your system unusable.

fsck

Use the **fsck** boot loader command to check the file system for consistency.

fsck [**-test** | **-f**] *filesystem***:**

Syntax Description

-test	(Optional) Initialize the file system code and perform extra POST on flash memory. An extensive, nondestructive memory test is performed on every byte that makes up the file system.
-f	(Optional) Initialize the file system code and perform a fast file consistency check. Cyclic redundancy checks (CRCs) in the flashfs sectors are not checked.
*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.

Defaults

No file system check is performed.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

To stop an in-progress file system consistency check, disconnect the switch power and then reconnect the power.

Examples

This example shows how to perform an extensive file system check on flash memory:

```
switch: fsck -test flash:
```

help

Use the **help** boot loader command to display the available commands.

help

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

You can also use the question mark (?) to display a list of available boot loader commands.

memory

Use the **memory** boot loader command to display memory heap utilization information.

memory

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Examples

This example shows how to display memory heap utilization information:

```
switch: memory
Text:   0x00700000 - 0x0071cf24 (0x0001cf24 bytes)
Rotext: 0x00000000 - 0x00000000 (0x00000000 bytes)
Data:   0x0071cf24 - 0x00723a0c (0x00006ae8 bytes)
Bss:    0x0072529c - 0x00746f94 (0x00021cf8 bytes)
Stack:  0x00746f94 - 0x00756f94 (0x00010000 bytes)
Heap:   0x00756f98 - 0x00800000 (0x000a9068 bytes)

Bottom heap utilization is 22 percent.
Top heap utilization is 0 percent.
Total heap utilization is 22 percent.
Total bytes: 0xa9068 (692328)
Bytes used: 0x26888 (157832)
Bytes available: 0x827e0 (534496)

Alternate heap utilization is 0 percent.
Total alternate heap bytes: 0x6fd000 (7327744)
Alternate heap bytes used: 0x0 (0)
Alternate heap bytes available: 0x6fd000 (7327744)
```

Table A-2 describes the fields in the display.

Table A-2 memory Field Descriptions

Field	Description
Text	Beginning and ending address of the text storage area.
Rotext	Beginning and ending address of the read-only text storage area. This part of the data segment is grouped with the Text entry.
Data	Beginning and ending address of the data segment storage area.
Bss	Beginning and ending address of the block started by symbol (Bss) storage area. It is initialized to zero.

Table A-2 memory Field Descriptions (continued)

Field	Description
Stack	Beginning and ending address of the area in memory allocated to the software to store automatic variables, return addresses, and so forth.
Heap	Beginning and ending address of the area in memory that memory is dynamically allocated to and freed from.

mgmt_clr

Use the **mgmt_clr** boot loader command to clear the Ethernet management port statistics.

mgmt_clr

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Examples

This example shows how to clear the Ethernet management port statistics:

```
switch: mgmt_clr
```

mgmt_init

Use the **mgmt_init** boot loader command to initialize the Ethernet management port.

mgmt_init

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Use the **mgmt_init** command only during debugging of the Ethernet management port.

Examples

This example shows how to initialize the Ethernet management port:

```
switch: mgmt_init
```

mgmt_show

Use the **mgmt_show** boot loader command to display the Ethernet management port statistics.

mgmt_show

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Examples

This example shows how to display the Ethernet management port statistics:

```
switch: mgmt_show
Statistics               Received    Transmitted
-------------------------------------------------
good frame bytes      :         60            120
good frames           :          1              2
bad frames            :          0              0
dropped frames        :          0              0
queue overflowed      :          0              0
memory access errors  :          0              0
```

mkdir

Use the **mkdir** boot loader command to create one or more new directories on the specified file system.

mkdir *filesystem***:/***directory-url* ...

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*directory-url*	Name of the directories to create. Separate each directory name with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Examples

This example shows how to make a directory called Saved_Configs:

```
switch: mkdir flash:Saved_Configs
Directory "flash:Saved_Configs" created
```

This example shows how to make two directories:

```
switch: mkdir flash:Saved_Configs1 flash:Test
Directory "flash:Saved_Configs1" created
Directory "flash:Test" created
```

You can verify that the directory was created by entering the **dir** *filesystem***:** boot loader command.

Related Commands

Command	Description
dir	Displays a list of files and directories on the specified file system.
rmdir	Removes one or more directories from the specified file system.

more

Use the **more** boot loader command to display the contents of one or more files.

more *filesystem*:*/file-url* ...

Syntax Description

filesystem:	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	Path (directory) and name of the files to display. Separate each filename with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of a file:

```
switch: more flash:c2360-universalk9-mz/info
version_suffix: lanlite-122-46.EY
version_directory: c2360-universalk9-mz
image_system_type_id: 0x00000002
image_name: c2360-universalk9-mz.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: C230
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

Related Commands

Command	Description
cat	Displays the contents of one or more files.
type	Displays the contents of one or more files.

rename

Use the **rename** boot loader command to rename a file.

rename *filesystem***:/***source-file-url filesystem***:/***destination-file-url*

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*source-file-url*	Original path (directory) and filename.
/*destination-file-url*	New path (directory) and filename.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Examples

This example shows a file named *config.text* being renamed to *config1.text*:

```
switch: rename flash:config.text flash:config1.text
```

You can verify that the file was renamed by entering the **dir** *filesystem***:** boot loader command.

Related Commands

Command	Description
copy	Copies a file from a source to a destination.

reset

Use the **reset** boot loader command to perform a hard reset on the system. A hard reset is similar to power-cycling the switch, clearing the processor, registers, and memory.

reset

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Examples

This example shows how to reset the system:

```
switch: reset
Are you sure you want to reset the system (y/n)?y
System resetting...
```

Related Commands

Command	Description
boot	Loads and boots an executable image and enters the command-line interface.

rmdir

Use the **rmdir** boot loader command to remove one or more empty directories from the specified file system.

rmdir *filesystem***:***/directory-url ...*

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/directory-url	Path (directory) and name of the empty directories to remove. Separate each directory name with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Directory names are case sensitive and limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Before removing a directory, you must first delete all the files in the directory.

The switch prompts you for confirmation before deleting each directory.

Examples

This example shows how to remove a directory:

```
switch: rmdir flash:Test
```

You can verify that the directory was deleted by entering the **dir** *filesystem***:** boot loader command.

Related Commands

Command	Description
dir	Displays a list of files and directories on the specified file system.
mkdir	Creates one or more new directories on the specified file system.

set

Use the **set** boot loader command to set or display environment variables, which can be used to control the boot loader or any other software running on the switch.

set *variable value*

Syntax Description

variable value	Use one of these keywords for *variable and value*:
	MANUAL_BOOT—Decides whether the switch automatically or manually boots.
	Valid values are 1, yes, 0, and no. If it is set to no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.
	BOOT *filesystem***:/***file-url*—A semicolon-separated list of executable files to try to load and execute when automatically booting.
	If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.
	ENABLE_BREAK—Decides whether the automatic boot process can be interrupted by using the Break key on the console.
	Valid values are 1, yes, on, 0, no, and off. If it is set to 1, yes, or on, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system has initialized.
	HELPER *filesystem***:/***file-url*—A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
	PS1 *prompt*—A string that is used as the command-line prompt in boot loader mode.
	CONFIG_FILE flash:/*file-url*—The filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	BAUD *rate*—The rate in bits per second (b/s) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting. The range is from 0 to 4294967295 b/s. Valid values are 50, 75, 110, 150, 300, 600, 1200, 1800, 2000, 2400, 3600, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, and 128000.
	The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.
	HELPER_CONFIG_FILE *filesystem***:/***file-url*—The name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of Cisco IOS that are loaded, including the helper image. This variable is used only for internal development and testing.

Defaults

The environment variables have these default values:

MANUAL_BOOT: No (0)

BOOT: Null string

ENABLE_BREAK: No (Off or 0) (the automatic boot process cannot be interrupted by pressing the Break key on the console).

HELPER: No default value (helper files are not automatically loaded).

PS1: switch:

CONFIG_FILE: config.text

BAUD: 9600 b/s

HELPER_CONFIG_FILE: No default value (no helper configuration file is specified).

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1

Note Environment variables that have values are stored in the flash file system in various files. The format of these files is that each line contains an environment variable name and an equal sign followed by the value of the variable. A variable has no value if it is not listed in this file; it has a value if it is listed in the file even if the value is a null string. A variable that is set to a null string (for example, " ") is a variable with a value. Many environment variables are predefined and have default values.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Environment variables are case sensitive and must be entered as documented.

Environment variables that have values are stored in flash memory outside of the flash file system.

Under normal circumstances, it is not necessary to alter the setting of the environment variables.

The MANUAL_BOOT environment variable can also be set by using the **boot manual** global configuration command.

The BOOT environment variable can also be set by using the **boot system** *filesystem***:/***file-url* global configuration command.

The ENABLE_BREAK environment variable can also be set by using the **boot enable-break** global configuration command.

The HELPER environment variable can also be set by using the **boot helper** *filesystem***:/***file-url* global configuration command.

The CONFIG_FILE environment variable can also be set by using the **boot config-file flash:/***file-url* global configuration command.

The HELPER_CONFIG_FILE environment variable can also be set by using the **boot helper-config-file** *filesystem***:/***file-url* global configuration command.

The boot loader prompt string (PS1) can be up to 120 printable characters except the equal sign (=).

Examples

This example shows how to change the boot loader prompt:

```
switch: set PS1 loader:
loader:
```

You can verify your setting by using the **set** boot loader command.

Related Commands

Command	Description
unset	Resets one or more environment variables to its previous setting.

type

Use the **type** boot loader command to display the contents of one or more files.

type *filesystem***:***/file-url ...*

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	Path (directory) and name of the files to display. Separate each filename with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of a file:

```
switch: type flash:c2360-universalk9-mz/info
version_suffix: lanlite-122-46.EY
version_directory: c2360-universalk9-mz
image_system_type_id: 0x00000002
image_name: c2360-universalk9-mz.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: c2360
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

Related Commands

Command	Description
cat	Displays the contents of one or more files.
more	Displays the contents of one or more files.

unset

Use the **unset** boot loader command to reset one or more environment variables.

unset *variable ...*

Syntax Description

variable	Use one of these keywords for *variable*:
	MANUAL_BOOT—Decides whether the switch automatically or manually boots.
	BOOT—Resets the list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.
	ENABLE_BREAK—Decides whether the automatic boot process can be interrupted by using the Break key on the console after the flash file system has been initialized.
	HELPER—A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
	PS1—A string that is used as the command-line prompt in boot loader mode.
	CONFIG_FILE—Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	BAUD—Resets the rate in bits per second (b/s) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting.
	HELPER_CONFIG_FILE—Resets the name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of Cisco IOS that are loaded, including the helper image. This variable is used only for internal development and testing.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

Under normal circumstances, it is not necessary to alter the setting of the environment variables.

The MANUAL_BOOT environment variable can also be reset by using the **no boot manual** global configuration command.

The BOOT environment variable can also be reset by using the **no boot system** global configuration command.

The ENABLE_BREAK environment variable can also be reset by using the **no boot enable-break** global configuration command.

The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

The CONFIG_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

The HELPER_CONFIG_FILE environment variable can also be reset by using the **no boot helper-config-file** global configuration command.

Examples

This example shows how to reset the prompt string to its previous setting:

```
switch: unset PS1
switch:
```

Related Commands

Command	Description
set	Sets or displays environment variables.

version

Use the **version** boot loader command to display the boot loader version.

version

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Examples

This example shows how to display the boot loader version on a Catalyst 2360 switch:

```
switch: version

c2360 Boot Loader (C2360-HBOOT-M) Version 12.2(53)EY

Compiled Wed 21-Feb-02 14:58 by devgoyal
```

APPENDIX B

Debug Commands

This appendix describes the **debug** privileged EXEC commands that have been created or changed for use with the switch. These commands are helpful in diagnosing and resolving internetworking problems and should be enabled only under the guidance of Cisco technical support staff.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use the **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

debug cluster

Use the **debug cluster** privileged EXEC command to enable debugging of cluster-specific events. Use the **no** form of this command to disable debugging.

debug cluster {**discovery** | **events** | **extended** | **http** | **ip** [**packet**] | **members** | **nat** | **neighbors** | **platform** | **snmp** | **vqpxy**}

no debug cluster {**discovery** | **events** | **extended** | **http** | **ip** [**packet**] | **members** | **nat** | **neighbors** | **platform** | **snmp** | **vqpxy**}

Syntax Description

discovery	Display cluster discovery debug messages.
events	Display cluster event debug messages.
extended	Display extended discovery debug messages.
http	Display Hypertext Transfer Protocol (HTTP) debug messages.
ip [**packet**]	Display IP or transport packet debug messages.
members	Display cluster member debug messages.
nat	Display Network Address Translation (NAT) debug messages.
neighbors	Display cluster neighbor debug messages.
platform	Display platform-specific cluster debug messages.
snmp	Display Simple Network Management Protocol (SNMP) debug messages.
vqpxy	Display VLAN Query Protocol (VQP) proxy debug messages.

Note Though visible in the command-line help, the **hsrp** keyword is not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

This command is available only on the cluster command switch.

The **undebug cluster** command is the same as the **no debug cluster** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show cluster candidates	Displays a list of candidate switches when entered on the command switch.
show cluster members	Displays information about cluster members when executed on the command switch.

debug dtp

Use the **debug dtp** privileged EXEC command to enable debugging of the Dynamic Trunking Protocol (DTP) activity. Use the **no** form of this command to disable debugging.

debug dtp {**aggregation** | **all** | **decision** | **events** | **oserrs** | **packets** | **queue** | **states** | **timers**}

no debug dtp {**aggregation** | **all** | **decision** | **events** | **oserrs** | **packets** | **queue** | **states** | **timers**}

Syntax Description

aggregation	Display DTP user-message aggregation debug messages.
all	Display all DTP debug messages.
decision	Display the DTP decision-table debug messages.
events	Display the DTP event debug messages.
oserrs	Display DTP operating system-related error debug messages.
packets	Display DTP packet-processing debug messages.
queue	Display DTP packet-queueing debug messages.
states	Display DTP state-transition debug messages.
timers	Display DTP timer-event debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug dtp** command is the same as the **no debug dtp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show dtp	Displays DTP information for the switch or for a specified interface.

debug eap

Use the **debug eap** privileged EXEC command to enable debugging of the Extensible Authentication Protocol (EAP) activity. Use the **no** form of this command to disable debugging.

debug dot1x {**all** | **authenticator** | **errors** | **events** | **md5** | **packets** | **peer** | **sm**}

no debug dot1x {**all** | **authenticator** | **errors** | **events** | **md5** | **packets** | **peer** | **sm**}

Syntax Description

all	Display all EAP debug messages.
authenticator	Display authenticator debug messages.
errors	Display EAP error debug messages.
events	Display EAP event debug messages.
md5	Display EAP-MD5 debug messages.
packets	Display EAP packet debug messages.
peer	Display EAP peer debug messages.
sm	Display EAP state-machine related-events debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug dot1x** command is the same as the **no debug dot1x** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show eap	Displays EAP registration and session information for the switch or for the specified port.

debug etherchannel

Use the **debug etherchannel** privileged EXEC command to enable debugging of the EtherChannel/PAgP shim. This shim is the software module that is the interface between the Port Aggregation Protocol (PAgP) software module and the port manager software module. Use the **no** form of this command to disable debugging.

debug etherchannel [**all** | **detail** | **error** | **event** | **idb**]

no debug etherchannel [**all** | **detail** | **error** | **event** | **idb**]

Syntax Description

all	(Optional) Display all EtherChannel debug messages.
detail	(Optional) Display detailed EtherChannel debug messages.
error	(Optional) Display EtherChannel error debug messages.
event	(Optional) Debug major EtherChannel event messages.
idb	(Optional) Display PAgP interface descriptor block debug messages.

Note Though visible in the command-line help strings, the **linecard** keyword is not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If you do not specify a keyword, all debug messages appear.

The **undebug etherchannel** command is the same as the **no debug etherchannel** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show etherchannel	Displays EtherChannel information for the channel.

debug fastethernet

Use the **debug fastethernet** privileged EXEC command to enable debugging of the Ethernet management port. Use the **no** form of this command to disable debugging.

debug fastethernet {**af** | **events** | **packets**}

no debug fastethernet {**af** | **events** | **packets**}

Syntax Description

af	Display Ethernet management port software-address-filter debug messages.
events	Display Ethernet management port event debug messages.
packets	Display Ethernet management port packet debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug fastethernet** {**af** | **events** | **packets**} command is the same as the **no debug fastethernet** {**af** | **events** | **packets**} command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show controllers ethernet-controller fastethernet	Displays information about the Ethernet management port.

debug interface

Use the **debug interface** privileged EXEC command to enable debugging of interface-related activities. Use the **no** form of this command to disable debugging.

debug interface {*interface-id* | **null** *interface-number* | **port-channel** *port-channel-number* | **vlan** *vlan-id*}

no debug interface {*interface-id* | **null** *interface-number* | **port-channel** *port-channel-number* | **vlan** *vlan-id*}

Syntax Description

interface-id	Display debug messages for the specified physical port, identified by module number (always 0) and port, for example **gigabitethernet 0/2**.
null *interface-number*	Display debug messages for null interfaces. The *interface-number* is always **0**.
port-channel *port-channel-number*	Display debug messages for the specified EtherChannel port-channel interface. The *port-channel-number* range is 1 to 48.
vlan *vlan-id*	Display debug messages for the specified VLAN. The *vlan-id* range is 1 to 4094.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

If you do not specify a keyword, all debug messages appear.

The **undebug interface** command is the same as the **no debug interface** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show etherchannel	Displays EtherChannel information for the channel.

debug ip igmp filter

Use the **debug ip igmp filter** privileged EXEC command to enable debugging of Internet Group Management Protocol (IGMP) filter events. Use the **no** form of this command to disable debugging.

debug ip igmp filter

no debug ip igmp filter

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug ip igmp filter** command is the same as the **no debug ip igmp filter** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug ip igmp max-groups

Use the **debug ip igmp max-groups** privileged EXEC command to enable debugging of Internet Group Management Protocol (IGMP) maximum groups events. Use the **no** form of this command to disable debugging.

debug ip igmp max-groups

no debug ip igmp max-groups

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug ip igmp max-groups** command is the same as the **no debug ip igmp max-groups** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug ip igmp snooping

Use the **debug igmp snooping** privileged EXEC command to enable debugging of Internet Group Management Protocol (IGMP) snooping activity. Use the **no** form of this command to disable debugging.

debug ip igmp snooping [**group** | **management** | **querier** | **router** | **timer**]

no debug ip igmp snooping [**group** | **management** | **querier** | **router** | **timer**]

Syntax Description

group	(Optional) Display IGMP snooping group activity debug messages.
management	(Optional) Display IGMP snooping management activity debug messages.
querier	(Optional) Display IGMP snooping querier debug messages.
router	(Optional) Display IGMP snooping router activity debug messages.
timer	(Optional) Display IGMP snooping timer event debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug ip igmp snooping** command is the same as the **no debug ip igmp snooping** command.

Related Commands

Command	Description
debug platform ip igmp snooping	Displays information about platform-dependent IGMP snooping activity.
show debugging	Displays information about the types of debugging that are enabled.

debug lacp

Use the **debug lacp** privileged EXEC command to enable debugging of Link Aggregation Control Protocol (LACP) activity. Use the **no** form of this command to disable debugging.

debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

Syntax Description

all	(Optional) Display all LACP debug messages.
event	(Optional) Display LACP event debug messages.
fsm	(Optional) Display LACP finite state-machine debug messages.
misc	(Optional) Display miscellaneous LACP debug messages.
packet	(Optional) Display LACP packet debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug lacp** command is the same as the **no debug lacp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show lacp	Displays LACP channel-group information.

debug matm

Use the **debug matm** privileged EXEC command to enable debugging of platform-independent MAC address management. Use the **no** form of this command to disable debugging.

debug matm

no debug matm

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug matm** command is the same as the **no debug matm** command.

Related Commands

Command	Description
debug platform matm	Displays information about platform-dependent MAC address management.
show debugging	Displays information about the types of debugging that are enabled.

debug matm move update

Use the **debug matm move update** privileged EXEC command to enable debugging of MAC address-table move update message processing.

debug matm move update

no debug matm move update

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug matm move update** command is the same as the **no debug matm move update** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug monitor

Use the **debug monitor** privileged EXEC command to enable debugging of the Switched Port Analyzer (SPAN) feature. Use the **no** form of this command to disable debugging.

debug monitor {**all** | **errors** | **idb-update** | **info** | **list** | **notifications** | **platform** | **requests** | **snmp**}

no debug monitor {**all** | **errors** | **idb-update** | **info** | **list** | **notifications** | **platform** | **requests** | **snmp**}

Syntax Description

all	Display all SPAN debug messages.
errors	Display detailed SPAN error debug messages.
idb-update	Display SPAN interface description block (IDB) update-trace debug messages.
info	Display SPAN informational-tracing debug messages.
list	Display SPAN port and VLAN-list tracing debug messages.
notifications	Display SPAN notification debug messages.
platform	Display SPAN platform-tracing debug messages.
requests	Display SPAN request debug messages.
snmp	Display SPAN and Simple Network Management Protocol (SNMP) tracing debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug monitor** command is the same as the **no debug monitor** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show monitor	Displays information about all SPAN and remote SPAN (RSPAN) sessions on the switch.

debug nvram

Use the **debug nvram** privileged EXEC command to enable debugging of NVRAM activity. Use the **no** form of this command to disable debugging.

debug nvram

no debug nvram

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug nvram** command is the same as the **no debug nvram** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug pagp

Use the **debug pagp** privileged EXEC command to enable debugging of Port Aggregation Protocol (PAgP) activity. Use the **no** form of this command to disable debugging.

debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

no debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

Syntax Description

all	(Optional) Display all PAgP debug messages.
dual-active	(Optional) Display dual-active detection messages.
event	(Optional) Display PAgP event debug messages.
fsm	(Optional) Display PAgP finite state-machine debug messages.
misc	(Optional) Display miscellaneous PAgP debug messages.
packet	(Optional) Display PAgP packet debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug pagp** command is the same as the **no debug pagp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show pagp	Displays PAgP channel-group information.

debug platform acl

Use the **debug platform acl** privileged EXEC command to enable debugging of the access control list (ACL) manager. Use the **no** form of this command to disable debugging.

debug platform acl {**all** | **exit** | **label** | **main** |~~**racl** | **stack** | **vacl** | **vlmap** |~~**warn**}

no debug platform acl {**all** | **exit** | **label** | **main** |~~**racl** | **stack** | **vacl** | **vlmap** |~~ **warn**}

Syntax Description

all	Display all ACL manager debug messages.
exit	Display ACL exit-related debug messages.
expand	Display VMR Layer 4 VMR Operation allocation/expansion debug messages.
fspan	Display ACL FSPAN-related debug messages.
ipe	Display ACL IPE-related debug messages.
ipv6	Display ACL IPv6-related debug messages.
label	Display ACL label-related debug messages.
limitations	Display ACL limitations-related debug messages.
main	Display the main or important ACL debug messages.
odm	Display ODM-related debug messages.
port acl	Display Port ACL -related debug messages.
racl	Display router ACL related debug messages.
stack	Display ACL stack-related debug messages.
urpf	Display ACL URPF-related debug messages.
vacl	Display VLAN ACL-related debug messages.
vlmap	Display ACL VLAN-map-related debug messages.
warn	Display ACL warning-related debug messages.

Note Though visible in the command-line help strings, not all of the keywords are supported on the switch.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines The **undebug platform acl** command is the same as the **no debug platform acl** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform cpu-queues

Use the **debug platform cpu-queues** privileged EXEC command to enable debugging of platform central processing unit (CPU) receive queues. Use the **no** form of this command to disable debugging.

debug platform cpu-queues {**broadcast-q** | **cbt-to-spt-q** | **cpuhub-q** | **host-q** | **icmp-q** | **igmp-snooping-q** | **layer2-protocol-q** | **logging-q** | **remote-console-q** | **routing-protocol-q** | **rpffail-q** | **software-fwd-q** | **stp-q**}

no debug platform cpu-queues {**broadcast-q** | **cbt-to-spt-q** | **cpuhub-q** | **host-q** | **icmp-q** | **igmp-snooping-q** | **layer2-protocol-q** | **logging-q** | **remote-console-q** | **routing-protocol-q** | **rpffail-q** | **software-fwd-q** | **stp-q**}

Syntax Description

broadcast-q	Display debug messages about packets received by the broadcast queue.
cbt-to-spt-q	Display debug messages about packets received by the core-based tree to shortest-path tree (cbt-to-spt) queue.
cpuhub-q	Display debug messages about packets received by the CPU heartbeat queue.
host-q	Display debug messages about packets received by the host queue.
icmp-q	Display debug messages about packets received by the Internet Control Message Protocol (ICMP) queue.
igmp-snooping-q	Display debug messages about packets received by the Internet Group Management Protocol (IGMP)-snooping queue.
layer2-protocol-q	Display debug messages about packets received by the Layer 2 protocol queue.
logging-q	Display debug messages about packets received by the logging queue.
remote-console-q	Display debug messages about packets received by the remote console queue.
routing-protocol-q	Display debug messages about packets received by the routing protocol queue.
rpffail-q	Display debug messages about packets received by the reverse path forwarding (RFP) failure queue.
software-fwd-q	Debug packets received by the software forwarding queue.
stp-q	Debug packets received by the Spanning Tree Protocol (STP) queue.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform cpu-queues** command is the same as the **no debug platform cpu-queues** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform etherchannel

Use the **debug platform etherchannel** privileged EXEC command to enable debugging of platform-dependent EtherChannel events. Use the **no** form of this command to disable debugging.

debug platform etherchannel {**init** | **link-up** | **rpc** | **warnings**}

no debug platform etherchannel {**init** | **link-up** | **rpc** | **warnings**}

Syntax Description

init	Display EtherChannel module initialization debug messages.
link-up	Display EtherChannel link-up and link-down related debug messages.
rpc	Display EtherChannel remote procedure call (RPC) debug messages.
warnings	Display EtherChannel warning debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform etherchannel** command is the same as the **no debug platform etherchannel** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform frontend-controller

Use the **debug platform frontend-controller** privileged EXEC command to enable debugging of front-end controller activity. Use the **no** form of this command to disable debugging.

debug platform frontend-controller {**all** | **image** | **led** | **manager** | **register** | **thermal**}

no debug platform frontend-controller {**all** | **image** | **led** | **manager** | **register** | **thermal**}

Syntax Description

all	Display all the debug messages for front-end controller.
image	Display Image Manager debug messages.
led	Display LED debug messages.
manager	Display front-end-controller manager debug messages.
register	Display Register Access debug messages.
thermal	Display thermal debug messages.

Note Though visible in the command-line help strings, the **poe** keyword is not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform frontend-controller** command is the same as the **no debug platform frontend-controller** command.

Related Commands

Command	Description
show platform frontend-controller	Displays counter and status information for the front-end controller manager and subordinate applications, and displays the hardware and software information for the front-end controller.
show debugging	Displays information about the types of debugging that are enabled.

debug platform ip igmp snooping

Use the **debug platform ip igmp snooping** privileged EXEC command to enable debugging of platform-dependent Internet Group Management Protocol (IGMP) snooping. Use the **no** form of this command to disable debugging.

debug platform ip igmp snooping {**all** | **di** | **error** | **event** | **group** | **mgmt** | **pak** | **retry** | **rpc** | **warn**}

debug platform ip igmp snooping pak {*ip-address* | **error** | **ipopt** | **leave** | **query** | **report** | **rx** | **svi** | **tx**}

debug platform ip igmp snooping rpc [**cfg** | **l3mm** | **misc** | **vlan**]

no debug platform ip igmp snooping {**all** | **di** | **error** | **event** | **group** | **mgmt** | **pak** | **retry** | **rpc** | **warn**}

Syntax Description

all	Display all IGMP snooping debug messages.
di	Display IGMP snooping destination index (di) coordination remote procedure call (RPC) debug messages.
error	Display IGMP snooping error messages.
event	Display IGMP snooping event debug messages.
group	Display IGMP snooping group debug messages.
mgmt	Display IGMP snooping management debug messages.
pak {*ip-address* | **error** | **ipopt** | **leave** | **query** | **report** | **rx** | **svi** | **tx**}	Display IGMP snooping packet event debug messages. The keywords have these meanings: • *ip-address*—IP address of the IGMP group. • **error**—Display IGMP snooping packet error debug messages. • **ipopt**—Display IGMP snooping IP bridging options debug messages. • **leave**—Display IGMP snooping leave debug messages. • **query**—Display IGMP snooping query debug messages. • **report**—Display IGMP snooping report debug messages. • **rx**—Display IGMP snooping received packet debug messages. • **svi**—Display IGMP snooping switched virtual interface (SVI) packet debug messages. • **tx**—Display IGMP snooping sent packet debug messages.
retry	Display IGMP snooping retry debug messages.

rpc [**cfg** | **l3mm** | **misc** | **vlan**]	Display IGMP snooping remote procedure call (RPC) event debug messages. The keywords have these meanings: • **cfg**—(Optional) Display IGMP snooping RPC debug messages. • **l3mm**—(Optional) IGMP snooping Layer 3 multicast router group RPC debug messages. • **misc**—(Optional) IGMP snooping miscellaneous RPC debug messages. • **vlan**—(Optional) IGMP snooping VLAN assert RPC debug messages.
warn	Display IGMP snooping warning messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform ip igmp snooping** command is the same as the **no debug platform ip igmp snooping** command.

Related Commands

Command	Description
debug ip igmp snooping	Displays information about platform-independent IGMP snooping activity.
show debugging	Displays information about the types of debugging that are enabled.

debug platform led

Use the **debug platform led** privileged EXEC command to enable debugging of light-emitting diode (LED) actions. Use the **no** form of this command to disable debugging.

debug platform led {**generic** | **signal**}

no debug platform led {**generic** | **signal**}

Syntax Description

generic	Display LED generic action debug messages.
signal	Display LED signal bit map debug messages.

Note Although visible in the command-line help, the **stack** keyword is not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform led** command is the same as the **no debug platform led** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform matm

Use the **debug platform matm** privileged EXEC command to enable debugging of platform-dependent MAC address management. Use the **no** form of this command to disable debugging.

debug platform matm {**aging** | **all** | **ec-aging** | **errors** | **learning** | **rpc** | **secure-address** | **warnings**}

no debug platform matm {**aging** | **all** | **ec-aging** | **errors** | **learning** | **rpc** | **secure-address** | **warnings**}

Syntax Description

aging	Display MAC address aging debug messages.
all	Display all platform MAC address management event debug messages.
ec-aging	Display EtherChannel address aging-related debug messages.
errors	Display MAC address management error messages.
learning	Display MAC address management address-learning debug messages.
rpc	Display MAC address management remote procedure call (RPC) related debug messages.
secure-address	Display MAC address management secure address learning debug messages.
warning	Display MAC address management warning messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform matm** command is the same as the **no debug platform matm** command.

Related Commands

Command	Description
debug matm	Displays information about platform-independent MAC address management.
show debugging	Displays information about the types of debugging that are enabled.

debug platform messaging application

Use the **debug platform messaging application** privileged EXEC command to enable debugging of application messaging activity. Use the **no** form of this command to disable debugging.

debug platform messaging application {**all** | **badpak** | **cleanup** | **events** | **memerr** | **messages** | **usererr**}

no debug platform messaging application {**all** | **badpak** | **cleanup** | **events** | **memerr** | **messages** | **usererr**}

Syntax Description

all	Display all application-messaging debug messages.
badpak	Display bad-packet debug messages.
cleanup	Display clean-up debug messages.
events	Display event debug messages.
memerr	Display memory-error debug messages.
messages	Display application-messaging debug messages.
usererr	Display user-error debug messages.

Note Although visible in the command-line help, the **stackchg** keyword is not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform messaging application** command is the same as the **no debug platform messaging application** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform phy

Use the **debug platform phy** privileged EXEC command to enable debugging of PHY driver information. Use the **no** form of this command to disable debugging.

debug platform phy {**automdix** | **cablediag** | **dual-purpose** | **flcd** {**configure** | **ipc** | **iter** | **trace**} | **flowcontrol** | **forced** | **init-seq** | **link-status** | **read** | **sfp** | **show-controller** | **speed** | **write** | **xenpak**}

no debug platform phy {**automdix** | **cablediag** | **dual-purpose** | **flcd** {**configure** | **ipc** | **iter** | **trace**} | **flowcontrol** | **forced** | **init-seq** | **link-status** | **read** | **sfp** | **show-controller** | **speed** | **write** | **xenpak**}

Syntax Description

automdix	Display PHY automatic medium-dependent interface crossover (auto-MDIX) debug messages.
cablediag	Display PHY cable-diagnostic debug messages.
dual-purpose	Display PHY dual-purpose event debug messages.
flcd {**configure** | **ipc** | **iter** | **trace**}	Display PHY FLCD debug messages. The keywords have these meanings: • **configure**—Display PHY configure debug messages. • **ipc**—Display Interprocess Communication Protocol (IPC) debug messages. • **iter**—Display iter debug messages. • **trace**—Display trace debug messages.
flowcontrol	Display PHY flowcontrol debug messages.
forced	Display PHY forced-mode debug messages.
init-seq	Display PHY initialization-sequence debug messages.
link-status	Display PHY link-status debug messages.
read	Display PHY-read debug messages.
sfp	Display PHY small form-factor pluggable (SFP) modules debug messages.
show-controller	Display PHY show-controller debug messages.
speed	Display PHY speed-change debug messages.
write	Display PHY-write debug messages.
xenpak	Display PHY XENPAK debug messages

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform phy** command is the same as the **no debug platform phy** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform pm

Use the **debug platform pm** privileged EXEC command to enable debugging of the platform-dependent port manager software module. Use the **no** form of this command to disable debugging.

debug platform pm {**all** | **counters** | **errdisable** | **etherchnl** | **exceptions** | **hpm-events** | **idb-events** | **if-numbers** | **ios-events** | **link-status** | **platform** | **pm-events** | **pm-span** | **pm-vectors** [**detail**] | **rpc** [**general** | **oper-info** | **state** | **vectors** | **vp-events**] | **soutput-vectors** | **sync** | **vlans**}

no debug platform pm {**all** | **counters** | **errdisable** | **etherchnl** | **exceptions** | **hpm-events** | **idb-events** | **if-numbers** | **ios-events** | **link-status** | **platform** | **pm-events** | **pm-span** | **pm-vectors** [**detail**] | **rpc** [**general** | **oper-info** | **state** | **vectors** | **vp-events**] | **soutput-vectors** | **sync** | **vlans**}

Syntax Description

all	Display all port-manager debug messages.
counters	Display counters for remote procedure call (RPC) debug messages.
errdisable	Display error-disabled related-events debug messages.
etherchnl	Display EtherChannel related-events debug messages.
exceptions	Display system exception debug messages.
hpm-events	Display platform port-manager event debug messages.
idb-events	Display interface descriptor block (IDB) related-events debug messages.
if-numbers	Display interface-number translation-event debug messages.
ios-events	Display Cisco IOS event debug messages.
link-status	Display interface link-detection event debug messages.
platform	Display port-manager function-event debug messages.
pm-events	Display port manager event debug messages.
pm-span	Display port manager Switched Port Analyzer (SPAN) event debug messages.
pm-vectors [**detail**]	Display port-manager vector-related-event debug messages. The keyword has this meaning: • **detail**—Display vector-function details.
rpc [**general** | **oper-info** | **state** | **vectors** | **vp-events**]	Display RPC related-event debug messages. The keywords have these meanings: • **general**—(Optional) Display RPC general events. • **oper-info**—(Optional) Display operational- and informational-related RPC messages. • **state**—(Optional) Display administrative- and operational-related RPC messages. • **vectors**—(Optional) Display vector-related RPC messages. • **vp-events**—(Optional) Display virtual ports related-events RP messages.
soutput-vectors	Display IDB output vector event debug messages.
sync	Display operational synchronization and VLAN line-state event debug messages.
vlans	Display VLAN creation and deletion event debug messages.

Note Although visible in the command-line help, the **stack-manager** keyword is not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform pm** command is the same as the **no debug platform pm** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform port-asic

Use the **debug platform port-asic** privileged EXEC command to enable debugging of the port application-specific integrated circuit (ASIC) driver. Use the **no** form of this command to disable debugging.

debug platform port-asic {**interrupt** | **read** | **write**}

no debug platform port-asic {**interrupt** | **read** | **write**}

Syntax Description

interrupt	Display port-ASIC interrupt-related function debug messages.
read	Display port-ASIC read debug messages.
write	Display port-ASIC write debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform port-asic** command is the same as the **no debug platform port-asic** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform qos-acl-tcam

Use the **debug platform qos-acl-tcam** privileged EXEC command to enable debugging of the quality of service (QoS) and access control list (ACL) hardware memory manager software. Use the **no** form of this command to disable debugging.

debug platform qos-acl-tcam {**all** | **errors** | **labels** | **mask** | **tcam**}

no debug platform qos-acl-tcam {**all** | **errors** | **labels** | **mask** | **tcam**}

Syntax Description

all	Display all QoS and ACL ternary content addressable memory (QATM) manager debug messages.
errors	Display QATM error-related-events debug messages.
labels	Display QATM label-related-events debug messages.
mask	Display QATM mask-related-events debug messages.
tcam	Display QATM hardware-memory-related events debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform qos-acl-tcam** command is the same as the **no debug platform qos-acl-tcam** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform resource-manager

Use the **debug platform resource-manager** privileged EXEC command to enable debugging of the resource manager software. Use the **no** form of this command to disable debugging.

debug platform resource-manager {**all** | **dm** | **erd** | **errors** | **madmed** | **sd** | **stats** | **vld**}

no debug platform resource-manager {**all** | **dm** | **erd** | **errors** | **madmed** | **sd** | **stats** | **vld**}

Syntax Description

all	Display all resource manager debug messages.
dm	Display destination-map debug messages.
erd	Display equal-cost-route descriptor-table debug messages.
errors	Display error debug messages.
madmed	Display the MAC address descriptor table and multi-expansion descriptor table debug messages.
sd	Display the station descriptor table debug messages.
stats	Display statistics debug messages.
vld	Display the VLAN-list descriptor debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform resource-manager** command is the same as the **no debug platform resource-manager** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform snmp

Use the **debug platform snmp** privileged EXEC command to enable debugging of the platform-dependent Simple Network Management Protocol (SNMP) software. Use the **no** form of this command to disable debugging.

debug platform snmp

no debug platform snmp

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform snmp** command is the same as the **no debug platform snmp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform span

Use the **debug platform span** privileged EXEC command to enable debugging of the platform-dependent Switched Port Analyzer (SPAN) software. Use the **no** form of this command to disable debugging.

debug platform span

no debug platform span

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform span** command is the same as the **no debug platform span** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform supervisor-asic

Use the **debug platform supervisor-asic** privileged EXEC command to enable debugging of the supervisor application-specific integrated circuit (ASIC). Use the **no** form of this command to disable debugging.

debug platform supervisor-asic {**all** | **errors** | **receive** | **send**}

no debug platform supervisor-asic {**all** | **errors** | **receive** | **send**}

Syntax Description

all	Display all supervisor-ASIC event debug messages.
errors	Display the supervisor-ASIC error debug messages.
receive	Display the supervisor-ASIC receive debug messages.
send	Display the supervisor-ASIC send debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform supervisor-asic** command is the same as the **no debug platform supervisor-asic** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform sw-bridge

Use the **debug platform sw-bridge** privileged EXEC command to enable debugging of the software bridging function. Use the **no** form of this command to disable debugging.

debug platform sw-bridge {**broadcast** | **control** | **multicast** | **packet** | **unicast**}

no debug platform sw-bridge {**broadcast** | **control** | **multicast** | **packet** | **unicast**}

Syntax Description

broadcast	Display broadcast-data debug messages.
control	Display protocol-packet debug messages.
multicast	Display multicast-data debug messages.
packet	Display sent and received data debug messages.
unicast	Display unicast-data debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform sw-bridge** command is the same as the **no debug platform sw-bridge** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform tcam-driver

Use the **debug platform tcam-driver** privileged EXEC command to enable debugging of hardware memory access and lookups. Use the **no** form of this command to disable debugging.

debug platform tcam-driver {**detail** | **log** | **read** | **search** | **shadow** | **trace** | **write**}

debug platform tcam-driver log {**asic** | **clear** | **reset** | **set** | **start** | **stop**}

debug platform tcam-driver read {**fram** | **hash** | **mapping** | **otcam** | **scr** | **tcam**}

debug platform tcam-driver search

debug platform tcam-driver shadow

debug platform tcam-driver trace

debug platform tcam-driver write {**fram** | **hash** | **mapping** | **otcam** | **scr** | **tcam**}

no debug platform tcam-driver {**detail** | **log** | **read** | **search** | **shadow** | **trace** | **write**}

no debug platform tcam-driver log {**asic** | **clear** | **reset** | **set** | **start** | **stop**}

no debug platform tcam-driver read {**fram** | **hash** | **mapping** | **otcam** | **scr** | **tcam**}

no debug platform tcam-driver search

no debug platform tcam-driver shadow

no debug platform tcam-driver trace

no debug platform tcam-driver write {**fram** | **hash** | **mapping** | **otcam** | **scr** | **tcam**}

Syntax Description

log {**asic** | **clear** | **reset** | **set** | **start** | **stop**}	Display TCAM test log debug messages. The keywords have these meanings: • **asic**—Specify the ASIC to perform the operation. • **clear**—Clear the TCAM log results table. • **reset**—Reset the TCAM log criteria. • **set**—Specify TCAM log criteria (see cli help for more information) • **start**—Continuously capture matching packets in TCAM log. • **stop**—Stop capturing packets.

read {**fram** | **hash** | **mapping** | **otcam** | **scr** | **tcam**}	Display hardware-memory-read debug read messages. The keywords have these meanings: • **fram**—Display forwarding RAM read debug messages. • **hash**—Display hash read debug messages. • **mapping**—Display mapping RAM read debug messages. • **otcam**—Display overflow TCAM read debug messages. • **scr**—Display search CAM result read debug messages. • **tcam**—Display hardware-memory-read debug messages.
search	Display supervisor-initiated hardware-memory-search results debug messages.
shadow	Display shadow table debug messages.
trace	Display traceback debug messages.
write {**fram** | **hash** | **mapping** | **otcam** | **scr** | **tcam**}	Display hardware-memory-read debug write messages. The keywords have these meanings: • **fram**—Display forwarding RAM write debug messages. • **hash**—Display hash write debug messages. • **mapping**—Display mapping RAM write debug messages. • **otcam**—Display overflow TCAM write debug messages. • **scr**—Display search CAM result write debug messages. • **tcam**—Display hardware-memory-write debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform tcam** command is the same as the **no debug platform tcam** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform udld

Use the **debug platform udld** privileged EXEC command to enable debugging of the platform-dependent UniDirectional Link Detection (UDLD) software. Use the **no** form of this command to disable debugging.

debug platform udld [**all** | **error** | **rpc** {**events** | **messages**}]

no debug platform udld [**all** | **error** | **rpc** {**events** | **messages**}]

Syntax Description

all	(Optional) Display all UDLD debug messages.
error	(Optional) Display error condition debug messages.
rpc {**events** | **messages**}	(Optional) Display UDLD remote procedure call (RPC) debug messages. The keywords have these meanings: • **events**—Display UDLD RPC events. • **messages**—Display UDLD RPC messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform udld** command is the same as the **no debug platform udld** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug platform vlan

Use the **debug platform vlan** privileged EXEC command to enable debugging of the VLAN manager software. Use the **no** form of this command to disable debugging.

debug platform vlan {**errors** | **mvid** | **rpc**}

no debug platform vlan {**errors** | **mvid** | **rpc**}

Syntax Description

errors	Display VLAN error debug messages.
mvid	Display mapped VLAN ID allocations and free debug messages.
rpc	Display remote procedure call (RPC) debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug platform vlan** command is the same as the **no debug platform vlan** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug pm

Use the **debug pm** privileged EXEC command to enable debugging of port manager (PM) activity. The port manager is a state machine that controls all the logical and physical interfaces. All features, such as VLANs, UniDirectional Link Detection (UDLD), and so forth, work with the port manager to provide switch functions. Use the **no** form of this command to disable debugging.

debug pm {**all** | **assert** | **card** | **etherchnl** | **hatable** | **messages** | **port** | **redundancy** | **registry** | **sm** | **span** | **split** | **vlan** | **vp**}

no debug pm {**all** | **assert** | **card** | **etherchnl** | **hatable** | **messages** | **port** | **redundancy** | **registry** | **sm** | **span** | **split** | **vlan** | **vp**}

Syntax Description

all	Display all PM debug messages.
assert	Display assert debug messages.
card	Display line-card related-events debug messages.
etherchnl	Display EtherChannel related-events debug messages.
hatable	Display Host Access Table events debug messages.
messages	Display PM debug messages.
port	Display port related-events debug messages.
redundancy	Display redundancy debug messages.
registry	Display PM registry invocation debug messages.
sm	Display state-machine related-events debug messages.
span	Display spanning-tree related-events debug messages.
split	Display split-processor debug messages.
vlan	Display VLAN related-events debug messages.
vp	Display virtual port related-events debug messages.

Note Though visible in the command-line help strings, the **scp** and **pvlan** keywords are not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug pm** command is the same as the **no debug pm** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug qos

Use the **debug qos** privileged EXEC command to enable debugging of the quality of service (QoS) feature. Use the **no** form of this command to disable debugging.

debug qos {**capability** | **event** | **service-policy** | **set**}

no debug qos {**capability** | **event** | **service-policy** | **set**}

Syntax Description

capability	Display QoS capability debug messages.
event	Display QoS-related MPQC event debug messages.
service-policy	Display QoS service-policy debug message.
set	Display QoS packet marking debug message.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug qos** command is the same as the **no debug qos** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug spanning-tree

Use the **debug spanning-tree** privileged EXEC command to enable debugging of spanning-tree activities. Use the **no** form of this command to disable debugging.

debug spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **config** | **etherchannel** | **events** | **exceptions** | **general** | **mstp** | **pvst+** | **root** | **snmp** | **switch** | **synchronization** | **uplinkfast**}

no debug spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **config** | **etherchannel** | **events** | **exceptions** | **general** | **mstp** | **pvst+** | **root** | **snmp** | **switch** | **synchronization** | **uplinkfast**}

Syntax Description

all	Display all spanning-tree debug messages.
backbonefast	Display BackboneFast-event debug messages.
bpdu	Display spanning-tree bridge protocol data unit (BPDU) debug messages.
bpdu-opt	Display optimized BPDU handling debug messages.
config	Display spanning-tree configuration change debug messages.
etherchannel	Display EtherChannel-support debug messages.
events	Display spanning-tree topology event debug messages.
exceptions	Display spanning-tree exception debug messages.
general	Display general spanning-tree activity debug messages.
mstp	Debug Multiple Spanning Tree Protocol events.
pvst+	Display per-VLAN spanning-tree plus (PVST+) event debug messages.
root	Display spanning-tree root-event debug messages.
snmp	Display spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.
synchronization	Display the spanning-tree synchronization event debug messages.
switch	Display switch shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various switch platforms.
uplinkfast	Display UplinkFast-event debug messages.

Note Although visible in the command-line help the **csuf/csrt** keyword is not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(46)EY	This command was introduced.
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug spanning-tree command is the** same as the **no debug spanning-tree** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree backbonefast

Use the **debug spanning-tree backbonefast** privileged EXEC command to enable debugging of spanning-tree BackboneFast events. Use the **no** form of this command to disable debugging.

debug spanning-tree backbonefast [**detail** | **exceptions**]

no debug spanning-tree backbonefast [**detail** | **exceptions**]

Syntax Description

detail	(Optional) Display detailed BackboneFast debug messages.
exceptions	(Optional) Display spanning-tree BackboneFast-exception debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug spanning-tree backbonefast** command is the same as the **no debug spanning-tree backbonefast** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree bpdu

Use the **debug spanning-tree bpdu** privileged EXEC command to enable debugging of sent and received spanning-tree bridge protocol data units (BPDUs). Use the **no** form of this command to disable debugging.

debug spanning-tree bpdu [**receive** | **transmit**]

no debug spanning-tree bpdu [**receive** | **transmit**]

Syntax Description

receive	(Optional) Display the nonoptimized path for received BPDU debug messages.
transmit	(Optional) Display the nonoptimized path for sent BPDU debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug spanning-tree bpdu** command is the same as the **no debug spanning-tree bpdu** command**.**

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree bpdu-opt

Use the **debug spanning-tree bpdu-opt** privileged EXEC command to enable debugging of optimized spanning-tree bridge protocol data units (BPDUs) handling. Use the **no** form of this command to disable debugging.

debug spanning-tree bpdu-opt [**detail** | **packet**]

no debug spanning-tree bpdu-opt [**detail** | **packet**]

Syntax Description

detail	(Optional) Display detailed optimized BPDU-handling debug messages.
packet	(Optional) Display packet-level optimized BPDU-handling debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug spanning-tree bpdu-opt** command is the same as the **no debug spanning-tree bpdu-opt** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree mstp

Use the **debug spanning-tree mstp** privileged EXEC command to enable debugging of the Multiple Spanning Tree Protocol (MSTP) software. Use the **no** form of this command to disable debugging.

debug spanning-tree mstp {**all** | **boundary** | **bpdu-rx** | **bpdu-tx** | **errors** | **flush** | **init** | **migration** | **pm** | **proposals** | **region** | **roles** | **sanity_check** | **sync** | **tc** | **timers**}

no debug spanning-tree mstp {**all** | **boundary** | **bpdu-rx** | **bpdu-tx** | **errors** | **flush** | **init** | **migration** | **pm** | **proposals** | **region** | **roles** | **sanity_check** | **sync** | **tc** | **timers**}

Syntax Description

all	Enable all the debugging messages.
boundary	Debug flag changes at these boundaries: • An multiple spanning-tree (MST) region and a single spanning-tree region running Rapid Spanning Tree Protocol (RSTP) • An MST region and a single spanning-tree region running 802.1D • An MST region and another MST region with a different configuration
bpdu-rx	Debug the received MST bridge protocol data units (BPDUs).
bpdu-tx	Debug the sent MST BPDUs.
errors	Debug MSTP errors.
flush	Debug the port flushing mechanism.
init	Debug the initialization of the MSTP data structures.
migration	Debug the protocol migration state machine.
pm	Debug MSTP port manager events.
proposals	Debug handshake messages between the designated switch and the root switch.
region	Debug the region synchronization between the switch processor (SP) and the route processor (RP).
roles	Debug MSTP roles.
sanity_check	Debug the received BPDU sanity check messages.
sync	Debug the port synchronization events.
tc	Debug topology change notification events.
timers	Debug the MSTP timers for start, stop, and expire events.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug spanning-tree mstp** command is the same as the **no debug spanning-tree mstp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree switch

Use the **debug spanning-tree switch** privileged EXEC command to enable debugging of the software interface between the Spanning Tree Protocol (STP) software module and the port manager software module. Use the **no** form of this command to disable debugging.

debug spanning-tree switch {**all** | **errors** | **flush** | **general** | **helper** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**] | **uplinkfast**}

no debug spanning-tree switch {**all** | **errors** | **flush** | **general** | **helper** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**] | **uplinkfast**}

Syntax Description

all	Display all spanning-tree switch debug messages.
errors	Display debug messages for the interface between the spanning-tree software module and the port manager software module.
flush	Display debug messages for the shim flush operation.
general	Display general event debug messages.
helper	Display spanning-tree helper-task debug messages. Helper tasks handle bulk spanning-tree updates.
pm	Display port-manager event debug messages.
rx	Display received bridge protocol data unit (BPDU) handling debug messages. The keywords have these meanings: • **decode**—Display decoded received packets. • **errors**—Display receive error debug messages. • **interrupt**—Display interrupt service request (ISR) debug messages. • **process**—Display process receive BPDU debug messages.
state	Display spanning-tree port state change debug messages;
tx [**decode**]	Display sent BPDU handling debug messages. The keyword has this meaning: • **decode**—(Optional) Display decoded sent packets.
uplinkfast	Display uplinkfast packet transmission debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug spanning-tree switch** command is the same as the **no debug spanning-tree switch** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree uplinkfast

Use the **debug spanning-tree uplinkfast** privileged EXEC command to enable debugging of spanning-tree UplinkFast events. Use the **no** form of this command to disable debugging.

debug spanning-tree uplinkfast [**exceptions**]

no debug spanning-tree uplinkfast [**exceptions**]

Syntax Description

exceptions	(Optional) Display spanning-tree UplinkFast-exception debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug spanning-tree uplinkfast** command is the same as the **no debug spanning-tree uplinkfast** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug sw-vlan

Use the **debug sw-vlan** privileged EXEC command to enable debugging of VLAN manager activities. Use the **no** form of this command to disable debugging.

debug sw-vlan {**badpmcookies** | **cfg-vlan** {**bootup** | **cli**} | **events** | **ifs** | **management** | **mapping** | **notification** | **packets** | **redundancy** | **registries** | **vtp**}

no debug sw-vlan {**badpmcookies** | **cfg-vlan** {**bootup** | **cli**} | **events** | **ifs** | **management** | **mapping** | **notification** | **packets** | **redundancy** | **registries** | **vtp**}

Syntax Description

badpmcookies	Display debug messages for VLAN manager incidents of bad port manager cookies.
cfg-vlan {**bootup** | **cli**}	Display config-vlan debug messages. The keywords have these meanings: • **bootup**—Display messages when the switch is booting up. • **cli**—Display messages when the command-line interface (CLI) is in config-vlan mode.
events	Display debug messages for VLAN manager events.
ifs	See the **debug sw-vlan ifs** command.
management	Display debug messages for VLAN manager management of internal VLANs.
mapping	Display debug messages for VLAN mapping.
notification	See the **debug sw-vlan notification** command.
packets	Display debug messages for packet handling and encapsulation processes.
redundancy	Display debug messages for VTP VLAN redundancy.
registries	Display debug messages for VLAN manager registries.
vtp	See the **debug sw-vlan vtp** command.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug sw-vlan** command is the same as the **no debug sw-vlan** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.
show vtp	Displays general information about VTP management domain, status, and counters.

debug sw-vlan ifs

Use the **debug sw-vlan ifs** privileged EXEC command to enable debugging of the VLAN manager IOS file system (IFS) error tests. Use the **no** form of this command to disable debugging.

debug sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

no debug sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

Syntax Description

open {**read** | **write**}	Display VLAN manager IFS file-open operation debug messages. The keywords have these meanings: • **read**—Display VLAN manager IFS file-read operation debug messages. • **write**—Display VLAN manager IFS file-write operation debug messages.
read {**1** | **2** | **3** | **4**}	Display file-read operation debug messages for the specified error test (1, 2, 3, or 4).
write	Display file-write operation debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

When selecting the file read operation, Operation **1** reads the file header, which contains the header verification word and the file version number. Operation **2** reads the main body of the file, which contains most of the domain and VLAN information. Operation **3** reads type length version (TLV) descriptor structures. Operation **4** reads TLV data.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

debug sw-vlan notification

Use the **debug sw-vlan notification** privileged EXEC command to enable debugging of the activation and deactivation of Inter-Link Switch (ISL) VLAN IDs. Use the **no** form of this command to disable debugging.

debug sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}

no debug sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}

Syntax Description

accfwdchange	Display debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
allowedvlancfgchange	Display debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
fwdchange	Display debug messages for VLAN manager notification of spanning-tree forwarding changes.
linkchange	Display debug messages for VLAN manager notification of interface link-state changes.
modechange	Display debug messages for VLAN manager notification of interface mode changes.
pruningcfgchange	Display debug messages for VLAN manager notification of changes to the pruning configuration.
statechange	Display debug messages for VLAN manager notification of interface state changes.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

debug sw-vlan vtp

Use the **debug sw-vlan vtp** privileged EXEC command to enable debugging of the VLAN Trunking Protocol (VTP) code. Use the **no** form of this command to disable debugging.

debug sw-vlan vtp {**events** | **packets** | **pruning** [**packets** | **xmit**] | **redundancy** | **xmit**}

no debug sw-vlan vtp {**events** | **packets** | **pruning** | **redundancy** | **xmit**}

Syntax Description

events	Display debug messages for general-purpose logic flow and detailed VTP messages generated by the VTP_LOG_RUNTIME macro in the VTP code.
packets	Display debug messages for the contents of all incoming VTP packets that have been passed into the VTP code from the IOS VTP platform-dependent layer, except for pruning packets.
pruning [**packets** | **xmit**]	Display debug messages generated by the pruning segment of the VTP code. The keywords have these meanings: • **packets**—(Optional) Display debug messages for the contents of all incoming VTP pruning packets that have been passed into the VTP code from the IOS VTP platform-dependent layer. • **xmit**—(Optional) Display debug messages for the contents of all outgoing VTP packets that the VTP code requests the IOS VTP platform-dependent layer to send.
redundancy	Display debug messages for VTP redundancy.
xmit	Display debug messages for the contents of all outgoing VTP packets that the VTP code requests the IOS VTP platform-dependent layer to send, except for pruning packets.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug sw-vlan vtp** command is the same as the **no debug sw-vlan vtp** command.

If no further parameters are entered after the **pruning keyword**, VTP pruning debugging messages appear. They are generated by the VTP_PRUNING_LOG_NOTICE, VTP_PRUNING_LOG_INFO, VTP_PRUNING_LOG_DEBUG, VTP_PRUNING_LOG_ALERT, and VTP_PRUNING_LOG_WARNING macros in the VTP pruning code.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show vtp	Displays general information about VTP management domain, status, and counters.

debug udld

Use the **debug udld** privileged EXEC command to enable debugging of the UniDirectional Link Detection (UDLD) feature. Use the **no** form of this command to disable UDLD debugging.

debug udld {**events** | **packets** | **registries**}

no debug udld {**events** | **packets** | **registries**}

Syntax Description

events	Display debug messages for UDLD process events as they occur.
packets	Display debug messages for the UDLD process as it receives packets from the packet queue and tries to send them at the request of the UDLD protocol code.
registries	Display debug messages for the UDLD process as it processes registry calls from the UDLD process-dependent module and other feature modules.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug udld** command is the same as the **no debug udld** command.

For **debug udld events**, these debugging messages appear:

- General UDLD program logic flow
- State machine state changes
- Program actions for the set and clear ErrDisable state
- Neighbor cache additions and deletions
- Processing of configuration commands
- Processing of link-up and link-down indications

For **debug udld packets**, these debugging messages appear:

- General packet processing program flow on receipt of an incoming packet
- Indications of the contents of the various pieces of packets received (such as type length versions [TLVs]) as they are examined by the packet reception code
- Packet transmission attempts and the outcome

For **debug udld registries**, these categories of debugging messages appear:

- Sub-block creation
- Fiber-port status changes

- State change indications from the port manager software
- MAC address registry calls

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show udld	Displays UDLD administrative and operational status for all ports or the specified port.

debug vqpc

Use the **debug vqpc** privileged EXEC command to enable debugging of the VLAN Query Protocol (VQP) client. Use the **no** form of this command to disable debugging.

debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

no debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

Syntax Description

all	(Optional) Display all VQP client debug messages.
cli	(Optional) Display the VQP client command-line interface (CLI) debug messages.
events	(Optional) Display VQP client event debug messages.
learn	(Optional) Display VQP client address learning debug messages.
packet	(Optional) Display VQP client packet information debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53)EY	This command was introduced.

Usage Guidelines

The **undebug vqpc** command is the same as the **no debug vqpc** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

APPENDIX C

Show Platform Commands

This appendix describes the **show platform** privileged EXEC commands that have been created or changed for use with the switch. These commands display information helpful in diagnosing and resolving internetworking problems and should be used only under the guidance of Cisco technical support staff.

show platform acl

Use the **show platform acl** privileged EXEC command to display platform-dependent access control list (ACL) manager information.

show platform acl {**interface** *interface-id* | **label** *label-number* [**detail**] | **statistic**s *asic-number* | **usage** *asic-number* [**summary**] | **vlan** *vlan-id*} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	Display per-interface ACL manager information for the specified interface. The interface can be a physical interface or a VLAN.
label *label-number* [**detail**]	Display per-label ACL manager information. The *label-number* range is 0 to 255. The keyword has this meaning: • **detail**—(Optional) Display detailed ACL manager label information.
statistics *asic-number*	Display per-ASIC ACL manager information. The *asic-numbe*r is the port ASIC number, either 0 or 1.
usage *asic-number* [**summary**]	Display per-ASIC ACL usage information. The keyword has this meaning: • **summary**—(Optional) Display usage information in a brief format.
vlan *vlan-id*	Display per-VLAN ACL manager information. The *vlan-id* range is from 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Although visible in the command-line help, the **fspan** keyword is not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform dl

Use the **show platform dl** privileged EXEC command to display dynamically loaded module information.

show platform dl [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

detail	(Optional) Display detailed dynamically loaded module information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform etherchannel

Use the **show platform etherchannel** privileged EXEC command to display platform-dependent EtherChannel information.

show platform etherchannel {**data-structures** | **flags** | **time-stamps**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

data-structures	Display EtherChannel data structures.
flags	Display EtherChannel port flags.
time-stamps	Display EtherChannel time stamps.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform forward

Use the **show platform forward** privileged EXEC command for an interface to specify how the hardware would forward a frame that matches the specified parameters.

show platform forward *interface-id* [**vlan** *vlan-id*] *src-mac dst-mac* [*l3protocol-id*] [**ipv6** | **sap** | **snap**] [**cos** *cos*] [**ip** *src-ip dst-ip* [**frag** *field*] [**dscp** *dscp*] {*l4protocol-id* | **icmp** *icmp-type icmp-code* | **igmp** *igmp-version igmp-type* | **sctp** *src-port dst-port* | **tcp** *src-port dst-port flags* | **udp** *src-port dst-port*]} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	The input physical interface, the port on which the packet comes in to the switch (including type and port number).
vlan *vlan-id*	(Optional) Input VLAN ID. The range is 1 to 4094. If not specified, and the input interface is not a routed port, the default is 1.
src-mac	48-bit source MAC address.
dst-mac	48-bit destination MAC address.
l3protocol-id	(Optional) The Layer 3 protocol used in the packet. The number is a value 0 to 65535.
ipv6	(Optional) IPv6 frame.
sap	(Optional) Service access point (SAP) encapsulation type.
snap	(Optional) Subnetwork Access Protocol (SNAP) encapsulation type.
cos *cos*	(Optional) Class of service (CoS) value of the frame. The range is 0 to 7.
ip *src-ip dst-ip*	(Optional, but required for IP packets) Source and destination IP addresses in dotted decimal notation.
frag *field*	(Optional) The IP fragment field for a fragmented IP packet. The range is 0 to 65535.
dscp *dscp*	(Optional) Differentiated Services Code Point (DSCP) field in the IP header. The range is 0 to 63.
l4protocol-id	The numeric value of the Layer 4 protocol field in the IP header. The range is 0 to 255. For example, 47 is generic routing encapsulation (GRE), and 89 is Open Shortest Path First (OSPF). If the protocol is TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or Internet Group Management Protocol (IGMP), you should use the appropriate keyword instead of a numeric value.
icmp *icmp-type icmp-code*	ICMP parameters. The *icmp-type* and *icmp-code* ranges are 0 to 255.
igmp *igmp-version igmp-type*	IGMP parameters. The *igmp-version* range is 1 to 15; the *igmp-type* range is 0 to 15.
sctp *src-port dst-port*	Stream Control Transmission Protocol (SCTP) parameters. The ranges for the SCTP source and destination ports are 0 to 65535.
tcp *src-port dst-port flags*	TCP parameters: TCP source port, destination port, and the numeric value of the TCP flags byte in the header. The *src-port* and *dst-port* ranges are 0 to 65535. The flag range is 0 to 1024.
udp *src-port dst-port*	UDP parameters. The *src-port* and *dst-port* ranges are 0 to 65535.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.

| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

For examples of the **show platform forward** command output displays and what they mean, see the "Troubleshooting" chapter of the software configuration guide for this release.

show platform frontend-controller

Use the **show platform frontend-controller** privileged EXEC command to display counter and status information for the front-end controller manager and subordinate applications and to display the hardware and software information for the front-end controller.

show platform frontend-controller {**buffer** | **generic** | **manager** *number* | **subordinate** *number* | **version** *number*} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

buffer	Display the last 1024 bytes sent from the manager to the subordinate and the reverse.
generic	Display the generic counters that do not specifically apply to the manager or subordinate.
manager *number*	Display the counters for the manager and the subordinate specified by *number*. See the "Usage Guidelines" section for the *number* range.
subordinate *number*	Display the subordinate status and the counters for the subordinate specified by *number*. See the "Usage Guidelines" section for the *number* range.
version *number*	Display the hardware and software version information for the subordinate status specified by *number*. The range is from 0 to 2.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform ip igmp snooping

Use the **show platform ip igmp snooping** privileged EXEC command to display platform-dependent Internet Group Management Protocol (IGMP) snooping information.

show platform ip igmp snooping {**all** | **control** [**di**] | **counters** | **flood** [**vlan** *vlan-id*] | **group** *ip-address* | **hardware** | **retry** [**count** | **local** [**count**] | **remote** [**count**]]} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

all	Display all IGMP snooping platform IP multicast information.
control [**di**]	Display IGMP snooping control entries. The keyword has this meaning: • **di**—(Optional) Display IGMP snooping control destination index entries.
counters	Display IGMP snooping counters.
flood [**vlan** *vlan-id*]	Display IGMP snooping flood information. The keyword has this meaning: • **vlan** *vlan-id*—(Optional) Display flood information for the specified VLAN. The range is 1 to 4094.
group *ip-address*	Display the IGMP snooping multicast group information, where *ip-address* is the IP address of the group.
hardware	Display IGMP snooping information loaded into hardware.
retry [**count** | **local** [**count**]	Display IGMP snooping retry information. The keywords have these meanings: • **count**—(Optional) Display only the retry count. • **local**—(Optional) Display local retry entries.
remote [**count**]	Display remote entries. The keyword has this meaning: • **count**—(Optional) Display only the remote count.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform layer4op

Use the **show platform layer4op** privileged EXEC command to display platform-dependent Layer 4 operator information.

show platform layer4op {**acl** | **pacl** [*port-asic*] | **qos** [*port-asic*]} {**and-or** | **map** | **or-and** | **vcu**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

acl	Display access control list (ACL) Layer 4 operators information.
pacl [*port-asic*]	Display port ACL Layer 4 operators information. The keyword has this meaning: • *port-asic*—(Optional) Port ASIC number.
qos [*port-asic*]	Display quality of service (QoS) Layer 4 operators information. The keyword has this meaning: • *port-asic*—(Optional) QoS port ASIC number.
and-or	Display AND-OR registers information.
map	Display select map information.
or-and	Display OR-AND registers information.
vcu	Display value compare unit (VCU) register information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform mac-address-table

Use the **show platform mac-address-table** privileged EXEC command to display platform-dependent MAC address table information.

show platform mac-address-table [**aging-array** | **hash-table** | **mac-address** *mac-address* | **retry-q** [**mac-address** *mac-address* | **vlan** *vlan-id*]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

aging-array	(Optional) Display the MAC address table aging array.
hash-table	(Optional) Display the MAC address table hash table.
mac-address *mac-address*	(Optional) Display the MAC address table MAC address information, where *mac-address* is the 48-bit hardware address.
vlan *vlan-id*	(Optional) Display information for the specified VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform messaging

Use the **show platform messaging** privileged EXEC command to display platform-dependent application and performance message information.

show platform messaging {**application** [**incoming** | **outgoing** | **summary**] | **hiperf** [*class-number*]} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

application [**incoming** | **outgoing** | **summary**]	Display application message information. The keywords have these meanings: • **incoming**—(Optional) Display only information about incoming application messaging requests. • **outgoing**—(Optional) Display only information about incoming application messaging requests. • **summary**—(Optional) Display summary information about all application messaging requests.
hiperf [*class-number*]	Display outgoing high-performance message information. Specify the *class-number* option to display information about high-performance messages for this class number. The range is 0 to 62.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform monitor

Use the **show platform monitor** privileged EXEC command to display platform-dependent Switched Port Analyzer (SPAN) information.

show platform monitor [**session** *session-number*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

session *session-number*	(Optional) Display SPAN information for the specified SPAN session. The range is 1 to 66.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform pm

Use the **show platform pm** privileged EXEC command to display platform-dependent port-manager information.

show platform pm {**counters** | **group-masks** | **idbs** {**active-idbs** | **deleted-idbs**} | **if-numbers** | **link-status** | **platform-block** | **port-info** *interface-id* | **vlan** {**info** | **line-state**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

counters	Display module counters information.
group-masks	Display EtherChannel group masks information.
idbs {**active-idbs** | **deleted-idbs**}	Display interface data block (IDB) information. The keywords have these meanings: • **active-idbs**—Display active IDB information. • **deleted-idbs**—Display deleted and leaked IDB information.
if-numbers	Display interface numbers information.
link-status	Display local port link status information.
platform-block	Display platform port block information.
port-info *interface-id*	Display port administrative and operation fields for the specified interface.
vlan {**info** | **line-state**}	Display platform VLAN information. The keywords have these meanings: • **info**—Display information for active VLANs. • **line-state**—Display line-state information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help strings, the **stack-view** keyword is not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform port-asic

Use the **show platform port-asic** privileged EXEC command to display platform-dependent port ASIC register information.

show platform port-asic {**cpu-queue-map-table** [**asic** *number* | **port** *number* [**asic** *number*]] |
dest-map index *number* |
etherchannel-info [**asic** *number* | **port** *number* [**asic** *number*]] |
exception [**asic** *number* | **port** *number* [**asic** *number*]] |
global-status [**asic** *number* | **port** *number* [**asic** *number*]] |
learning [**asic** *number* | **port** *number* [**asic** *number*]] |
mac-info [**asic** *number* | **port** *number* [**asic** *number*]] |
mvid [**asic** *number*] |
packet-info-ram [**asic** *number* | **index** *number* [**asic** *number*]] |
port-info [**asic** *number* | **port** *number* [**asic** *number*]] |
prog-parser [**asic** *number* | **port** *number* [**asic** *number*]] |
receive {**buffer-queue** | **port-fifo** | **supervisor-sram**} [**asic** *number* | **port** *number* [**asic** *number*]] |
span [*vlan-id* [**asic** *number*] | [**asic** *number*]
stats {**drop** | **enqueue** | **miscellaneous** | **supervisor**} [**asic** *number* | **port** *number* [**asic** *number*]] |
transmit {**port-fifo** | **queue** | **supervisor-sram**} [**asic** *number* | **port** *number* [**asic** *number*]]
vct [**asic** *number* | **port** *number* [**asic** *number*]]
version}
[| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

cpu-queue-map-table [**asic** *number* | **port** *number* [**asic** *number*]]	Display the CPU queue-map table entries. The keywords have these meanings: • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1. • **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27.
dest-map index *number*	Display destination-map information for the specified index. The range is 0 to 65535.
etherchannel-info [**asic** *number* | **port** *number* [**asic** *number*]]	Display the contents of the EtherChannel information register. The keywords have these meanings: • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1. • **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.

exception [**asic** *number* | **port** *number* [**asic** *number*]]	Display the exception-index register information. The keywords have these meanings: • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1. • **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
global-status [**asic** *number* | **port** *number* [**asic** *number*]]	Display global and interrupt status. The keywords have these meanings: • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1. • **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
learning [**asic** *number* | **port** *number* [**asic** *number*]]	Display entries in the learning cache. The keywords have these meanings: • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1. • **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
mac-info [**asic** *number* | **port** *number* [**asic** *number*]]	Display the contents of the MAC information register. The keywords have these meanings: • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1. • **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
mvid [**asic** *number*]	Display the mapped VLAN ID table. The keyword has this meaning: • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1.
packet-info-ram [**asic** *number* | **index** *number* [**asic** *number*]]	Display the packet information RAM. The keywords have these meanings: • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1. • **index** *number*—(Optional) Display information for the specified packet RAM index number and ASIC number. The range is 0 to 63.

port-info [**asic** *number* | **port** *number* [**asic** *number*]]	Display port information register values. The keywords have these meanings: • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1. • **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
prog-parser [**asic** *number* | **port** *number* [**asic** *number*]]	Display the programmable parser tables. The keywords have these meanings: • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1. • **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
receive {**buffer-queue** | **port-fifo** | **supervisor-sram**} [**asic** *number* | **port** *number* [**asic** *number*]]	Display receive information. The keywords have these meanings: • **buffer-queue**—Display the buffer queue information. • **port-fifo**—Display the port-FIFO information. • **supervisor-sram**—Display the supervisor static RAM (SRAM) information. • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1. • **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
span [*vlan-id* | **asic** *number*]	Display the Switched Port Analyzer (SPAN)-related information. The keywords have these meanings: • *vlan-id*—(Optional) Display information for the specified VLAN. The range is 0 to 1023. • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1.
stats {**drop** | **enqueue** | **miscellaneous** | **supervisor**} [**asic** *number* | **port** *number* [**asic** *number*]]	Display raw statistics for the port ASIC. The keywords have these meanings: • **drop**—Display drop statistics. • **enqueue**—Display enqueue statistics. • **miscellaneous**—Display miscellaneous statistics. • **supervisor**—Display supervisor statistics. • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1. • **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.

transmit {**port-fifo** | **queue** | **supervisor-sram**} [**asic** *number* | **port** *number* [**asic** *number*]]	Display transmit information. The keywords have these meanings: • **port-fifo**—Display the contents of the port-FIFO information register. • **queue**—Display the contents of the queue information register. • **supervisor-sram**—Display supervisor SRAM information. • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1. • **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
vct [**asic** *number* | **port** *number* [**asic** *number*]]	Display the VLAN compression table entries for the specified ASIC or for the specified port and ASIC. The keywords have these meanings: • **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1. • **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
version	Display version and device type information for port ASICs.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help strings, the **stack** {**control** | **dest-map** | **learning** | **messages** | **mvid** | **prog-parser** | **span** | **stats** [**asic** *number* | **port** *number* [**asic** *number*]] keywords are not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform qos

Use the **show platform qos** privileged EXEC command to display platform-dependent quality of service (QoS) information.

show platform qos {**label asic** *number* | **policer** {**parameters asic** *number* | **port alloc** *number* **asic** *number*}} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

label asic *number*	Display QoS label maps for the specified ASIC. (Optional) For **asic** *number*, the range is 0 to 1.
policer {**parameters asic** *number* | **port alloc** *number* **asic** *number*}	Display policer information. The keywords have these meanings: • **parameters asic** *number*—Display parameter information for the specified ASIC. The range is 0 to 1. • **port alloc** *number* **asic** *number*—Display port allocation information for the specified port and ASIC. The port allocation range is 0 to 25. The ASIC range is 0 to 1.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform resource-manager

Use the **show platform resource-manager** privileged EXEC command to display platform-dependent resource-manager information.

show platform resource-manager {**dm** [**index** *number*] | **erd** [**index** *number*] | **mad** [**index** *number*] | **med** [**index** *number*] | **mod** | **msm** {**hash-table** [**vlan** *vlan-id*] | **mac-address** *mac-address* [**vlan** *vlan-id*]} | **sd** [**index** *number*] | **vld** [**index** *number*]} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

dm [**index** *number*]	Display the destination map. The keyword has this meaning: • **index** *number*—(Optional) Display the specified index. The range is 0 to 65535.
erd [**index** *number*]	Display the equal-cost-route descriptor table for the specified index. The keyword has this meaning: • **index** *number*—(Optional) Display the specified index. The range is 0 to 65535.
mad [**index** *number*]	Display the MAC-address descriptor table for the specified index. The keyword has this meaning: • **index** *number*—(Optional) Display the specified index. The range is 0 to 65535.
med [**index** *number*]	Display the multi-expansion descriptor table for the specified index. The keyword has this meaning: • **index** *number*—(Optional) Display the specified index. The range is 0 to 65535.
mod	Display the resource-manager module information.
msm {**hash-table** [**vlan** *vlan-id*] | **mac-address** *mac-address* [**vlan** *vlan-id*]}	Display the MAC-address descriptor table and the station descriptor table information. The keywords have these meanings: • **hash-table** [**vlan** *vlan-id*]—Display the hash table for all VLANs or the specified VLAN. The range is 1 to 4094. • **mac-address** *mac-address* [**vlan** *vlan-id*]—Display the MAC-address descriptor table for the specified MAC address represented by the 48-bit hardware address for all VLANs or the specified VLAN. The range is 1 to 4094.
sd [**index** *number*]	Display the station descriptor table for the specified index. The keyword has this meaning: • **index** *number*—(Optional) Display the specified index. The range is 0 to 65535.
vld [**index** *number*]	Display the VLAN-list descriptor table for the specified index. The keyword has this meaning: • **index** *number*—(Optional) Display the specified index. The range is 0 to 65535.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.

| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform snmp counters

Use the **show platform snmp counters** privileged EXEC command to display platform-dependent Simple Network Management Protocol (SNMP) counter information.

show platform snmp counters [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform spanning-tree synchronization

Use the **show platform spanning-tree synchronization** privileged EXEC command to display platform-dependent spanning-tree synchronization information.

show platform spanning-tree synchronization [**detail** | **vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

detail	Optional) Display detailed spanning-tree information.
vlan *vlan-id*	(Optional) Display VLAN switch spanning-tree information for the specified VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform stp-instance

Use the **show platform stp-instance** privileged EXEC command to display platform-dependent spanning-tree instance information.

show platform stp-instance *vlan-id* [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan-id	Display spanning-tree instance information for the specified VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform tcam

Use the **show platform tcam** privileged EXEC command to display platform-dependent hardware memory driver information.

show platform tcam {**handle** *number* | **log {results** | **settings** [**asic** *number*]} | **table** {**acl** | **all** | **local** | **mac-address** | **qos** | **static-address** | **station** | **vlan-list**} | **usage**} [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table acl [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table all [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table l2 [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table mac-address [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table qos [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table station [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table vlan-list [[**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

handle *number*	Display the hardware memory handle. The range is 0 to 4294967295.
log results	Display the hardware memory log results.
log settings	Display the log register settings.

table {**acl** | **all** | **l2** | **mac-address** | **qos** | **static-address** | **station** | **vlan-list**}	Display lookup and forwarding table information. The keywords have these meanings: • **acl**—Display the access-control list (ACL) table. • **all**—Display all the hardware memory tables. • **l2**—Display the Layer 2 lookup table. • **mac-address**—Display the MAC-address table. • **qos**—Display the QoS table. • **static-address**—Display the static-address table. • **station**—Display the station table. • **vlan-list**—Display the VLAN list table.
[[**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]]	Display information. The keywords have these meanings: • **asic** *number*—Display information for the specified ASIC device ID. The range is 0 to 15. • **detail** [**invalid**]—(Optional) Display valid or invalid details. • **index** *number*—(Optional) Display information for the specified hardware memory table index. The range is 0 to 32768. • **num** *number*—(Optional) Display information for the specified hardware memory table number. The range is 0 to 32768.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help strings, the **usage, equal-cost-route, ipv6, mcast, metprt, multicast-expansion, pbr, unicast-direct, unicast-indirect, unicast-rpf-check,** and **usage** keywords are not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform vlan

Use the **show platform vlan** privileged EXEC command to display platform-dependent VLAN information.

show platform vlan {**misc** | **mvid** | **prune** | **refcount** | **rpc** {**receive** | **transmit**}} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

misc	Display miscellaneous VLAN module information.
mvid	Display the mapped VLAN ID (MVID) allocation information.
prune	Display the platform-maintained pruning database.
refcount	Display the VLAN lock module-wise reference counts.
rpc {**receive** | **transmit**}	Display remote procedure call (RPC) messages. The keywords have these meanings: • **receive**—Display received information. • **transmit**—Display sent information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(53EY	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

APPENDIX D

Acknowledgments for Open-Source Software

The Cisco IOS software pipe command uses Henry Spencer's regular expression library (regex). The most recent version of the library has been modified slightly in the Catalyst operating system software to maintain compatibility with earlier versions of the library.

Henry Spencer's regular expression library (regex). Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

INDEX

A

aaa authorization network command 2-1
access groups
  IP 2-74
access mode 2-396
access ports 2-396
ACLs
  displaying 2-177
  IP 2-74
  on Layer 2 interfaces 2-74
aggregate-port learner 2-153
allowed VLANs 2-400
archive download-sw command 2-3
archive tar command 2-6
archive upload-sw command 2-9
arp (boot loader) command A-2
autonegotiation of duplex mode 2-56

B

BackboneFast, for STP 2-338
boot (boot loader) command A-3
boot config-file command 2-11
boot enable-break command 2-12
boot helper command 2-13
boot helper-config file command 2-14
booting
  Cisco IOS image 2-17
  displaying environment variables 2-181
  interrupting 2-12
  manually 2-15
boot loader
  accessing A-1
  booting
    Cisco IOS image A-3
    helper image 2-13
  directories
    creating A-19
    displaying a list of A-8
    removing A-23
  displaying
    available commands A-13
    memory heap utilization A-14
    version A-30
  environment variables
    described A-24
    displaying settings A-24
    location of A-25
    setting A-24
    unsetting A-28
  files
    copying A-6
    deleting A-7
    displaying a list of A-8
    displaying the contents of A-5, A-20, A-27
    renaming A-21
  file system
    formatting A-11
    initializing flash A-10
    running a consistency check A-12
  prompt A-1
  resetting the system A-22
boot manual command 2-15
boot private-config-file command 2-16
boot system command 2-17

BPDU filtering, for spanning tree 2-339, 2-373
BPDU guard, for spanning tree 2-341, 2-373

C

candidate switches
See clusters
cat (boot loader) command A-5
channel-group command 2-18
channel-protocol command 2-21
class-map command 2-22
class maps
creating 2-22
defining the match criteria 2-132
displaying 2-184
class of service
See CoS
clear eap command 2-24
clear errdisable interface 2-25
clear lacp command 2-26
clear logging onboard command 2-27
clear mac address-table command 2-28
clear pagp command 2-29
clear spanning-tree counters command 2-30
clear spanning-tree detected-protocols command 2-31
clear vtp counters command 2-32
cluster commander-address command 2-33
cluster discovery hop-count command 2-35
cluster enable command 2-36
cluster holdtime command 2-38
cluster member command 2-39
cluster outside-interface command 2-41
cluster run command 2-42
clusters
adding candidates 2-39
building manually 2-39
communicating with
devices outside the cluster 2-41
members by using Telnet 2-165
debug messages, display B-2
displaying
candidate switches 2-187
debug messages B-2
member switches 2-189
status 2-185
hop-count limit for extended discovery 2-35
SNMP trap 2-329
cluster timer command 2-43
command modes defined 1-1
command switch
See clusters
configuration files
password recovery disable considerations A-1
specifying the name 2-11, 2-16
configuring multiple interfaces 2-69
config-vlan mode
commands 2-418
description 1-4
entering 2-417
summary 1-2
copy (boot loader) command A-6
copy logging onboard command 2-44
CoS
assigning default value to incoming packets 2-140
overriding the incoming value 2-140
CPU ASIC statistics, displaying 2-191
crashinfo files 2-63

D

debug cluster command B-2
debug dtp command B-4
debug eap command B-5
debug etherchannel command B-6
debug fastethernet command B-7
debug interface command B-8
debug ip igmp filter command B-9
debug ip igmp max-groups command B-10

debug ip igmp snooping command B-11
debug lacp command B-12
debug matm command B-13
debug matm move update command B-14
debug monitor command B-15
debug nvram command B-16
debug pagp command B-17
debug platform acl command B-18
debug platform configuration command B-23
debug platform cpu-queues command B-20
debug platform etherchannel command B-22
debug platform ip igmp snooping command B-24
debug platform led command B-26
debug platform matm command B-27
debug platform messaging application command B-28
debug platform phy command B-29
debug platform pm command B-31
debug platform port-asic command B-33
debug platform qos-acl-tcam command B-34
debug platform resource-manager command B-35
debug platform snmp command B-36
debug platform span command B-37
debug platform supervisor-asic command B-38
debug platform sw-bridge command B-39
debug platform tcam-driver command B-40
debug platform udld command B-42
debug platform vlan command B-43
debug pm command B-44
debug qos command B-46
debug spanning-tree backbonefast command B-49
debug spanning-tree bpdu command B-50
debug spanning-tree bpdu-opt command B-51
debug spanning-tree command B-47
debug spanning-tree mstp command B-52
debug spanning-tree switch command B-54
debug spanning-tree uplinkfast command B-56
debug sw-vlan command B-57
debug sw-vlan ifs command B-59
debug sw-vlan notification command B-60
debug sw-vlan vtp command B-62
debug udld command B-64
debug vqpc command B-66
define interface-range command 2-46
delete (boot loader) command A-7
delete command 2-48
detect mechanism, causes 2-57
Digital Optical Monitoring
    see DoM
dir (boot loader) command A-8
directories, deleting 2-48
DoM
    displaying supported transceivers 2-243
domain name, VTP 2-422, 2-426
DTP 2-397
DTP flap
    error detection for 2-57
    error recovery timer 2-60
DTP negotiation 2-398
duplex command 2-55
dynamic-access ports
    configuring 2-392
dynamic auto VLAN membership mode 2-396
dynamic desirable VLAN membership mode 2-396
Dynamic Trunking Protocol
    See DTP

E

environment variables, displaying 2-181
errdisable detect cause command 2-57
errdisable detect cause small-frame command 2-59
errdisable recovery cause small-frame 2-62
errdisable recovery command 2-60
error conditions, displaying 2-220
error disable detection 2-57
error-disabled interfaces, displaying 2-232
EtherChannel
    assigning Ethernet interface to channel group 2-18

creating port-channel logical interface 2-67
debug EtherChannel/PAgP, display B-6
debug platform-specific events, display B-22
displaying 2-223
interface information, displaying 2-232
LACP
clearing channel-group information 2-26, 2-27
debug messages, display B-12
displaying 2-266
modes 2-18
port priority for hot-standby ports 2-115
restricting a protocol 2-21
system priority 2-117
load-distribution methods 2-157
PAgP
aggregate-port learner 2-153
clearing channel-group information 2-29
debug messages, display B-17
displaying 2-301
error detection for 2-57
error recovery timer 2-60
learn method 2-153
modes 2-18
physical-port learner 2-153
priority of interface for transmitted traffic 2-155
Ethernet controller, internal register display 2-193, 2-201
Ethernet Management port, debugging B-7
Ethernet statistics, collecting 2-169
exception crashinfo command 2-63, 2-66
extended discovery of candidate switches 2-35
extended-range VLANs
and allowed VLAN list 2-400
and pruning-eligible list 2-400
configuring 2-417
extended system ID for STP 2-347

F

fallback profile command 2-64
fallback profiles, displaying 2-226
fan information, displaying 2-216
file name, VTP 2-422
files, deleting 2-48
flash_init (boot loader) command A-10
flowcontrol command 2-64
format (boot loader) command A-11
forwarding results, display C-5
frame forwarding information, displaying C-5
front-end controller counter and status information C-7
fsck (boot loader) command A-12

G

global configuration mode 1-2, 1-3

H

hardware ACL statistics 2-177
health monitoring diagnostic tests 2-49
help (boot loader) command A-13
hop-count limit for clusters 2-35
host connection, port configuration 2-395

I

IGMP filters
applying 2-80
debug messages, display B-9
IGMP groups, setting maximum 2-81
IGMP maximum groups, debugging B-10
IGMP profiles
creating 2-83
displaying 2-248
IGMP snooping
adding ports as a static member of a group 2-97
displaying 2-249, 2-254, 2-256
enabling 2-85

enabling the configurable-leave timer 2-87
enabling the Immediate-Leave feature 2-96
flooding query count 2-93
interface topology change notification behavior 2-95
multicast table 2-252
querier 2-89
query solicitation 2-93
report suppression 2-91
switch topology change notification behavior 2-93
images
See software images
Immediate-Leave processing
IGMP 2-96
IPv6 2-113
interface configuration mode 1-2, 1-4
interface port-channel command 2-67
interface range command 2-69
interface-range macros 2-46
interfaces
assigning Ethernet interface to channel group 2-18
configuring 2-55
configuring multiple 2-69
creating port-channel logical 2-67
debug messages, display B-8
disabling 2-325
displaying the MAC address table 2-285
restarting 2-325
interface speed, configuring 2-384
interface vlan command 2-72
internal registers, displaying 2-193, 2-201, 2-203
Internet Group Management Protocol
See IGMP
invalid GBIC
error detection for 2-57
error recovery timer 2-60
ip access-group command 2-74
ip address command 2-76
IP addresses, setting 2-76
ip admission command 2-78
ip admission name proxy http command 2-79
ip igmp filter command 2-80
ip igmp max-groups command 2-81
ip igmp profile command 2-83
ip igmp snooping command 2-85
ip igmp snooping last-member-query-interval command 2-87
ip igmp snooping querier command 2-89
ip igmp snooping report-suppression command 2-91
ip igmp snooping tcn command 2-93
ip igmp snooping tcn flood command 2-95
ip igmp snooping vlan immediate-leave command 2-96
ip igmp snooping vlan static command 2-97
ip ssh command 2-99
ipv6 mld snooping command 2-101
ipv6 mld snooping last-listener-query count command 2-103
ipv6 mld snooping last-listener-query-interval command 2-105
ipv6 mld snooping listener-message-suppression command 2-107
ipv6 mld snooping robustness-variable command 2-109
ipv6 mld snooping tcn command 2-111
ipv6 mld snooping vlan command 2-113

J

jumbo frames
See MTU

L

lacp port-priority command 2-115
lacp system-priority command 2-117
Layer 2 protocol-tunnel
error detection for 2-57
error recovery timer 2-60
Layer 2 traceroute
IP addresses 2-409
MAC addresses 2-406

line configuration mode 1-2, 1-4
link flap
error detection for 2-57
error recovery timer 2-60
link state group command 2-119
link state track command 2-121
load-distribution methods for EtherChannel 2-157
location (global configuration) command 2-122
location (interface configuration) command 2-124
logging file command 2-126
logical interface 2-67
loopback error
detection for 2-57
recovery timer 2-60
loop guard, for spanning tree 2-349, 2-353

M

MAC addresses
displaying
aging time 2-279
all 2-277
dynamic 2-283
number of addresses in a VLAN 2-281
per interface 2-285
per VLAN 2-289
static 2-287
static and dynamic entries 2-275
dynamic
aging time 2-128
deleting 2-28
displaying 2-283
static
adding and removing 2-129
displaying 2-287
dropping on an interface 2-130
tables 2-277
mac address-table aging-time command 2-128
mac address-table static command 2-129
mac address-table static drop command 2-130
MAC frames
See MTU
macros
interface range 2-46, 2-69
maps
QoS
displaying 2-294
match (class-map configuration) command 2-132
maximum transmission unit
See MTU
mdix auto command 2-135
media-type rj45 command 2-137
member switches
See clusters
memory (boot loader) command A-14
mgmt_clr (boot loader) command A-16
mgmt_init (boot loader) command A-17, A-18
mkdir (boot loader) command A-19
MLD snooping
configuring 2-107, 2-109
configuring queries 2-103, 2-105
configuring topology change notification 2-111
displaying 2-258, 2-260, 2-262, 2-264
enabling 2-101
enabling on a VLAN 2-113
mls qos command 2-138
mls qos cos command 2-140
mls qos queue-set output buffers command 2-142
mls qos queue-set output threshold command 2-144
mls qos-srr-queue output cos-map command 2-146
mls qos trust command 2-148
Mode button, and password recovery 2-170
modes, commands 1-1
monitor session command 2-149
more (boot loader) command A-20
MSTP
displaying 2-305
interoperability 2-31

link type 2-351
MST region
aborting changes 2-357
applying changes 2-357
configuration name 2-357
configuration revision number 2-357
current or pending display 2-357
displaying 2-305
MST configuration mode 2-357
VLANs-to-instance mapping 2-357
path cost 2-359
protocol mode 2-355
restart protocol migration process 2-31
root port
loop guard 2-349
preventing from becoming designated 2-349
restricting which can be root 2-349
root guard 2-349
root switch
affects of extended system ID 2-347
hello-time 2-362, 2-369
interval between BDPU messages 2-363
interval between hello BPDU messages 2-362, 2-369
max-age 2-363
maximum hop count before discarding BPDU 2-364
port priority for selection of 2-365
primary or secondary 2-369
switch priority 2-368
state changes
blocking to forwarding state 2-376
enabling BPDU filtering 2-339, 2-373
enabling BPDU guard 2-341, 2-373
enabling Port Fast 2-373, 2-376
forward-delay time 2-361
length of listening and learning states 2-361
rapid transition to forwarding 2-351
shutting down Port Fast-enabled ports 2-373
state information display 2-304
MTU
configuring size 2-404
displaying global setting 2-310
MAC 2-404
Multicase Listener Discovery
See MLD
Multicast Listener Discovery
See MLD
multicast router ports, IPv6 2-113
Multiple Spanning Tree Protocol
See MSTP

N

native VLANs 2-400
nonegotiate
DTP messaging 2-398
speed 2-384
normal-range VLANs 2-417
no vlan command 2-417

O

online diagnostics
configuring health monitoring diagnostic tests 2-49
displaying
configured boot-up coverage level 2-207
current scheduled tasks 2-207
event logs 2-207
supported test suites 2-207
test ID 2-207
test results 2-207
test statistics 2-207
enabling
scheduling 2-51
syslog messages 2-49
global configuration mode

clearing health monitoring diagnostic test schedule 2-49

clearing test-based testing schedule 2-51

setting health monitoring diagnostic testing 2-49

setting test-based testing 2-51

setting up health monitoring diagnostic test schedule 2-49

setting up test-based testing 2-51

removing scheduling 2-51

scheduled switchover

disabling 2-51

enabling 2-51

setting test interval 2-51

specifying health monitoring diagnostic tests 2-49

starting testing 2-53

P

PAgP

See EtherChannel

pagp learn-method command 2-153

pagp port-priority command 2-155

password, VTP 2-422, 2-426

password-recovery mechanism, enabling and disabling 2-170

per-VLAN spanning-tree plus

See STP

physical-port learner 2-153

PID, displaying 2-247

policy maps

applying to an interface 2-172

Port Aggregation Protocol

See EtherChannel

port-channel load-balance command 2-157

Port Fast, for spanning tree 2-376

port ranges, defining 2-44, 2-46

ports, debugging B-44

port trust states for QoS 2-148

power information, displaying 2-216

priority-queue command 2-159

privileged EXEC mode 1-2, 1-3

product identification information, displaying 2-247

pruning

VLANs 2-400

VTP

displaying interface information 2-232

enabling 2-422, 2-426

pruning-eligible VLAN list 2-401

PVST+

See STP

Q

QoS

class maps

creating 2-22

defining the match criteria 2-132

displaying 2-184

defining the CoS value for an incoming packet 2-140

displaying configuration information 2-291

egress queues

allocating buffers 2-142

defining the CoS output queue threshold map 2-146

displaying buffer allocations 2-292

displaying CoS output queue threshold map 2-294

displaying DSCP output queue threshold map 2-294

displaying queueing strategy 2-292

displaying queue-set settings 2-297

enabling bandwidth shaping and scheduling 2-388

enabling bandwidth sharing and scheduling 2-390

limiting the maximum output on a port 2-386

mapping CoS values to a queue and threshold 2-146

setting maximum and reserved memory allocations 2-144

setting WTD thresholds 2-144
enabling 2-138
ingress queues
displaying buffer allocations 2-292
displaying CoS input queue threshold map 2-294
displaying DSCP input queue threshold map 2-294
displaying queueing strategy 2-292
maps
defining 2-146
displaying 2-294
policy maps
applying to an interface 2-172
port trust states 2-148
queues, enabling the expedite 2-159
statistics
in-profile and out-of-profile packets 2-292
packets enqueued or dropped 2-292
sent and received CoS values 2-292
sent and received DSCP values 2-292

R

radius-server dead-criteria command 2-161
radius-server host command 2-163
rapid per-VLAN spanning-tree plus
See STP
rapid PVST+
See STP
rcommand command 2-165
receiving flow-control packets 2-64
recovery mechanism
causes 2-60
display 2-25, 2-218, 2-221
timer interval 2-60
reload command 2-167
Remote Switched Port Analyzer
See RSPAN
rename (boot loader) command A-21
reset (boot loader) command A-22
rmdir (boot loader) command A-23
rmon collection stats command 2-169
root guard, for spanning tree 2-349
routing frames
See MTU
RSPAN
configuring 2-149
displaying 2-299
filter RSPAN traffic 2-149
sessions
add interfaces to 2-149
displaying 2-299
start new 2-149

S

scheduled switchover
disabling 2-51
enabling 2-51
sending flow-control packets 2-64
service password-recovery command 2-170
set (boot loader) command A-24
setup command 2-172
setup express command 2-175
show access-lists command 2-177
show archive status command 2-180
show boot command 2-181
show class-map command 2-184
show cluster candidates command 2-187
show cluster command 2-185
show cluster members command 2-189
show controllers cpu-interface command 2-191
show controllers ethernet-controller command 2-193
show controllers ethernet-controller fastethernet command 2-201
show controllers tcam command 2-203
show controller utilization command 2-205
show dtp 2-211

show eap command 2-213
show env command 2-216
show errdisable detect command 2-218
show errdisable flap-values command 2-220
show errdisable recovery command 2-221
show etherchannel command 2-223
show fallback profile command 2-226
show flowcontrol command 2-228
show idprom command 2-230
show interfaces command 2-232
show interfaces counters command 2-241
show interface transceivers command 2-243
show inventory command 2-247
show ip igmp profile command 2-248
show ip igmp snooping address command 2-260
show ip igmp snooping command 2-249, 2-258
show ip igmp snooping groups command 2-252
show ip igmp snooping mrouter command 2-254, 2-262
show ip igmp snooping querier command 2-256, 2-264
show lacp command 2-266
show link state group command 2-270
show location 2-272
show location command 2-272
show mac address-table address command 2-277
show mac address-table aging time command 2-279
show mac address-table command 2-275
show mac address-table count command 2-281
show mac address-table dynamic command 2-283
show mac address-table interface command 2-285
show mac address-table notification command B-14
show mac address-table static command 2-287
show mac address-table vlan command 2-289
show mls qos command 2-291
show mls qos interface command 2-292
show mls qos maps command 2-294
show mls qos queue-set command 2-297
show monitor command 2-299
show pagp command 2-301
show platform acl command C-2
show platform dl command C-3
show platform etherchannel command C-4
show platform forward command C-5
show platform frontend-controller command C-7
show platform igmp snooping command C-8
show platform layer4op command C-10
show platform mac-address-table command C-11
show platform messaging command C-12
show platform monitor command C-13
show platform pm command C-14
show platform port-asic command C-15
show platform qos command C-20
show platform resource-manager command C-21
show platform snmp counters command C-23
show platform spanning-tree synchronization command C-24
show platform stp-instance command C-25
show platform tcam command C-26
show platform vlan command C-28
show setup express command 2-303
show spanning-tree command 2-304
show system mtu command 2-310
show udld command 2-311
show version command 2-314
show vlan command 2-316
show vlan command, fields 2-318
show vtp command 2-320
shutdown command 2-325
shutdown vlan command 2-326
small-frame violation rate command 2-327
SNMP host, specifying 2-332
SNMP informs, enabling the sending of 2-329
snmp-server enable traps command 2-329
snmp-server host command 2-332
snmp trap mac-notification command 2-336
SNMP traps
  enabling MAC address notification trap 2-336
  enabling the sending of 2-329
software images

deleting 2-48
downloading 2-3
upgrading 2-3
uploading 2-9
software version, displaying 2-314
SPAN
configuring 2-149
debug messages, display B-15
displaying 2-299
filter SPAN traffic 2-149
sessions
add interfaces to 2-149
displaying 2-299
start new 2-149
spanning-tree backbonefast command 2-338
spanning-tree bpdufilter command 2-339
spanning-tree bpduguard command 2-341
spanning-tree cost command 2-343
spanning-tree etherchannel command 2-345
spanning-tree extend system-id command 2-347
spanning-tree guard command 2-349
spanning-tree link-type command 2-351
spanning-tree loopguard default command 2-353
spanning-tree mode command 2-355
spanning-tree mst configuration command 2-357
spanning-tree mst cost command 2-359
spanning-tree mst forward-time command 2-361
spanning-tree mst hello-time command 2-362
spanning-tree mst max-age command 2-363
spanning-tree mst max-hops command 2-364
spanning-tree mst port-priority command 2-365
spanning-tree mst pre-standard command 2-367
spanning-tree mst priority command 2-368
spanning-tree mst root command 2-369
spanning-tree portfast (global configuration) command 2-373
spanning-tree portfast (interface configuration) command 2-376
spanning-tree port-priority command 2-371
Spanning Tree Protocol
See STP
spanning-tree transmit hold-count command 2-378
spanning-tree uplinkfast command 2-379
spanning-tree vlan command 2-381
speed command 2-384
srr-queue bandwidth limit command 2-386
srr-queue bandwidth shape command 2-388
srr-queue bandwidth share command 2-390
SSH, configuring version 2-99
static-access ports, configuring 2-392
statistics, Ethernet group 2-169
STP
BackboneFast 2-338
counters, clearing 2-30
debug messages, display
BackboneFast events B-49
MSTP B-52
optimized BPDUs handling B-51
spanning-tree activity B-47
switch shim B-54
transmitted and received BPDUs B-50
UplinkFast B-56
detection of indirect link failures 2-338
EtherChannel misconfiguration 2-345
extended system ID 2-347
path cost 2-343
protocol modes 2-355
root port
accelerating choice of new 2-379
loop guard 2-349
preventing from becoming designated 2-349
restricting which can be root 2-349
root guard 2-349
UplinkFast 2-379
root switch
affects of extended system ID 2-347, 2-382
hello-time 2-381
interval between BDPU messages 2-381

interval between hello BPDU messages 2-381
max-age 2-381
port priority for selection of 2-371
primary or secondary 2-381
switch priority 2-381
state changes
blocking to forwarding state 2-376
enabling BPDU filtering 2-339, 2-373
enabling BPDU guard 2-341, 2-373
enabling Port Fast 2-373, 2-376
enabling timer to recover from error state 2-60
forward-delay time 2-381
length of listening and learning states 2-381
shutting down Port Fast-enabled ports 2-373
state information display 2-304
VLAN options 2-368, 2-381
SVIs, creating 2-72
SVI status calculation 2-393
Switched Port Analyzer
See SPAN
switchport access command 2-392
switchport autostate exclude command 2-393
switchport host command 2-395
switchport mode command 2-396
switchport nonegotiate command 2-398
switchports, displaying 2-232
switchport trunk command 2-400
system env temperature threshold yellow command 2-403
system message logging, save message to flash 2-126
system mtu command 2-404

T

tar files, creating, listing, and extracting 2-6
Telnet, using to communicate to cluster switches 2-165
temperature information, displaying 2-216
traceroute mac command 2-406
traceroute mac ip command 2-409
trunking, VLAN mode 2-396
trunk mode 2-396
trunk ports 2-396
trunks, to non-DTP device 2-397
trusted port states for QoS 2-148
type (boot loader) command A-27

U

UDLD
aggressive mode 2-411, 2-413
debug messages, display B-64
enable globally 2-411
enable per interface 2-413
error recovery timer 2-60
message timer 2-411
normal mode 2-411, 2-413
reset a shutdown interface 2-415
status 2-311
udld command 2-411
udld port command 2-413
udld reset command 2-415
UniDirectional Link Detection
See UDLD
unset (boot loader) command A-28
upgrading
downloading software images 2-3
software images, monitoring status of 2-180
UplinkFast, for STP 2-379
usb-inactivity-timeout (console configuration) command 2-416
user EXEC mode 1-2

V

version (boot loader) command A-30
vlan (global configuration) command 2-417
VLAN configuration
rules 2-420
saving 2-417

VLAN configuration mode
commands
VTP 2-426
VLAN ID range 2-417
VLANs
adding 2-417
configuring 2-417
debug messages, display
ISL B-60
VLAN IOS file system error tests B-59
VLAN manager activity B-57
VTP B-62
displaying configurations 2-316
extended-range 2-417
MAC addresses
displaying 2-289
number of 2-281
media types 2-419
normal-range 2-417
restarting 2-326
saving the configuration 2-417
shutting down 2-326
SNMP traps for VTP 2-330, 2-333
suspending 2-326
VLAN Trunking Protocol
See VTP
VTP
changing characteristics 2-422
clearing pruning counters 2-32
configuring
domain name 2-422, 2-426
file name 2-422
mode 2-422, 2-426
password 2-422, 2-426
counters display fields 2-321
displaying information 2-320
enabling
pruning 2-422, 2-426
Version 2 2-422, 2-426
mode 2-422, 2-426
pruning 2-422, 2-426
saving the configuration 2-417
statistics 2-320
status 2-320
status display fields 2-322
vtp (global configuration) command 2-422
vtp (VLAN configuration) command 2-426