



Consolidated Platform Command Reference, Cisco IOS Release 15.2(6)E (Catalyst 2960-X Switches)

First Published: 2017-08-08

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



CONTENTS

CHAPTER 1

Using the Command-Line Interface 1

- Using the Command-Line Interface 2
- Understanding Command Modes 2
- Understanding the Help System 3
- Understanding Abbreviated Commands 4
- Understanding no and default Forms of Commands 4
- Understanding CLI Error Messages 4
- Using Configuration Logging 5
- Using Command History 5
 - Changing the Command History Buffer Size 5
 - Recalling Commands 6
 - Disabling the Command History Feature 6
- Using Editing Features 6
 - Enabling and Disabling Editing Features 7
 - Editing Commands through Keystrokes 7
 - Editing Command Lines that Wrap 9
- Searching and Filtering Output of show and more Commands 10
- Accessing the CLI 10
 - Accessing the CLI through a Console Connection or through Telnet 11

PART I

IGMP Snooping and MVR 13

CHAPTER 2

IGMP Snooping and MVR Commands 15

- ip igmp snooping 16
- ip igmp snooping last-member-query-count 17
- ip igmp snooping last-member-query-interval 19

- ip igmp snooping querier 20
- ip igmp snooping report-suppression 22
- ip igmp snooping robustness-variable 23
- ip igmp snooping vlan immediate-leave 24
- ip igmp snooping vlan mrouter 25
- ip igmp snooping vlan static 27
- mvr (global configuration) 28
- mvr (interface configuration) 31
- show ip igmp snooping 34
- show ip igmp snooping groups 36
- show ip igmp snooping mrouter 38
- show ip igmp snooping querier 39
- show mvr 41
- show mvr interface 42
- show mvr members 44

PART II

Interface and Hardware 47

CHAPTER 3

Interface and Hardware Commands 49

- debug fastethernet 51
- debug ilpower 52
- debug interface 53
- debug lldp packets 54
- debug nmsp 55
- duplex 56
- errdisable detect cause 58
- errdisable detect cause small-frame 60
- errdisable recovery cause 61
- errdisable recovery cause small-frame 64
- errdisable recovery interval 65
- lldp (interface configuration) 66
- mdix auto 67
- network-policy 68
- network-policy profile (global configuration) 69

nmsp attachment suppress	70
power efficient-ethernet auto	71
power inline	72
power inline consumption	75
power inline police	78
show eee	80
show env	83
show errdisable detect	85
show errdisable recovery	86
show interfaces	87
show interfaces counters	92
show interfaces switchport	94
show interfaces transceiver	98
show ip ports all	101
show network-policy profile	102
show power inline	103
show system mtu	108
speed	109
switchport backup interface	111
switchport block	113
system mtu	114
voice-signaling vlan (network-policy configuration)	115
voice vlan (network-policy configuration)	117

PART III
Layer 2 119

CHAPTER 4
Layer 2 Commands 121

channel-group	123
channel-protocol	127
clear lacp	128
clear pagp	129
clear spanning-tree counters	130
clear spanning-tree detected-protocols	131
debug etherchannel	132

debug lacp	133
debug pagp	134
debug platform etherchannel	135
debug platform pm	136
debug spanning-tree	138
debug platform udld	140
interface port-channel	141
lacp port-priority	143
lacp system-priority	145
link state group	146
link state track	147
pagp learn-method	148
pagp port-priority	150
pagp timer	151
port-channel load-balance	152
rep admin vlan	153
rep block port	154
rep lsl-age-timer	156
rep preempt delay	157
rep preempt segment	158
rep segment	159
rep stcn	161
show etherchannel	162
show interfaces rep detail	165
show lacp	166
show link state group	170
show pagp	171
show platform backup interface	173
show platform etherchannel	174
show platform pm	175
show platform spanning-tree	176
show rep topology	177
show spanning-tree	179
show udld	183

spanning-tree backbonefast	186
spanning-tree bpdufilter	187
spanning-tree bpduguard	188
spanning-tree bridge assurance	189
spanning-tree cost	191
spanning-tree etherchannel guard misconfig	192
spanning-tree extend system-id	193
spanning-tree guard	194
spanning-tree link-type	196
spanning-tree loopguard default	197
spanning-tree mode	198
spanning-tree mst configuration	199
spanning-tree mst cost	201
spanning-tree mst forward-time	202
spanning-tree mst hello-time	203
spanning-tree mst max-age	204
spanning-tree mst max-hops	205
spanning-tree mst port-priority	206
spanning-tree mst pre-standard	207
spanning-tree mst priority	208
spanning-tree mst root	209
spanning-tree mst simulate pvst (global configuration)	210
spanning-tree mst simulate pvst (interface configuration)	212
spanning-tree pathcost method	214
spanning-tree port-priority	215
spanning-tree portfast edge (global configuration)	216
spanning-tree portfast edge (interface configuration)	218
spanning-tree transmit hold-count	220
spanning-tree uplinkfast	221
spanning-tree vlan	223
switchport access vlan	225
switchport mode	227
switchport nonegotiate	229
udld	230

udld port 232
udld reset 234

PART IV**NetFlow Lite 235**

CHAPTER 5**NetFlow Lite Commands 237**

cache 239
clear flow exporter 242
clear flow monitor 243
collect counter 245
collect flow sampler 246
collect interface 247
collect timestamp sys-uptime 248
collect transport tcp flags 249
datalink flow monitor 251
debug flow exporter 252
debug flow monitor 253
debug sampler 254
description 255
destination 256
dscp 257
export-protocol netflow-v9 258
exporter 259
flow exporter 260
flow monitor 261
flow record 262
ip flow monitor 263
ipv6 flow monitor 264
match datalink ethertype 265
match datalink mac 266
match ipv4 267
match ipv4 destination address 268
match ipv4 source address 269
match ipv6 270

- match ipv6 destination address 271
- match ipv6 source address 272
- match transport 273
- mode 274
- option 276
- record 278
- sampler 279
- show flow exporter 280
- show flow interface 282
- show flow monitor 284
- show flow record 290
- show sampler 291
- source 293
- statistics packet protocol 295
- template data timeout 296
- transport 297
- ttl 298

PART V
Network Management 299

CHAPTER 6
Network Management 301

- monitor session 302
- monitor session destination 304
- monitor session filter 308
- monitor session source 310
- show monitor 313
- snmp-server enable traps 316
- snmp-server enable traps bridge 319
- snmp-server enable traps cpu 320
- snmp-server enable traps envmon 321
- snmp-server enable traps errdisable 322
- snmp-server enable traps flash 323
- snmp-server enable traps mac-notification 324
- snmp-server enable traps port-security 325

snmp-server enable traps rtr 326
 snmp-server enable traps snmp 328
 snmp-server enable traps storm-control 329
 snmp-server enable traps stpx 330

PART VI
QoS 331

CHAPTER 7
Auto-QoS 333

auto qos classify 334
 auto qos trust 337
 auto qos video 341
 auto qos voip 346
 debug auto qos 351
 show auto qos 354

CHAPTER 8
QoS 359

class 360
 class-map 362
 debug qos 364
 match (class-map configuration) 366
 mls qos 368
 mls qos aggregate-policer 370
 mls qos cos 372
 mls qos dscp-mutation 374
 mls qos map 376
 mls qos queue-set output buffers 377
 mls qos queue-set output threshold 379
 mls qos rewrite ip dscp 382
 mls qos srr-queue output cos-map 384
 mls qos srr-queue output dscp-map 386
 mls qos trust 388
 police 390
 police aggregate 392
 policy map 394

queue-set	396
service-policy	397
set	398
show class-map	400
show mls qos	401
show mls qos aggregate-policer	402
show mls qos interface	403
show mls qos maps	407
show mls qos queue-set	410
show policy-map	411
srr-queue bandwidth limit	412
srr-queue bandwidth shape	414
srr-queue bandwidth share	416
trust	418

PART VII**Security 421**

CHAPTER 9**Security 423**

aaa accounting dot1x	425
aaa accounting identity	427
aaa authentication dot1x	429
aaa authorization network	430
aaa new-model	431
authentication host-mode	433
authentication mac-move permit	435
authentication priority	436
authentication violation	439
auto security	441
auto security-port	442
cisp enable	443
clear errdisable interface vlan	444
clear mac address-table	445
debug ip rip	447
deny (MAC access-list configuration)	449

device-role (IPv6 snooping)	453
device-role (IPv6 nd inspection)	454
device-tracking policy	455
dot1x critical (global configuration)	457
dot1x pae	458
dot1x supplicant force-multicast	459
dot1x test eapol-capable	460
dot1x test timeout	461
dot1x timeout	462
epm access-control open	464
ip admission	465
ip admission name	466
ip device tracking maximum	468
ip device tracking probe	469
ip dhcp snooping database	470
ip dhcp snooping information option format remote-id	472
ip dhcp snooping verify no-relay-agent-address	473
ip source binding	474
ip verify source	475
ipv6 snooping policy	477
limit address-count	478
mab request format attribute 32	479
match (access-map configuration)	481
mls qos copp protocol	483
authentication logging verbose	487
dot1x logging verbose	488
mab logging verbose	489
permit (MAC access-list configuration)	490
protocol (IPv6 snooping)	494
radius server	495
router rip	497
security level (IPv6 snooping)	498
show aaa acct-stop-cache	499
show aaa clients	500

show aaa command handler	501
show aaa local	502
show aaa servers	503
show aaa sessions	504
show authentication sessions	505
show auto security	508
show cisp	510
show dot1x	512
show eap pac peer	514
show ip dhcp snooping statistics	515
show ip rip database	518
show mls qos copp protocols	520
show radius server-group	521
show vlan group	523
switchport port-security aging	524
switchport port-security mac-address	526
switchport port-security maximum	528
switchport port-security violation	530
tracking (IPv6 snooping)	532
trusted-port	534
vlan access-map	535
vlan filter	537
vlan group	538

PART VIII
Stack Manager 539

CHAPTER 10
Stack Manager Commands 541

debug platform remote-commands	542
debug platform stack-manager	543
reload	544
remote command	546
session	547
show platform stack compatibility configuration	548
show platform stack compatibility feature	549

show platform stack compatibility table	551
show platform stack manager	553
show switch	555
stack-mac persistent timer	558
switch stack port	561
switch priority	563
switch provision	564
switch renumber	566
switch stack port-speed 10	567

PART IX
System Management 569

CHAPTER 11
System Management Commands 571

archive download-sw	574
archive tar	578
archive upload-sw	582
avc dns-as client	584
show logging smartlog	586
boot	588
boot buffersize	589
boot enable-break	590
boot host dhcp	591
boot host retry timeout	592
boot manual	593
boot system	594
cat	595
clear logging onboard	596
clear mac address-table	597
clear mac address-table move update	598
clear nmsp statistics	599
cluster commander-address	600
cluster discovery hop-count	602
cluster enable	603
cluster holdtime	604

cluster member	605
cluster outside-interface	607
cluster run	608
cluster timer	609
copy	610
debug cluster	611
debug matm move update	612
delete	613
dir	614
help	616
hw-module	617
ip name-server	619
license boot level	621
logging	622
logging buffered	623
logging console	624
logging file flash	625
logging history	626
logging history size	627
logging monitor	628
logging trap	629
mac address-table aging-time	630
mac address-table learning vlan	631
logging smartlog	633
mac address-table notification	634
mac address-table static	635
mkdir	636
more	637
nmsp notification interval	638
rcommand	640
rename	642
reset	643
rmdir	644
service sequence-numbers	645

set	646
show avc dns-as client	649
show boot	652
show cable-diagnostics prbs	654
show cable-diagnostics tdr	656
show cluster	658
show cluster candidates	660
show cluster members	662
show ip name-server	664
show license right-to-use	665
show logging onboard	668
show mac address-table	673
show mac address-table address	674
show mac address-table aging-time	675
show mac address-table count	676
show mac address-table dynamic	677
show mac address-table interface	678
show mac address-table learning	679
show mac address-table move update	680
show mac address-table multicast	681
show mac address-table notification	682
show mac address-table secure	684
show mac address-table static	685
show mac address-table vlan	686
show nmsp	687
show onboard switch	688
shutdown	690
test cable-diagnostics prbs	691
test cable-diagnostics tdr	692
traceroute mac	693
traceroute mac ip	696
type	698
unset	699
version	701

PART X**VLANs 703**

CHAPTER 12**VLAN 705**

- client vlan 706
- clear vmps statistics 707
- clear vtp counters 708
- debug platform vlan 709
- debug sw-vlan 710
- debug sw-vlan ifs 712
- debug sw-vlan notification 713
- debug sw-vlan vtp 715
- interface vlan 717
- show platform vlan 719
- show vlan 720
- show vmps 723
- show vtp 725
- switchport priority extend 731
- switchport trunk 732
- switchport voice vlan 735
- vlan 738
- vmps reconfirm (global configuration) 744
- vmps reconfirm (privileged EXEC) 745
- vmps retry 746
- vmps server 747
- vtp (global configuration) 749
- vtp (interface configuration) 754
- vtp primary 755



Using the Command-Line Interface

This chapter contains the following topics:

- [Using the Command-Line Interface, on page 2](#)

Using the Command-Line Interface

This chapter describes the Cisco IOS command-line interface (CLI) and how to use it to configure your switch.

Understanding Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

When you start a session on the switch, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the switch reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the switch reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the hostname *Switch*.

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch.	Switch>	Enter logout or quit .	Use this mode to <ul style="list-style-type: none"> • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the enable command.	Device#	Enter disable to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the configure command.	Device(config)#	To exit to privileged EXEC mode, enter exit or end , or press Ctrl-Z .	Use this mode to configure parameters that apply to the entire switch.

Mode	Access Method	Prompt	Exit Method	About This Mode
VLAN configuration	While in global configuration mode, enter the vlan <i>vlan-id</i> command.	Device (config-vlan) #	To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
Interface configuration	While in global configuration mode, enter the interface command (with a specific interface).	Device (config-if) #	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the Ethernet ports.
Line configuration	While in global configuration mode, specify a line with the line vty or line console command.	Device (config-line) #	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the terminal line.

For more detailed information on the command modes, see the command reference guide for this release.

Understanding the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

Table 2: Help Summary

Command	Purpose
help	Obtains a brief description of the help system in any command mode.
<i>abbreviated-command-entry ?</i> Device# di? dir disable disconnect	Obtains a list of commands that begin with a particular character string.

Command	Purpose
<p><i>abbreviated-command-entry</i> <Tab></p> <pre>Device# sh conf<tab> Device# show configuration</pre>	Completes a partial command name.
<p>?</p> <pre>Switch> ?</pre>	Lists all commands available for a particular command mode.
<p><i>command ?</i></p> <pre>Switch> show ?</pre>	Lists the associated keywords for a command.
<p><i>command keyword ?</i></p> <pre>Device(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet</pre>	Lists the associated arguments for a keyword.

Understanding Abbreviated Commands

You need to enter only enough characters for the switch to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Device# show conf
```

Understanding no and default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

Understanding CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your switch.

Table 3: Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for your switch to recognize the command.	Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
% Incomplete command.	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
% Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Using Configuration Logging

You can log and view changes to the switch configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.



Note Only CLI or HTTP changes are logged.

Using Command History

The software provides a history or record of commands that you have entered. The command history feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize this feature to suit your needs.

Changing the Command History Buffer Size

By default, the switch records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. These procedures are optional.

Beginning in privileged EXEC mode, enter this command to change the number of command lines that the switch records during the current terminal session:

```
Device# terminal history [size number-of-lines]
```

The range is from 0 to 256.

Beginning in line configuration mode, enter this command to configure the number of command lines the switch records for all sessions on a particular line:

```
Device(config-line)# history [size number-of-lines]
```

The range is from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in this table. These actions are optional.



Note

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

Table 4: Recalling Commands

Action	Result
Press Ctrl-P or the up arrow key.	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press Ctrl-N or the down arrow key.	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.
show history Device(config)# help	While in privileged EXEC mode, lists the last several commands that you just entered. The number of commands that appear is controlled by the setting of the terminal history global configuration command and the history line configuration command.

Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. These procedures are optional.

To disable the feature during the current terminal session, enter the **terminal no history** privileged EXEC command.

To disable command history for the line, enter the **no history** line configuration command.

Using Editing Features

This section describes the editing features that can help you manipulate the command line.

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it, re-enable it, or configure a specific line to have enhanced editing. These procedures are optional.

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
Switch (config-line)# no editing
```

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
Device# terminal editing
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
Device (config-line)# editing
```

Editing Commands through Keystrokes

This table shows the keystrokes that you need to edit command lines. These keystrokes are optional.



Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

Table 5: Editing Commands through Keystrokes

Capability	Keystroke	Purpose
Move around the command line to make changes or corrections.	Press Ctrl-B , or press the left arrow key.	Moves the cursor back one character.
	Press Ctrl-F , or press the right arrow key.	Moves the cursor forward one character.
	Press Ctrl-A .	Moves the cursor to the beginning of the command line.
	Press Ctrl-E .	Moves the cursor to the end of the command line.
	Press Esc B .	Moves the cursor back one word.
	Press Esc F .	Moves the cursor forward one word.
	Press Ctrl-T .	Transposes the character to the left of the cursor with the character located at the cursor.

Capability	Keystroke	Purpose
Recall commands from the buffer and paste them in the command line. The switch provides a buffer with the last ten items that you deleted.	Press Ctrl-Y .	Recalls the most recent entry in the buffer.
	Press Esc Y .	Recalls the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press Esc Y more than ten times, you cycle to the first buffer entry.
Delete entries if you make a mistake or change your mind.	Press the Delete or Backspace key.	Erases the character to the left of the cursor.
	Press Ctrl-D .	Deletes the character at the cursor.
	Press Ctrl-K .	Deletes all characters from the cursor to the end of the command line.
	Press Ctrl-U or Ctrl-X .	Deletes all characters from the cursor to the beginning of the command line.
	Press Ctrl-W .	Deletes the word to the left of the cursor.
	Press Esc D .	Deletes from the cursor to the end of the word.
Capitalize or lowercase words or capitalize a set of letters.	Press Esc C .	Capitalizes at the cursor.
	Press Esc L .	Changes the word at the cursor to lowercase.
	Press Esc U .	Capitalizes letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	Press Ctrl-V or Esc Q .	

Capability	Keystroke	Purpose
Scroll down a line or screen on displays that are longer than the terminal screen can display. Note The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including show command output. You can use the Return and Space bar keystrokes whenever you see the More prompt.	Press the Return key.	Scrolls down one line.
	Press the Space bar.	Scrolls down one screen.
Redisplay the current command line if the switch suddenly sends a message to your screen.	Press Ctrl-L or Ctrl-R .	Redisplays the current command line.

Editing Command Lines that Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.



Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

In this example, the **access-list** global configuration command entry extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign (\$) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

```
Device(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Device(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
Device(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
Device(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

After you complete the entry, press **Ctrl-A** to check the complete syntax before pressing the **Return** key to execute the command. The dollar sign (\$) appears at the end of the line to show that the line has been scrolled to the right:

```
Device(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The software assumes that you have a terminal screen that is 80 columns wide. If you have a width other than that, use the **terminal width** privileged EXEC command to set the width of your terminal.

Use line wrapping with the command history feature to recall and modify previous complex command entries.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

To use this functionality, enter a **show** or **more** command followed by the pipe character (`|`), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search for or filter out:

```
command | {begin | include | exclude} regular-expression
```

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.

This example shows how to include in the output display only lines where the expression *protocol* appears:

```
Device# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet1/0/1 is up, line protocol is down
GigabitEthernet1/0/2 is up, line protocol is up
```

Accessing the CLI

You can access the CLI through a console connection, through Telnet, or by using the browser.

You manage the switch stack and the switch member interfaces through the active switch. You cannot manage switch stack members on an individual switch basis. You can connect to the active switch through the console port or the Ethernet management port of one or more switch members. Be careful with using multiple CLI sessions to the active switch. Commands you enter in one session are not displayed in the other sessions. Therefore, it is possible to lose track of the session from which you entered commands.



Note We recommend using one CLI session when managing the switch stack.

If you want to configure a specific switch member port, you must include the switch member number in the CLI command interface notation.

To debug a specific switch member, you can access it from the active switch by using the **session stack-member-number** privileged EXEC command. The switch member number is appended to the system prompt. For example, *Switch-2#* is the prompt in privileged EXEC mode for switch member 2, and where the system prompt for the active switch is *Switch*. Only the **show** and **debug** commands are available in a CLI session to a specific switch member.

Accessing the CLI through a Console Connection or through Telnet

Before you can access the CLI, you must connect a terminal or a PC to the switch console or connect a PC to the Ethernet management port and then power on the switch, as described in the hardware installation guide that shipped with your switch.

CLI access is available before switch setup. After your switch is configured, you can access the CLI through a remote Telnet session or SSH client.

You can use one of these methods to establish a connection with the switch:

- Connect the switch console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the switch hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The switch must have network connectivity with the Telnet or SSH client, and the switch must have an enable secret password configured.

The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.

The switch supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.



PART **I**

IGMP Snooping and MVR

- [IGMP Snooping and MVR Commands, on page 15](#)



IGMP Snooping and MVR Commands

This chapter contains IGMP snooping and MVR commands.

- [ip igmp snooping](#), on page 16
- [ip igmp snooping last-member-query-count](#), on page 17
- [ip igmp snooping last-member-query-interval](#), on page 19
- [ip igmp snooping querier](#), on page 20
- [ip igmp snooping report-suppression](#), on page 22
- [ip igmp snooping robustness-variable](#), on page 23
- [ip igmp snooping vlan immediate-leave](#), on page 24
- [ip igmp snooping vlan mrouter](#), on page 25
- [ip igmp snooping vlan static](#), on page 27
- [mvr \(global configuration\)](#), on page 28
- [mvr \(interface configuration\)](#), on page 31
- [show ip igmp snooping](#), on page 34
- [show ip igmp snooping groups](#), on page 36
- [show ip igmp snooping mrouter](#), on page 38
- [show ip igmp snooping querier](#), on page 39
- [show mvr](#), on page 41
- [show mvr interface](#), on page 42
- [show mvr members](#), on page 44

ip igmp snooping

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

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

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

Syntax Description	vlan <i>vlan-id</i> (Optional) Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.	
Command Default	IGMP snooping is globally enabled on the device. IGMP snooping is enabled on VLAN interfaces.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

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

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

Example

The following example shows how to globally enable IGMP snooping:

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

The following example shows how to enable IGMP snooping on VLAN 1:

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

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

ip igmp snooping last-member-query-count

To configure how often Internet Group Management Protocol (IGMP) snooping will send query messages in response to receiving an IGMP leave message, use the **ip igmp snooping last-member-query-count** command in global configuration mode. To set *count* to the default value, use the **no** form of this command.

```
ip igmp snooping [vlan vlan-id] last-member-query-count count
no ip igmp snooping [vlan vlan-id] last-member-query-count count
```

Syntax Description	vlan <i>vlan-id</i> (Optional) Sets the count value on a specific VLAN ID. The range is from 1—1001. Do not enter leading zeroes.	
	<i>count</i> Interval at which query messages are sent, in milliseconds. The range is from 1—7. The default is 2.	
Command Default	A query is sent every 2 milliseconds.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines When a multicast host leaves a group, the host sends an IGMP leave message. To check if this host is the last to leave the group, IGMP query messages are sent when the leave message is seen until the **last-member-query-interval** timeout period expires. If no response is received to the last-member queries before the timeout period expires, the group record is deleted.

Use the **ip igmp snooping last-member-query-interval** command to configure the timeout period.

When both IGMP snooping immediate-leave processing and the query count are configured, immediate-leave processing takes precedence.



Note Do not set the count to 1 because the loss of a single packet (the query packet from the device to the host or the report packet from the host to the device) may result in traffic forwarding being stopped even if the receiver is still there. Traffic continues to be forwarded after the next general query is sent by the device, but the interval during which a receiver may not receive the query could be as long as 1 minute (with the default query interval).

The leave latency in Cisco IOS software may increase by up to 1 last-member query interval (LMQI) value when the device is processing more than one leave within an LMQI. In such a scenario, the average leave latency is determined by the $(\text{count} + 0.5) * \text{LMQI}$. The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 milliseconds and a count of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.

Example

The following example shows how to set the last member query count to 5:

```
Device(config)# ip igmp snooping last-member-query-count 5
```

ip igmp snooping last-member-query-interval

To enable the Internet Group Management Protocol (IGMP) configurable-leave timer globally or on a per-VLAN basis, use the **ip igmp snooping last-member-query-interval** command in global configuration mode. Use the **no** form of the 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 time
```

Syntax Description	vlan <i>vlan-id</i> (Optional) Enables IGMP snooping and the leave timer on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.						
	<i>time</i> Interval time out in seconds. The range is 100 to 32767 milliseconds.						
Command Default	The default timeout setting is 1000 milliseconds.						
Command Modes	Global configuration						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)E</td> <td>Cisco IOS Release 15.2(5)E</td> </tr> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E		This command was introduced.
Release	Modification						
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E						
	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:

```
Device(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:

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

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

```
Device(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.

ip igmp snooping querier

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

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

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

Syntax Description		
vlan <i>vlan-id</i>	(Optional) Enables IGMP snooping and the IGMP querier function on the specified VLAN. Ranges are 1—1001 and 1006—4094.	
address <i>ip-address</i>	(Optional) Specifies 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 <i>response-time</i>	(Optional) Sets the maximum time to wait for an IGMP querier report. The range is 1—25 seconds.	
query-interval <i>interval-count</i>	(Optional) Sets the interval between IGMP queriers. The range is 1—18000 seconds.	
tcn query	(Optional) Sets parameters related to Topology Change Notifications (TCNs).	
count <i>count</i>	Sets the number of TCN queries to be executed during the TCN interval time. The range is 1—10.	
interval <i>interval</i>	Sets the TCN query interval time. The range is 1—255.	
timer expiry <i>expiry-time</i>	(Optional) Sets the length of time until the IGMP querier expires. The range is 60—300 seconds.	
version <i>version</i>	(Optional) Selects the IGMP version number that the querier feature uses. Select either 1 or 2.	

Command Default The IGMP snooping querier feature is globally disabled on the device.
When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast router.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

Example

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

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

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

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

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

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

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

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

The following example shows how to set the IGMP snooping querier timeout value to 60 seconds:

```
Device(config)# ip igmp snooping querier timer expiry 60
```

The following example shows how to set the IGMP snooping querier feature to Version 2:

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

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

ip igmp snooping report-suppression

To enable Internet Group Management Protocol (IGMP) report suppression, use the **ip igmp snooping report-suppression** global configuration command on the device stack or on a standalone device. To disable IGMP report suppression, and to forward all IGMP reports to multicast routers, use the **no** form of this command.

ip igmp snooping report-suppression
no ip igmp snooping report-suppression

Syntax Description This command has no arguments or keywords.

Command Default IGMP report suppression is enabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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 device uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP report suppression is enabled (the default), the device sends the first IGMP report from all the hosts for a group to all the multicast routers. The device 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 device forwards only the first IGMPv1 or IGMPv2 report from all the hosts for a group to all of the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the device 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 of the multicast routers.

Example

The following example shows how to disable report suppression:

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

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

ip igmp snooping robustness-variable

To configure the IGMP robustness variable globally or on a per-VLAN basis, use the **ip igmp snooping robustness-variable** command in global configuration mode. Use the **no** form of the command to return to the default setting.

```
ip igmp snooping [vlan vlan-id] robustness-variable number
no ip igmp snooping [vlan vlan-id] robustness-variable number
```

Syntax Description	vlan <i>vlan-id</i> (Optional) Enables IGMP snooping and the leave timer on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.				
	<i>number</i> Robustness variable number. The range is 1 to 3.				
Command Default	None				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th data-bbox="386 884 477 911">Release</th> <th data-bbox="1154 884 1292 911">Modification</th> </tr> </thead> <tbody> <tr> <td data-bbox="386 938 1005 966">Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E</td> <td data-bbox="1154 938 1487 966">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.				

ip igmp snooping vlan immediate-leave

To enable IGMPv2 immediate leave processing, use the **immediate-leave** global configuration command on the device stack or on a standalone device. To return to the default settings, use the **no** form of this command.

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

Syntax Description	<i>vlan-id</i> Enables IGMPv2 immediate leave processing in the specified VLAN. The range is 1 to 1001 and 1006 to 4094.	
Command Default	By default, IGMPv2 immediate leave processing is off.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.
Usage Guidelines	You can verify your settings by entering the show ip igmp snooping privileged EXEC command.	

ip igmp snooping vlan mrouter

To add a multicast router port or to configure the multicast learning method, use the **ip igmp snooping mrouter** global configuration command on the device stack or on a standalone device. To return to the default settings, use the **no** form of this command.

```
ip igmp snooping vlan vlan-id mrouter {interface interface-id | learn {cgmp | pim-dvmrp} }
no ip igmp snooping vlan vlan-id mrouter {interface interface-id | learn {cgmp | pim-dvmrp} }
```

Syntax Description

<i>vlan-id</i>	Enables IGMP snooping and adds the port in the specified VLAN as the multicast router port. Ranges are 1—1001 and 1006—4094.
interface <i>interface-id</i>	Specifies the next-hop interface to the multicast router. The <i>interface-id</i> value has these options: <ul style="list-style-type: none"> • <i>fastethernet interface number</i>—A Fast Ethernet IEEE 802.3 interface. • <i>gigabitethernet interface number</i>—A Gigabit Ethernet IEEE 802.3z interface. • <i>tengigabitethernet interface number</i>—A 10-Gigabit Ethernet IEEE 802.3z interface. • <i>port-channel interface number</i>—A channel interface. The range is 0—48.
learn	Specifies the multicast router learning method.
cgmp	Sets the switch to learn multicast router ports by snooping on Cisco Group Management Protocol (CGMP) packets.
pim-dvmrp	Sets the switch to learn multicast router ports by snooping on IGMP queries and Protocol-Independent Multicast-Distance Vector Multicast Routing Protocol (PIM-DVMRP) packets.

Command Default

By default, there are no multicast router ports.

The default learning method is pim-dvmrp to snoop IGMP queries and PIM-DVMRP packets.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

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

The CGMP learn method is useful for reducing control traffic.

The configuration is saved in NVRAM.

Example

The following example shows how to configure a port as a multicast router port:

```
Device(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

The following example shows how to specify the multicast router learning method as CGMP:

```
Device(config)# ip igmp snooping vlan 1 mrouter learn cgmp
```

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

ip igmp snooping vlan static

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 **ip igmp snooping vlan static** global configuration command on the device stack or on a standalone device. To remove the port specified as members of a static multicast group, use the **no** form of this command.

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	<i>vlan-id</i>	Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.
	<i>ip-address</i>	Adds a Layer 2 port as a member of a multicast group with the specified group IP address.
	interface <i>interface-id</i>	Specifies the interface of the member port. The <i>interface-id</i> has these options: <ul style="list-style-type: none"> • <i>fastethernet interface number</i>—A Fast Ethernet IEEE 802.3 interface. • <i>gigabitethernet interface number</i>—A Gigabit Ethernet IEEE 802.3z interface. • <i>tengigabitethernet interface number</i>—A 10-Gigabit Ethernet IEEE 802.3z interface. • <i>port-channel interface number</i>—A channel interface. The range is 0—128.
Command Default	By default, no ports are statically configured as members of a multicast group.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	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.

Example

The following example shows how to statically configure a host on an interface:

```
Device(config)# ip igmp snooping vlan 1 static 224.2.4.12 interface
gigabitEthernet1/0/1
```

Configuring port gigabitethernet1/0/1 on group 224.2.4.12

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

mvr (global configuration)

To enable the multicast VLAN registration (MVR) feature on the switch, use the **mvr** global configuration command without keywords on the switch stack or on a standalone switch. To return to the default settings, use the **no** form of this command.

mvr [**group** *ip-address* [*count*] | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **vlan** *vlan-id*]

no mvr [**group** *ip-address* [*count*] | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **vlan** *vlan-id*]

Syntax Description

group <i>ip-address</i>	(Optional) Statically configures an MVR group IP multicast address on the switch. Use the no form of this command to remove a statically configured IP multicast address or contiguous addresses or, when no IP address is entered, to remove all statically configured MVR IP multicast addresses.
<i>count</i>	(Optional) Multiple contiguous MVR group addresses. The range is 1 to 256; the default is 0.
mode	(Optional) Specifies the MVR mode of operation. The default is compatible mode.
compatible	(Optional) Sets MVR mode to provide compatibility with Catalyst 2900 XL and Catalyst 3500 XL switches. This mode does not allow dynamic membership joins on source ports.
dynamic	(Optional) Sets MVR mode to allow dynamic MVR membership on source ports.
querytime <i>value</i>	(Optional) Sets the maximum time to wait for IGMP report memberships on a receiver port. This time applies only to receiver-port leave processing. When an IGMP query is sent from a receiver port, the switch waits for the default or configured MVR querytime for an IGMP group membership report before removing the port from multicast group membership. The value is the response time in units of tenths of a second. The range is 1 to 100; the default is 5 tenths or one-half second. Use the no form of the command to return to the default setting.

vlan <i>vlan-id</i>	(Optional) Specifies the VLAN on which MVR multicast data is expected to be received. This is also the VLAN to which all the source ports belong. The range is 1 to 4094; the default is VLAN 1.
----------------------------	--

Command Default

MVR is disabled by default.

The default MVR **mode** is compatible mode.

No IP multicast addresses are configured on the switch by default.

The default **group** *ip-address count* is 0.

The default query response time is five-tenths or one-half second.

The default multicast VLAN for MVR is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

A maximum of 256 MVR multicast groups can be configured on a switch.

Use the command with keywords to set the MVR mode for a switch, configure the MVR IP multicast address, set the maximum time to wait for a query reply before removing a port from group membership, and to specify the MVR multicast VLAN.

Use the **mvr group** command to statically set up all the IP multicast addresses that will take part in MVR. Any multicast data sent to a configured multicast address is sent to all the source ports on the switch and to all receiver ports that have registered to receive data on that IP multicast address.

MVR supports aliased IP multicast addresses on the switch. However, if the switch is interoperating with Catalyst 3550 or Catalyst 3500 XL switches, you should not configure IP addresses that alias between themselves or with the reserved IP multicast addresses (in the range 224.0.0.xxx).

The **mvr querytime** command applies only to receiver ports.

If the switch MVR is interoperating with Catalyst 2900 XL or Catalyst 3500 XL switches, set the multicast mode to compatible.

When operating in compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.

MVR can coexist with IGMP snooping on a switch.

Multicast routing and MVR cannot coexist on a switch. If you enable multicast routing and a multicast routing protocol while MVR is enabled, MVR is disabled and a warning message appears. If you try to enable MVR while multicast routing and a multicast routing protocol are enabled, the operation to enable MVR is cancelled with an error message.

Examples

This example shows how to enable MVR:

```
Device(config)# mvr
```

Use the **show mvr** privileged EXEC command to display the current setting for maximum multicast groups.

This example shows how to configure 228.1.23.4 as an IP multicast address:

```
Device(config)# mvr group 228.1.23.4
```

This example shows how to configure ten contiguous IP multicast groups with multicast addresses from 228.1.23.1 to 228.1.23.10:

```
Device(config)# mvr group 228.1.23.1 10
```

Use the **show mvr members** privileged EXEC command to display the IP multicast group addresses configured on the switch.

This example shows how to set the maximum query response time as one second (10 tenths):

```
Device(config)# mvr querytime 10
```

This example shows how to set VLAN 2 as the multicast VLAN:

```
Device(config)# mvr vlan 2
```

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

mvr (interface configuration)

To statically assign a port to an IP multicast VLAN and IP address, use the **mvr** interface configuration command on the switch stack or on a standalone switch. To return to the default settings, use the **no** form of this command.

```
mvr [immediate | type {receiver | source} | vlan vlan-id group [ip-address]]
no mvr [immediate | type | vlan vlan-id group [ip-address]]
```

Syntax Description	
immediate	(Optional) Enables the Immediate Leave feature of MVR on a port. Use the no mvr immediate command to disable the feature.
type	(Optional) Configures the port as an MVR receiver port or a source port. The default port type is neither an MVR source nor a receiver port. The no mvr type command resets the port as neither a source or a receiver port.
receiver	Configures the port as a subscriber port that can only receive multicast data. Receiver ports cannot belong to the multicast VLAN.
source	Configures the port as an uplink port that can send and receive multicast data for the configured multicast groups. All source ports on a switch belong to a single multicast VLAN.
vlan <i>vlan-id</i> group	(Optional) Adds the port as a static member of the multicast group with the specified VLAN ID. The no mvr vlan <i>vlan-id</i> group command removes a port on a VLAN from membership in an IP multicast address group.
<i>ip-address</i>	(Optional) Statically configures the specified MVR IP multicast group address for the specified multicast VLAN ID. This is the IP address of the multicast group that the port is joining.

Command Default

A port is configured as neither a receiver nor a source.
The Immediate Leave feature is disabled on all ports.
No receiver port is a member of any configured multicast group.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

Configure a port as a source port if that port should be able to both send and receive multicast data bound for the configured multicast groups. Multicast data is received on all ports configured as source ports.

Receiver ports cannot be trunk ports. Receiver ports on a switch can be in different VLANs, but should not belong to the multicast VLAN.

A port that is not taking part in MVR should not be configured as an MVR receiver port or a source port. A non-MVR port is a normal switch port, able to send and receive multicast data with normal switch behavior.

When Immediate Leave is enabled, a receiver port leaves a multicast group more quickly. Without Immediate Leave, when the switch receives an IGMP leave message from a group on a receiver port, it sends out an IGMP MAC-based query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership. With Immediate Leave, an IGMP MAC-based query is not sent from the receiver port on which the IGMP leave was received. As soon as the leave message is received, the receiver port is removed from multicast group membership, which speeds up leave latency.

The Immediate Leave feature should be enabled only on receiver ports to which a single receiver device is connected.

The **mvr vlan group** command statically configures ports to receive multicast traffic sent to the IP multicast address. A port statically configured as a member of group remains a member of the group until statically removed. In compatible mode, this command applies only to receiver ports; in dynamic mode, it can also apply to source ports. Receiver ports can also dynamically join multicast groups by using IGMP join messages.

When operating in compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.

An MVR port cannot be a private-VLAN port.

Examples

This example shows how to configure a port as an MVR receiver port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mvr type receiver
```

Use the **show mvr interface** privileged EXEC command to display configured receiver ports and source ports.

This example shows how to enable Immediate Leave on a port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mvr immediate
```

This example shows how to add a port on VLAN 1 as a static member of IP multicast group 228.1.23.4:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

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

show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of the device or the VLAN, use the **show ip igmp snooping** command in user EXEC or privileged EXEC mode.

show ip igmp snooping [**groups** | **mrouter** | **querier**] [**vlan** *vlan-id*] [**detail**]

Syntax Description	
groups	(Optional) Displays the IGMP snooping multicast table.
mrouter	(Optional) Displays the IGMP snooping multicast router ports.
querier	(Optional) Displays the configuration and operation information for the IGMP querier.
vlan <i>vlan-id</i>	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
detail	(Optional) Displays operational state information.

Command Default None

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines VLAN IDs 1002—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

The following is a sample output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN:

```
Device# 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
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
-----
```

```

IGMP snooping                : Enabled
IGMPv2 immediate leave       : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode    : IGMP_ONLY
Robustness variable          : 2
Last member query count       : 2
Last member query interval    : 1000

```

The following is a sample output from the **show ip igmp snooping** command. It displays snooping characteristics for all the VLANs on the device:

```

Device# 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
Robustness variable          : 2
Last member query count       : 2
Last member query interval    : 1000

Vlan 1:
-----
IGMP snooping                : Enabled
IGMPv2 immediate leave       : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode    : IGMP_ONLY
Robustness variable          : 2
Last member query count       : 2
Last member query interval    : 1000
Vlan 2:
-----
IGMP snooping                : Enabled
IGMPv2 immediate leave       : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode    : IGMP_ONLY
Robustness variable          : 2
Last member query count       : 2
Last member query interval    : 1000
-
.
.
.

```

show ip igmp snooping groups

To display the Internet Group Management Protocol (IGMP) snooping multicast table for the device or the multicast information, use the **show ip igmp snooping groups** command in privileged EXEC mode.

show ip igmp snooping groups [**vlan** *vlan-id*] [[**dynamic** | **user**] [**count**] | *ip_address*]

Syntax Description	
vlan <i>vlan-id</i>	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094. Use this option to display the multicast table for a specified multicast VLAN or specific multicast information.
dynamic	(Optional) Displays IGMP snooping learned group information.
user	(Optional) Displays user-configured group information.
count	(Optional) Displays the total number of entries for the specified command options instead of the actual entries.
<i>ip_address</i>	(Optional) Characteristics of the multicast group with the specified group IP address.

Command Modes	
	Privileged EXEC
	User EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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

The following is a sample output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the device.

```
Device# show ip igmp snooping groups
```

Vlan	Group	Type	Version	Port List
1	224.1.4.4	igmp		Gi1/0/11
1	224.1.4.5	igmp		Gi1/0/11
2	224.0.1.40	igmp	v2	Gi1/0/15
104	224.1.4.2	igmp	v2	Gi2/0/1, Gi2/0/2
104	224.1.4.3	igmp	v2	Gi2/0/1, Gi2/0/2

The following is a sample output from the **show ip igmp snooping groups count** command. It displays the total number of multicast groups on the device.

```
Device# show ip igmp snooping groups count
```

Total number of multicast groups: 2

The following is a sample 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:

```
Device# show ip igmp snooping groups vlan 104 224.1.4.2
```

Vlan	Group	Type	Version	Port List
104	224.1.4.2	igmp	v2	Gi2/0/1, Gi1/0/15

show ip igmp snooping mrouter

To display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the device or for the specified multicast VLAN, use the **show ip igmp snooping mrouter** command in privileged EXEC mode.

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

Syntax Description	vlan <i>vlan-id</i> (Optional) Specifies a VLAN; Ranges are from 1—1001 and 1006—4094.	
Command Modes	User EXEC Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.
Usage Guidelines	<p>VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.</p> <p>When multicast VLAN registration (MVR) is enabled, the show ip igmp snooping mrouter command displays MVR multicast router information and IGMP snooping information.</p> <p>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.</p>	

Example

The following is a sample output from the **show ip igmp snooping mrouter** command. It shows how to display multicast router ports on the device:

```
Device# show ip igmp snooping mrouter

Vlan      ports
----      -
  1       Gi2/0/1 (dynamic)
```


show ip igmp snooping querier

To display the configuration and operation information for the IGMP querier that is configured on a device, use the **show ip igmp snooping querier** command in user EXEC mode.

show ip igmp snooping querier [**vlan** *vlan-id*] [**detail**]

Syntax Description	vlan <i>vlan-id</i> (Optional) Specifies a VLAN; Ranges are from 1—1001 and 1006—4094.
	detail (Optional) Displays detailed IGMP querier information.

Command Modes	User EXEC Privileged EXEC
----------------------	------------------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	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 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 device.

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 device, the output shows the Port field as Router. If the querier is a router, the output shows the port number on which the querier was detected 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 device querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the device querier and this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the device 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

The following is a sample output from the **show ip igmp snooping querier** command:

```
Device> show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
```

show ip igmp snooping querier

```

1          172.20.50.11  v3          Gi1/0/1
2          172.20.40.20  v2          Router

```

The following is a sample output from the **show ip igmp snooping querier detail** command:

```

Device> show ip igmp snooping querier detail

Vlan      IP Address      IGMP Version  Port
-----
1         1.1.1.1        v2           Fa8/0/1
Global IGMP device 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 device querier status

-----
elected querier is 1.1.1.1      on port Fa8/0/1
-----
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

```

show mvr

To display the current Multicast VLAN Registration (MVR) global parameter values, including whether or not MVR is enabled, the MVR multicast VLAN, the maximum query response time, the number of multicast groups, and the MVR mode (dynamic or compatible), use the **show mvr** privileged EXEC command without keywords.

show mvr

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	This command was introduced.
Cisco IOS Release 15.2(5)E	

Examples

This is an example of output from the **show mvr** command:

```
Switch# show mvr
MVR Running: TRUE
MVR multicast VLAN: 1
MVR Max Multicast Groups: 256
MVR Current multicast groups: 0
MVR Global query response time: 5 (tenths of sec)
MVR Mode: compatible
```

In the preceding display, the maximum number of multicast groups is fixed at 256. The MVR mode is either compatible (for interoperability with Catalyst 2900 XL and Catalyst 3500 XL switches) or dynamic (where operation is consistent with IGMP snooping operation and dynamic MVR membership on source ports is supported).

show mvr interface

To display the Multicast VLAN Registration (MVR) receiver and source ports, use the **show mvr interface** privileged EXEC command without keywords. To display MVR parameters for a specific receiver port, use the command with keywords.

show mvr interface [*interface-id* [**members** [**vlan** *vlan-id*]]]

Syntax Description

interface-id	(Optional) Displays MVR type, status, and Immediate Leave setting for the interface. Valid interfaces include physical ports (including type, stack member (stacking-capable switches only) module, and port number).
members	(Optional) Displays all MVR groups to which the specified interface belongs.
vlan <i>vlan-id</i>	(Optional) Displays all MVR group members on this VLAN. The range is 1 to 4094.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

If the entered port identification is a non-MVR port or a source port, the command returns an error message. For receiver ports, it displays the port type, per port status, and Immediate-Leave setting.

If you enter the **members** keyword, all MVR group members on the interface appear. If you enter a VLAN ID, all MVR group members in the VLAN appear.

Examples

This is an example of output from the **show mvr interface** command:

```
Switch# show mvr interface
Port          Type          Status          Immediate Leave
----          -
Gi1/0/1      SOURCE        ACTIVE/UP       DISABLED
Gi1/0/2      RECEIVER      ACTIVE/DOWN     DISABLED
```

In the preceding display, Status is defined as follows:

- Active means the port is part of a VLAN.
- Up/Down means that the port is forwarding/nonforwarding.
- Inactive means that the port is not yet part of any VLAN.

This is an example of output from the **show mvr interface** command for a specified port:

```
Switch# show mvr interface gigabitethernet1/0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

This is an example of output from the **show mvr interface *interface-id* members** command:

```
Switch# show mvr interface gigabitethernet1/0/2 members
239.255.0.0      DYNAMIC ACTIVE
239.255.0.1      DYNAMIC ACTIVE
239.255.0.2      DYNAMIC ACTIVE
239.255.0.3      DYNAMIC ACTIVE
239.255.0.4      DYNAMIC ACTIVE
239.255.0.5      DYNAMIC ACTIVE
239.255.0.6      DYNAMIC ACTIVE
239.255.0.7      DYNAMIC ACTIVE
239.255.0.8      DYNAMIC ACTIVE
239.255.0.9      DYNAMIC ACTIVE
```

show mvr members

To display all receiver and source ports that are currently members of an IP multicast group, use the **show mvr members** privileged EXEC command.

show mvr members [*ip-address*] [**vlan** *vlan-id*]

Syntax Description	<i>ip-address</i>	(Optional) The IP multicast address. If the address is entered, all receiver and source ports that are members of the multicast group appear. If no address is entered, all members of all Multicast VLAN Registration (MVR) groups are listed. If a group has no members, the group is listed as Inactive.
	vlan <i>vlan-id</i>	(Optional) Displays all MVR group members on this VLAN. The range is 1 to 4094.
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.
Usage Guidelines	The show mvr members command applies to receiver and source ports. For MVR-compatible mode, all source ports are members of all multicast groups.	

Examples

This is an example of output from the **show mvr members** command:

```
Switch# show mvr members
MVR Group IP      Status      Members
-----
239.255.0.1      ACTIVE     Gi1/0/1(d), Gi1/0/5(s)
239.255.0.2      INACTIVE   None
239.255.0.3      INACTIVE   None
239.255.0.4      INACTIVE   None
239.255.0.5      INACTIVE   None
239.255.0.6      INACTIVE   None
239.255.0.7      INACTIVE   None
239.255.0.8      INACTIVE   None
239.255.0.9      INACTIVE   None
239.255.0.10     INACTIVE   None
<output truncated>
```

This is an example of output from the **show mvr members ip-address** command. It displays the members of the IP multicast group with that address:

```
Switch# show mvr members 239.255.0.2
239.255.003.--22    ACTIVE          Gi1//1(d), Gi1/0/2(d), Gi1/0/3(d), Gi1/0/4(d), Gi1/0/5(s)
```




PART II

Interface and Hardware

- [Interface and Hardware Commands, on page 49](#)



Interface and Hardware Commands

- [debug fastethernet](#), on page 51
- [debug ilpower](#), on page 52
- [debug interface](#), on page 53
- [debug lldp packets](#), on page 54
- [debug nmsp](#), on page 55
- [duplex](#), on page 56
- [errdisable detect cause](#), on page 58
- [errdisable detect cause small-frame](#), on page 60
- [errdisable recovery cause](#), on page 61
- [errdisable recovery cause small-frame](#), on page 64
- [errdisable recovery interval](#), on page 65
- [lldp \(interface configuration\)](#), on page 66
- [mdix auto](#), on page 67
- [network-policy](#), on page 68
- [network-policy profile \(global configuration\)](#), on page 69
- [nmsp attachment suppress](#), on page 70
- [power efficient-ethernet auto](#), on page 71
- [power inline](#), on page 72
- [power inline consumption](#), on page 75
- [power inline police](#), on page 78
- [show eee](#), on page 80
- [show env](#), on page 83
- [show errdisable detect](#), on page 85
- [show errdisable recovery](#), on page 86
- [show interfaces](#), on page 87
- [show interfaces counters](#), on page 92
- [show interfaces switchport](#), on page 94
- [show interfaces transceiver](#), on page 98
- [show ip ports all](#), on page 101
- [show network-policy profile](#), on page 102
- [show power inline](#), on page 103
- [show system mtu](#), on page 108
- [speed](#), on page 109

- [switchport backup interface](#), on page 111
- [switchport block](#), on page 113
- [system mtu](#), on page 114
- [voice-signaling vlan \(network-policy configuration\)](#), on page 115
- [voice vlan \(network-policy configuration\)](#), on page 117

debug fastethernet

To enable debugging of the Ethernet management port, use the **debug fastethernet** command in EXEC mode. To disable debugging, use the **no** form of this command.

```
debug fastethernet {af | events | packets}
no debug fastethernet {af | events | packets}
```

Syntax Description

af Displays Ethernet management port software-address-filter debug messages.

events Displays Ethernet management port event debug messages.

packets Displays Ethernet management port packet debug messages.

Command Default

Debugging is disabled.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a member switch, you can start a session from the active switch by using the **session switch-number EXEC** command. Then enter the **debug** command at the command-line prompt of the member switch. You also can use the **remote command stack-member-number LINE EXEC** command on the active switch to enable debugging on a member switch without first starting a session.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug ilpower

To enable debugging of the power controller and Power over Ethernet (PoE) system, use the **debug ilpower** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug ilpower {cdp | controller | event | ha | port | powerman | registries | scp | sense}
no debug ilpower {cdp | controller | event | ha | port | powerman | registries | scp | sense}
```

Syntax Description

cdp	Displays PoE Cisco Discovery Protocol (CDP) debug messages.
controller	Displays PoE controller debug messages.
event	Displays PoE event debug messages.
ha	Displays PoE high-availability messages.
port	Displays PoE port manager debug messages.
powerman	Displays PoE power management debug messages.
registries	Displays PoE registries debug messages.
scp	Displays PoE SCP debug messages.
sense	Displays PoE sense debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

This command is supported only on PoE-capable switches.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a member switch, you can start a session from the active switch by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the member switch. You also can use the **remote command** *stack-member-number* *LINE* EXEC command on the active switch to enable debugging on a member switch without first starting a session.

debug interface

To enable debugging of interface-related activities, use the **debug interface** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug interface {interface-id | counters {exceptions | protocol memory} | null interface-number |
port-channel port-channel-number | states | vlan vlan-id}
no debug interface {interface-id | counters {exceptions | protocol memory} | null interface-number |
port-channel port-channel-number | states | vlan vlan-id}
```

Syntax Description

<i>interface-id</i>	ID of the physical interface. Displays debug messages for the specified physical port, identified by type switch number/module number/port, for example, gigabitethernet 1/0/2.
null <i>interface-number</i>	Displays debug messages for null interfaces. The interface number is always 0 .
port-channel <i>port-channel-number</i>	Displays debug messages for the specified EtherChannel port-channel interface. The <i>port-channel-number</i> range is 1 to 48.
vlan <i>vlan-id</i>	Displays debug messages for the specified VLAN. The vlan range is 1 to 4094.
counters	Displays counters debugging information.
exceptions	Displays debug messages when a recoverable exceptional condition occurs during the computation of the interface packet and data rate statistics.
protocol memory	Displays debug messages for memory operations of protocol counters.
states	Displays intermediary debug messages when an interface's state transitions.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a member switch, you can start a session from the active switch by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the member switch. You also can use the **remote command** *stack-member-number* *LINE* EXEC command on the active switch to enable debugging on a member switch without first starting a session.

debug lldp packets

To enable debugging of Link Layer Discovery Protocol (LLDP) packets, use the **debug lldp packets** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug lldp packets
no debug lldp packets

Syntax Description This command has no arguments or keywords.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	This command was introduced.
	Cisco IOS Release 15.2(5)E	

Usage Guidelines The **undebug lldp packets** command is the same as the **no debug lldp packets** command. When you enable debugging on a switch stack, it is enabled only on the . To enable debugging on a member switch, you can start a session from the by using the **session switch-number** EXEC command.

debug nmsp

To enable debugging of the Network Mobility Services Protocol (NMSP) on the switch, use the **debug nmsp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

Syntax Description	all	Displays all NMSP debug messages.
	connection	Displays debug messages for NMSP connection events.
	error	Displays debugging information for NMSP error messages.
	event	Displays debug messages for NMSP events.
	rx	Displays debugging information for NMSP receive messages.
	tx	Displays debugging information for NMSP transmit messages.
	packet	Displays debug messages for NMSP packet events.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines



Note Attachment information is not supported in Cisco IOS XE Denali 16.1.1 and later releases.

The **undebug nmsp** command is the same as the **no debug nmsp** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a member switch, you can start a session from the active switch by using the **session switch-number** EXEC command. Then enter the **debug** command at the command-line prompt of the member switch. You also can use the **remote command stack-member-number LINE** EXEC command on the active switch to enable debugging on a member switch without first starting a session.

duplex

To specify the duplex mode of operation for a port, use the **duplex** command in interface configuration mode. To return to the default value, use the **no** form of this command.

duplex {**auto** | **full** | **half**}
no duplex {**auto** | **full** | **half**}

Syntax Description

auto Enables automatic duplex configuration. The port automatically detects whether it should run in full- or half-duplex mode, depending on the attached device mode.

full Enables full-duplex mode.

half Enables 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.

Command Default

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

The default is **half** for 100BASE-*x* (where *x* is -BX, -FX, -FX-FE, or -LX) SFP modules.

Duplex options are not supported on the 1000BASE-*x* or 10GBASE-*x* (where *x* is -BX, -CWDM, -LX, -SX, or -ZX) small form-factor pluggable (SFP) modules.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

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

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. How this command is applied 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, and 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 reenable the interface during the reconfiguration.

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

Examples

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

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# duplex full
```

errdisable detect cause

To enable error-disable detection for a specific cause or for all causes, use the **errdisable detect cause** command in global configuration mode. To disable the error-disable detection feature, use the **no** form of this command.

```
errdisable detect cause {all | arp-inspection | bpduguard shutdown vlan | dhcp-rate-limit | dtp-flap
| gbic-invalid | inline-power | link-flap | loopback | pagp-flap | pppoe-ia-rate-limit | psp shutdown
vlan | security-violation shutdown vlan | sfp-config-mismatch}
no errdisable detect cause {all | arp-inspection | bpduguard shutdown vlan | dhcp-rate-limit | dtp-flap
| gbic-invalid | inline-power | link-flap | loopback | pagp-flap | pppoe-ia-rate-limit | psp shutdown
vlan | security-violation shutdown vlan | sfp-config-mismatch}
```

Syntax Description	
all	Enables error detection for all error-disabled causes.
arp-inspection	Enables error detection for dynamic Address Resolution Protocol (ARP) inspection.
bpduguard shutdown vlan	Enables per-VLAN error-disable for BPDU guard.
dhcp-rate-limit	Enables error detection for DHCP snooping.
dtp-flap	Enables error detection for the Dynamic Trunking Protocol (DTP) flapping.
gbic-invalid	Enables error detection for an invalid Gigabit Interface Converter (GBIC) module. Note This error refers to an invalid small form-factor pluggable (SFP) module.
inline-power	Enables error detection for the Power over Ethernet (PoE) error-disabled cause. Note This keyword is supported only on switches with PoE ports.
link-flap	Enables error detection for link-state flapping.
loopback	Enables error detection for detected loopbacks.
pagp-flap	Enables error detection for the Port Aggregation Protocol (PAgP) flap error-disabled cause.
pppoe-ia-rate-limit	Enables error detection for the PPPoE Intermediate Agent rate-limit error-disabled cause.
psp shutdown vlan	Enables error detection for protocol storm protection (PSP).
security-violation shutdown vlan	Enables voice aware 802.1x security.
sfp-config-mismatch	Enables error detection on an SFP configuration mismatch.

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

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines A cause (such as a link-flap or dhcp-rate-limit) 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 bridge protocol data unit (BPDU) guard, voice-aware 802.1x security, and port-security features, you can configure the switch to shut down only 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, 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.

For protocol storm protection, excess packets are dropped for a maximum of two virtual ports. Virtual port error disabling using the **psp** keyword is not supported for EtherChannel and Flexlink interfaces.

To verify your settings, enter the **show errdisable detect** privileged EXEC command.

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

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

This command shows how to globally configure BPDU guard for a per-VLAN error-disabled state:

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

This command shows how to globally configure voice-aware 802.1x security for a per-VLAN error-disabled state:

```
Device(config)# errdisable detect cause security-violation shutdown vlan
```

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

errdisable detect cause small-frame

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 **errdisable detect cause small-frame** global configuration command on the switch stack or on a standalone switch. 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.

Command Default This feature is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E
		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:

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

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

errdisable recovery cause

To enable the error-disabled mechanism to recover from a specific cause, use the **errdisable recovery cause** command in global configuration mode. To return to the default setting, use the **no** form of this command.

```
errdisable recovery cause {all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit |
dtp-flap | gbic-invalid | inline-power | link-flap | loopback | mac-limit | pagp-flap | port-mode-failure |
pppoe-ia-rate-limit | psecure-violation | psp | security-violation | sfp-config-mismatch | storm-control |
udld | vmmps}
```

```
no errdisable recovery cause {all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit |
dtp-flap | gbic-invalid | inline-power | link-flap | loopback | mac-limit | pagp-flap | port-mode-failure |
pppoe-ia-rate-limit | psecure-violation | psp | security-violation | sfp-config-mismatch | storm-control |
udld | vmmps}
```

Syntax Description

all	Enables the timer to recover from all error-disabled causes.
arp-inspection	Enables the timer to recover from the Address Resolution Protocol (ARP) inspection error-disabled state.
bpduguard	Enables the timer to recover from the bridge protocol data unit (BPDU) guard error-disabled state.
channel-misconfig	Enables the timer to recover from the EtherChannel misconfiguration error-disabled state.
dhcp-rate-limit	Enables the timer to recover from the DHCP snooping error-disabled state.
dtp-flap	Enables the timer to recover from the Dynamic Trunking Protocol (DTP) flap error-disabled state.
gbic-invalid	Enables 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.
inline-power	Enables the timer to recover from the Power over Ethernet (PoE) error-disabled state. This keyword is supported only on switches with PoE ports.
link-flap	Enables the timer to recover from the link-flap error-disabled state.
loopback	Enables the timer to recover from a loopback error-disabled state.
mac-limit	Enables the timer to recover from the mac limit error-disabled state.
pagp-flap	Enables the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disabled state.

port-mode-failure	Enables the timer to recover from the port mode change failure error-disabled state.
pppoe-ia-rate-limit	Enables the timer to recover from the PPPoE IA rate limit error-disabled state.
psecure-violation	Enables the timer to recover from a port security violation disable state.
psp	Enables the timer to recover from the protocol storm protection (PSP) error-disabled state.
security-violation	Enables the timer to recover from an IEEE 802.1x-violation disabled state.
sfp-config-mismatch	Enables error detection on an SFP configuration mismatch.
storm-control	Enables the timer to recover from a storm control error.
udld	Enables the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.
vmmps	Enables the timer to recover from the VLAN Membership Policy Server (VMPS) error-disabled state.

Command Default Recovery is disabled for all causes.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines A cause (such as all or BPDU guard) 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 only 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.

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

Examples

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


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

errdisable recovery cause small-frame

Use the **errdisable recovery cause small-frame** global configuration command on the switch 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.

Command Default This feature is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	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** interface configuration command.

This example shows how to set the recovery timer:

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

errdisable recovery interval

To specify the time to recover from an error-disabled state, use the **errdisable recovery interval** command in global configuration mode. To return to the default setting, use the **no** form of this command.

errdisable recovery interval *timer-interval*
no errdisable recovery interval *timer-interval*

Syntax Description	<i>timer-interval</i> Time to recover from the error-disabled state. The range is 30 to 86400 seconds. The same interval is applied to all causes. The default interval is 300 seconds.						
Command Default	The default recovery interval is 300 seconds.						
Command Modes	Global configuration						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E</td> </tr> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E		This command was introduced.
Release	Modification						
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E						
	This command was introduced.						

Usage Guidelines 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.

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

Examples

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

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

lldp (interface configuration)

To enable Link Layer Discovery Protocol (LLDP) on an interface, use the **lldp** command in interface configuration mode. To disable LLDP on an interface, use the **no** form of this command.

Syntax Description		
med-tlv-select		Selects an LLDP Media Endpoint Discovery (MED) time-length-value (TLV) element to send.
<i>tlv</i>		String that identifies the TLV element. Valid values are the following: <ul style="list-style-type: none"> • inventory-management— LLDP MED Inventory Management TLV. • location— LLDP MED Location TLV. • network-policy— LLDP MED Network Policy TLV.
receive		Enables the interface to receive LLDP transmissions.
tlv-select		Selects the LLDP TLVs to send.
power-management		Sends the LLDP Power Management TLV.
transmit		Enables LLDP transmission on the interface.

Command Default LLDP is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines This command is supported on 802.1 media types.
If the interface is configured as a tunnel port, LLDP is automatically disabled.
The following example shows how to disable LLDP transmission on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no lldp transmit
```

The following example shows how to enable LLDP transmission on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# lldp transmit
```

mdix auto

To enable the automatic medium-dependent interface crossover (auto-MDIX) feature on the interface, use the **mdix auto** command in interface configuration mode. To disable auto-MDIX, use the **no** form of this command.

mdix auto
no mdix auto

Syntax Description This command has no arguments or keywords.

Command Default Auto-MDIX is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately.

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 the 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.

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.

This example shows how to enable auto-MDIX on a port:

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto
Device(config-if)# duplex auto
Device(config-if)# mdix auto
Device(config-if)# end
```

network-policy

To apply a network-policy profile to an interface, use the **network-policy** command in interface configuration mode. To remove the policy, use the **no** form of this command.

network-policy *profile-number*
no network-policy

Syntax Description

profile-number The network-policy profile number to apply to the interface.

Command Default

No network-policy profiles are applied.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

Use the **network-policy** *profile number* interface configuration command to apply a profile to an interface.

You cannot apply the **switchport voice vlan** command on an interface if you first configure a network-policy profile on it. However, if **switchport voice vlan** *vlan-id* is already configured on the interface, you can apply a network-policy profile on the interface. The interface then has the voice or voice-signaling VLAN network-policy profile applied.

This example shows how to apply network-policy profile 60 to an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# network-policy 60
```

network-policy profile (global configuration)

To create a network-policy profile and to enter network-policy configuration mode, use the **network-policy profile** command in global configuration mode. To delete the policy and to return to global configuration mode, use the **no** form of this command.

network-policy profile *profile-number*
no network-policy profile *profile-number*

Syntax Description	<i>profile-number</i> Network-policy profile number. The range is 1 to 4294967295.	
Command Default	No network-policy profiles are defined.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.
Usage Guidelines	<p>Use the network-policy profile global configuration command to create a profile and to enter network-policy profile configuration mode.</p> <p>To return to privileged EXEC mode from the network-policy profile configuration mode, enter the exit command.</p> <p>When you are in network-policy profile configuration mode, you can create the profile for voice and voice signaling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.</p> <p>These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).</p> <p>This example shows how to create network-policy profile 60:</p> <pre>Device(config)# network-policy profile 60 Device(config-network-policy)#</pre>	

nmsp attachment suppress

To suppress the reporting of attachment information from a specified interface, use the **nmsp attachment suppress** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

nmsp attachment suppress
no nmsp attachment suppress

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines Use the **nmsp attachment suppress** interface configuration command to configure an interface to not send location and attachment notifications to a Cisco Mobility Services Engine (MSE).



Note Attachment information is not supported in Cisco IOS XE Denali 16.1.1 and later releases.

This example shows how to configure an interface to not send attachment information to the MSE:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# nmsp attachment suppress
```


power efficient-ethernet auto

To enable Energy Efficient Ethernet (EEE) for an interface, use the **power efficient-ethernet auto** command in interface configuration mode. To disable EEE on an interface, use the **no** form of this command.

power efficient-ethernet auto
no power efficient-ethernet auto

Syntax Description This command has no arguments or keywords.

Command Default EEE is enabled

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines You can enable EEE on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

The **power efficient-ethernet auto** command is available only if the interface is EEE capable. To check if an interface is EEE capable, use the **show eee capabilities EXEC** command.

When EEE is enabled, the device advertises and autonegotiates EEE to its link partner. To view the current EEE status for an interface, use the **show eee status EXEC** command.

This command does not require a license.

This example shows how to enable EEE for an interface:

```
Device(config-if) # power efficient-ethernet auto
Device(config-if) #
```

This example shows how to disable EEE for an interface:

```
Device(config-if) # no power efficient-ethernet auto
Device(config-if) #
```

power inline

To configure the power management mode on Power over Ethernet (PoE) ports, use the **power inline** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
power inline {auto [max max-wattage] | never | port priority {high | low} | static [max
max-wattage]}
no power inline {auto | never | port priority {high | low} | static [max max-wattage]}
```

Syntax Description		
	auto	Enables powered-device detection. If enough power is available, automatically allocates power to the PoE port after device detection. Allocation is first-come, first-serve.
	max <i>max-wattage</i>	(Optional) Limits the power allowed on the port. The range is 4000 to 30000 mW. If no value is specified, the maximum is allowed.
	never	Disables device detection, and disables power to the port.
	port	Configures the power priority of the port. The default priority is low.
	priority { high low }	Sets the power priority of the port. In case of a power supply failure, ports configured as low priority are turned off first and ports configured as high priority are turned off last. The default priority is low.
	static	Enables powered-device detection. Pre-allocates (reserves) power for a port before the switch discovers the powered device. This action guarantees that the device connected to the interface receives enough power.

Command Default The default is **auto** (enabled).
The maximum wattage is 30,000 mW.
The default port priority is low.

Command Default Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

This command is supported only on PoE-capable ports. If you enter this command on a port that does not support PoE, this error message appears:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# power inline auto
                        ^
% Invalid input detected at '^' marker.
```

In a switch stack, this command is supported on all ports in the stack that support PoE.

Use the **max max-wattage** option to disallow higher-power powered devices. With this configuration, when the powered device sends Cisco Discovery Protocol (CDP) messages requesting more power than the maximum wattage, the switch removes power from the port. If the powered-device IEEE class maximum is greater than the maximum wattage, the switch does not power the device. The power is reclaimed into the global power budget.



Note

The switch never powers any class 0 or class 3 device if the **power inline max max-wattage** command is configured for less than 30 W.

If the switch denies power to a powered device (the powered device requests more power through CDP messages or if the IEEE class maximum is greater than the maximum wattage), the PoE port is in a power-deny state. The switch generates a system message, and the Oper column in the **show power inline** privileged EXEC command output shows *power-deny*.

Use the **power inline static max max-wattage** command to give a port high priority. The switch allocates PoE to a port configured in static mode before allocating power to a port configured in auto mode. The switch reserves power for the static port when it is configured rather than upon device discovery. The switch reserves the power on a static port even when there is no connected device and whether or not the port is in a shutdown or in a no shutdown state. The switch allocates the configured maximum wattage to the port, and the amount is never adjusted through the IEEE class or by CDP messages from the powered device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed power when it is connected to a static port. However, if the powered device IEEE class is greater than the maximum wattage, the switch does not supply power to it. If the switch learns through CDP messages that the powered device needs more than the maximum wattage, the powered device is shut down.

If the switch cannot pre-allocate power when a port is in static mode (for example, because the entire power budget is already allocated to other auto or static ports), this message appears: Command rejected: power inline static: pwr not available. The port configuration remains unchanged.

When you configure a port by using the **power inline auto** or the **power inline static** interface configuration command, the port autonegotiates by using the configured speed and duplex settings. This is necessary to determine the power requirements of the connected device (whether or not it is a powered device). After the power requirements have been determined, the switch hardcodes the interface by using the configured speed and duplex settings without resetting the interface.

When you configure a port by using the **power inline never** command, the port reverts to the configured speed and duplex settings.

If a port has a Cisco powered device connected to it, you should not use the **power inline never** command to configure the port. A false link-up can occur, placing the port in an error-disabled state.

Use the **power inline port priority {high | low}** command to configure the power priority of a PoE port. Powered devices connected to ports with low port priority are shut down first in case of a power shortage.

You can verify your settings by entering the **show power inline EXEC** command.

Examples

This example shows how to enable detection of a powered device and to automatically power a PoE port on a switch:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline auto
```

This example shows how to configure a PoE port on a switch to allow a class 1 or a class 2 powered device:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline auto max 7000
```

This example shows how to disable powered-device detection and to not power a PoE port on a switch:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline never
```


This example shows how to set the priority of a port to high, so that it would be one of the last ports to be shut down in case of power supply failure:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline port priority high
```

power inline consumption

To override the amount of power specified by the IEEE classification for a powered device, use the **power inline consumption** command in global or interface configuration to specify the wattage used by each device. To return to the default power setting, use the **no** form of this command.

power inline consumption [**default**] *wattage*
no power inline consumption [**default**]

Syntax Description	<p>default The default keyword appears only in the global configuration. The command has the same effect with or without the keyword.</p> <p><i>wattage</i> Specifies the power that the switch budgets for the port. The range is 4000 to 15400 mW.</p>				
Command Default	The default power on each Power over Ethernet (PoE) port is 15400 mW.				
Command Modes	Global configuration Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.				
Usage Guidelines	<p>This command is supported only on the LAN Base image.</p> <p>When Cisco powered devices are connected to PoE ports, the switch uses Cisco Discovery Protocol (CDP) to determine the <i>CDP-specific</i> power consumption of the devices, which is the amount of power to allocate based on the CDP messages. The switch adjusts the power budget accordingly. This does not apply to IEEE third-party powered devices. For these devices, when the switch grants a power request, the switch adjusts the power budget according to the powered-device IEEE classification. If the powered device is a class 0 (class status unknown) or a class 3, the switch budgets 15400 mW for the device, regardless of the CDP-specific amount of power needed.</p> <p>If the powered device reports a higher class than its CDP-specific consumption or does not support power classification (defaults to class 0), the switch can power fewer devices because it uses the IEEE class information to track the global power budget.</p> <p>With PoE+, powered devices use IEEE 802.3at and LLDP power with media dependent interface (MDI) type, length, and value descriptions (TLVs), Power-via-MDA TLVs, for negotiating power up to 30 W. Cisco pre-standard devices and Cisco IEEE powered devices can use CDP or the IEEE 802.3at power-via-MDI power negotiation mechanism to request power levels up to 30 W.</p>				
 Note	The initial allocation for Class 0, Class 3, and Class 4 powered devices is 15.4 W. When a device starts up and uses CDP or LLDP to send a request for more than 15.4 W, it can be allocated up to the maximum of 30 W.				

By using the **power inline consumption** *wattage* configuration command, you can override the default power requirement of the IEEE classification. The difference between what is mandated by the IEEE classification and what is actually needed by the device is reclaimed into the global power budget for use by additional devices. You can then extend the switch power budget and use it more effectively.

Before entering the **power inline consumption** *wattage* configuration command, we recommend that you enable policing of the real-time power consumption by using the **power inline police** [action log] interface configuration command.



Caution

You should carefully plan your switch power budget and make certain not to oversubscribe the power supply.

When you enter the **power inline consumption default** *wattage* or the **no power inline consumption default** global configuration command, or the **power inline consumption** *wattage* or the **no power inline consumption** interface configuration command, this caution message appears.

```
%CAUTION: Interface Gi1/0/1: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty. Take precaution not to
oversubscribe the power supply.
It is recommended to enable power policing if the switch supports it.
Refer to documentation.
```



Note

When you manually configure the power budget, you must also consider the power loss over the cable between the switch and the powered device.

For more information about the IEEE power classifications, see the “Configuring Interface Characteristics” chapter in the software configuration guide for this release.

This command is supported only on PoE-capable ports. If you enter this command on a switch or port that does not support PoE, an error message appears.

In a switch stack, this command is supported on all switches or ports in the stack that support PoE.

You can verify your settings by entering the **show power inline consumption** privileged EXEC command.

Examples

This example shows how to use the command in global configuration mode to configure the switch to budget 5000 mW to each PoE port:

```
Device(config)# power inline consumption default 5000
%CAUTION: Interface Gi1/0/1: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty. Take precaution not to
oversubscribe the power supply.
It is recommended to enable power policing if the switch supports it.
Refer to documentation.
```

This example shows how to use the command in interface configuration mode to configure the switch to budget 12000 mW to the powered device connected to a specific PoE port:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline consumption 12000
%CAUTION: Interface Gi1/0/2: Misconfiguring the 'power inline consumption/allocation'
```

command may cause damage to the switch and void your warranty. Take precaution not to oversubscribe the power supply.

It is recommended to enable power policing if the switch supports it.
Refer to documentation.

power inline police

To enable policing of real-time power consumption on a powered device, use the **power inline police** command in interface configuration mode. To disable this feature, use the **no** form of this command

```
power inline police [action {errdisable | log}]
no power inline police
```

Syntax Description

action errdisable	(Optional) Configures the device to turn off power to the port if the real-time power consumption exceeds the maximum power allocation on the port. This is the default action.
action log	(Optional) Configures the device to generate a syslog message while still providing power to a connected device if the real-time power consumption exceeds the maximum power allocation on the port.

Command Default

Policing of the real-time power consumption of the powered device is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

This command is supported only on the LAN Base image.

This command is supported only on Power over Ethernet (PoE)-capable ports. If you enter this command on a device or port that does not support PoE, an error message appears.

In a switch stack, this command is supported on all switches or ports in the stack that support PoE and real-time power-consumption monitoring.

When policing of the real-time power consumption is enabled, the device takes action when a powered device consumes more power than the allocated maximum amount.

When PoE is enabled, the device senses the real-time power consumption of the powered device. This feature is called *power monitoring* or *power sensing*. The device also polices the power usage with the *power policing* feature.

When power policing is enabled, the device uses one of these values as the cutoff power on the PoE port in this order:

1. The user-defined power level that limits the power allowed on the port when you enter the **power inline auto max** *max-wattage* or the **power inline static max** *max-wattage* interface configuration command
2. The device automatically sets the power usage of the device by using CDP power negotiation or by the IEEE classification and LLDP power negotiation.

If you do not manually configure the cutoff-power value, the device automatically determines it by using CDP power negotiation or the device IEEE classification and LLDP power negotiation. If CDP or LLDP are not enabled, the default value of 30 W is applied. However without CDP or LLDP, the device does not allow devices to consume more than 15.4 W of power because values from 15400 to 30000 mW are only allocated based on CDP or LLDP requests. If a powered device consumes more than 15.4 W without CDP or LLDP

negotiation, the device might be in violation of the maximum current I_{max} limitation and might experience an I_{cut} fault for drawing more current than the maximum. The port remains in the fault state for a time before attempting to power on again. If the port continuously draws more than 15.4 W, the cycle repeats.

When a powered device connected to a PoE+ port restarts and sends a CDP or LLDP packet with a power TLV, the device locks to the power-negotiation protocol of that first packet and does not respond to power requests from the other protocol. For example, if the device is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the device has locked on it, the device does not respond to LLDP power requests and can no longer power on any accessories. In this case, you should restart the powered device.

If power policing is enabled, the device polices power usage by comparing the real-time power consumption to the maximum power allocated on the PoE port. If the device uses more than the maximum power allocation (or *cutoff power*) on the port, the device either turns power off to the port, or the device generates a syslog message and updates the LEDs (the port LEDs are blinking amber) while still providing power to the device.

- To configure the device to turn off power to the port and put the port in the error-disabled state, use the **power inline police** interface configuration command.
- To configure the device to generate a syslog message while still providing power to the device, use the **power inline police action log** command.

If you do not enter the **action log** keywords, the default action is to shut down the port, turn off power to it, and put the port in the PoE error-disabled state. To configure the PoE port to automatically recover from the error-disabled state, use the **errdisable detect cause inline-power** global configuration command to enable error-disabled detection for the PoE cause and the **errdisable recovery cause inline-power interval interval** global configuration command to enable the recovery timer for the PoE error-disabled cause.



Caution

If policing is disabled, no action occurs when the powered device consumes more than the maximum power allocation on the port, which could adversely affect the device.

You can verify your settings by entering the **show power inline police** privileged EXEC command.

Examples

This example shows how to enable policing of the power consumption and configuring the device to generate a syslog message on the PoE port on a device:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline police action log
```

show eee

To display Energy Efficient Ethernet (EEE) information for an interface, use the **show eee** command in EXEC mode.

show eee{**counters** | **capabilities interface** *interface-id* | **status interface** *interface-id*}

Syntax Description		
counters		Displays EEE counters.
capabilities		Displays EEE capabilities for the specified interface.
status		Displays EEE status information for the specified interface.
interface <i>interface-id</i>		Specifies the interface for which to display EEE capabilities or status information.

Command Default None

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines You can enable EEE on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low power utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

To check if an interface is EEE capable, use the **show eee capabilities** command. You can enable EEE on an interface that is EEE capable by using the **power efficient-ethernet auto** interface configuration command.

To view the EEE status, LPI status, and wake error count information for an interface, use the **show eee status** command.

This is an example of output from the **show eee counters** command:

```
Device# show eee counters
ASIC #0
----
      LP Active 1G           : 0
      LP Transitioning 1G    : 0
      LP Active Tx 100M      : 0
      LP Transitioning Tx 100M : 0
      LP Active Rx 100M      : 0
      LP Transitioning Rx 100M : 0

ASIC #1
----
```

```

LP Active 1G           : 0
LP Transitioning 1G    : 0
LP Active Tx 100M     : 0
LP Transitioning Tx 100M : 0
LP Active Rx 100M     : 0
LP Transitioning Rx 100M : 0

```

This is an example of output from the **show eee capabilities** command on an interface where EEE is enabled:

```

Device# show eee capabilities interface gigabitethernet1/0/1
Gi1/0/1
EEE(efficient-ethernet): yes (100-Tx and 1000T auto)
Link Partner           : yes (100-Tx and 1000T auto)

```

This is an example of output from the **show eee capabilities** command on an interface where EEE is not enabled:

```

Device# show eee capabilities interface gigabitethernet2/0/1
Gi2/0/1
EEE(efficient-ethernet): not enabled
Link Partner           : not enabled

```

This is an example of output from the **show eee status** command on an interface where EEE is enabled and operational. The table that follows describes the fields in the display.

```

Device# show eee status interface gigabitethernet1/0/4
Gi1/0/4 is up
EEE(efficient-ethernet): Operational
Rx LPI Status           : Received
Tx LPI Status           : Received

```

This is an example of output from the **show eee status** command on an interface where EEE is operational and the ports are in low power save mode:

```

Device# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is up
EEE(efficient-ethernet): Operational
Rx LPI Status           : Low Power
Tx LPI Status           : Low Power
Wake Error Count       : 0

```

This is an example of output from the **show eee status** command on an interface where EEE is not enabled because a remote link partner is incompatible with EEE:

```

Device# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is down
EEE(efficient-ethernet): Disagreed
Rx LPI Status           : None
Tx LPI Status           : None
Wake Error Count       : 0

```

Table 6: show eee status Field Descriptions

Field	Description
EEE (efficient-ethernet)	<p>The EEE status for the interface. This field can have any of the following values:</p> <ul style="list-style-type: none"> • N/A—The port is not capable of EEE. • Disabled—The port EEE is disabled. • Disagreed—The port EEE is not set because a remote link partner might be incompatible with EEE; either it is not EEE capable, or its EEE setting is incompatible. • Operational—The port EEE is enabled and operating. <p>If the interface speed is configured as 10 Mbps, EEE is disabled internally. When the interface speed moves back to auto, 100 Mbps or 1000 Mbps, EEE becomes active again.</p>
Rx/Tx LPI Status	<p>The Low Power Idle (LPI) status for the link partner. These fields can have any of the following values:</p> <ul style="list-style-type: none"> • N/A—The port is not capable of EEE. • Interrupted—The link partner is in the process of moving to low power mode. • Low Power—The link partner is in low power mode. • None— EEE is disabled or not capable at the link partner side. • Received—The link partner is in low power mode and there is traffic activity. <p>If an interface is configured as half-duplex, the LPI status is None, which means the interface cannot be in low power mode until it is configured as full-duplex.</p>
Wake Error Count	<p>The number of PHY wake-up faults that have occurred. A wake-up fault can occur when EEE is enabled and the connection to the link partner is broken.</p> <p>This information is useful for PHY debugging.</p>

show env

To display fan, temperature, redundant power system (RPS) availability, and power information, use the **show env** command in EXEC mode.

```
show env {all | fan | power [{all | switch [stack-member-number]]} | rps | stack [stack-member-number] | temperature [status]}
```

Syntax Description		
all	Displays the fan and temperature environmental status and the status of the internal power supplies and the RPS.	
fan	Displays the switch fan status.	
power	Displays the internal power status of the active switch.	
all	(Optional) Displays the status of all the internal power supplies in a standalone switch when the command is entered on the switch, or in all the member switches when the command is entered on the active switch.	
switch	(Optional) Displays the status of the internal power supplies for each switch in the stack or for the specified switch. This keyword is available only on stacking-capable switches.	
<i>stack-member-number</i>	(Optional) Number of the member switch for which to display the status of the internal power supplies or the environmental status. The range is 1 to 8.	
rps	Displays the RPS status.	
stack	Displays all environmental status for each switch in the stack or for the specified switch. This keyword is available only on stacking-capable switches.	
temperature	Displays the switch temperature status.	
status	(Optional) Displays the switch internal temperature (not the external temperature) and the threshold values.	
Command Default	None	
Command Modes	User EXEC Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

Use the **show env EXEC** command to display the information for the switch being accessed—a standalone switch or the active switch. Use this command with the **stack** and **switch** keywords to display all information for the stack or for the specified member 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.

Examples

This is an example of output from the **show env power all** command on the active switch:

Table 7: States in the show env temperature status Command Output

State	Description
Green	The switch temperature is in the <i>normal</i> operating range.
Yellow	The temperature is in the <i>warning</i> range. You should check the external temperature around the switch.
Red	The temperature is in the <i>critical</i> range. The switch might not run properly if the temperature is in this range.

show errdisable detect

To display error-disabled detection status, use the **show errdisable detect** command in EXEC mode.

show errdisable detect

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines A gbic-invalid error reason refers to an invalid small form-factor pluggable (SFP) module.

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 is per-VLAN error-disabled on other ports.

This is an example of output from the **show errdisable detect** command:

show errdisable recovery

To display the error-disabled recovery timer information, use the **show errdisable recovery** command in EXEC mode.

show errdisable recovery

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines A gbic-invalid error-disable reason refers to an invalid small form-factor pluggable (SFP) module interface.



Note Though visible in the output, the unicast-flood field is not valid.

This is an example of output from the **show errdisable recovery** command:

show interfaces

To display the administrative and operational status of all interfaces or for a specified interface, use the **show interfaces** command in privileged EXEC mode.

```
show interfaces [{interface-id | vlan vlan-id}] [{accounting | capabilities [module number] | debounce | description | etherchannel | flowcontrol | pruning | stats | status [{err-disabled}] | trunk}]
```

Syntax Description	
<i>interface-id</i>	(Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member for stacking-capable switches, module, and port number) and port channels. The port channel range is 1 to 48.
vlan <i>vlan-id</i>	(Optional) VLAN identification. The range is 1 to 4094.
accounting	(Optional) Displays 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) Displays 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 <i>number</i>	(Optional) Displays capabilities of all interfaces on the switch or specified stack member. The range is 1 to 8. This option is not available if you entered a specific interface ID.
debounce	(Optional) Displays port debounce timer information for an interface.
description	(Optional) Displays the administrative status and description set for an interface.
etherchannel	(Optional) Displays interface EtherChannel information.
flowcontrol	(Optional) Displays interface flow control information.
mtu	(Optional) Displays the MTU for each interface or for the specified interface.
pruning	(Optional) Displays trunk VTP pruning information for the interface.
stats	(Optional) Displays the input and output packets by switching the path for the interface.

status	(Optional) Displays 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) Displays interfaces in an error-disabled state.
trunk	(Optional) Displays interface trunk information. If you do not specify an interface, only information for active trunking ports appears.



Note Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **random-detect**, and **rate-limit** keywords are not supported.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interface capabilities module *number*** command to display the capabilities of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, there is no output.
- 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 in the stack.

This is an example of output from the **show interfaces** command for an interface on stack member 3:

```
Device# show interfaces gigabitethernet3/0/2
GigabitEthernet3/0/2 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 2037.064d.4381 (bia 2037.064d.4381)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 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: 0/2000/0/0 (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 unknown protocol drops
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:

```

Device# show interfaces accounting
Vlan1
      Protocol  Pkts In  Chars In  Pkts Out  Chars Out
      IP        382021  29073978  41157     20408734
      ARP        981     58860     179       10740
FastEthernet0
      Protocol  Pkts In  Chars In  Pkts Out  Chars Out
      Other      4        276      0         0
      Spanning Tree  41      2132     0         0
      CDP        5        2270     10        4318
GigabitEthernet1/0/1
      Protocol  Pkts In  Chars In  Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/2
      Protocol  Pkts In  Chars In  Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/3
      Protocol  Pkts In  Chars In  Pkts Out  Chars Out
      Other      0         0       226505    14949330
      Spanning Tree  679120  40747200  0         0
      CDP        22623   10248219  22656    10670858
      DTP        45226   2713560   0         0
GigabitEthernet1/0/4
      Protocol  Pkts In  Chars In  Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/5
      Protocol  Pkts In  Chars In  Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/6
      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:

```

Device# show interfaces gigabitethernet1/0/1 capabilities
GigabitEthernet1/0/1
Model: WS-C2960X-48TS-L
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:

```

Device# show interfaces gigabitethernet1/0/2 description
Interface          Status      Protocol Description
Gi1/0/2            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:

This is an example of output from the **show interfaces interface-id pruning** command when pruning is enabled in the VTP domain:

```

Device# show interfaces gigabitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3

```

This is an example of output from the **show interfaces stats** command for a specified VLAN interface:

```

Device# 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:

This is an example of output from the **show interfaces interface-id status** command:

```

Device# show interfaces gigabitethernet1/0/20 status
Port   Name           Status      Vlan   Duplex  Speed   Type
Gi1/0/20          notconnect  1         auto   auto    10/100/1000BaseTX

```

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:

```

Device# show interfaces status err-disabled
Port   Name           Status      Reason
Gi1/0/2          err-disabled  gbic-invalid
Gi2/0/3          err-disabled  dtp-flap

```

This is an example of output from the **show interfaces interface-id pruning** command:

```
Device# show interfaces gigabitethernet1/0/2 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.

```
Device# show interfaces gigabitethernet1/0/1 trunk
Port      Mode      Encapsulation  Status      Native vlan
Gi1/0/1   on        802.1q         other       10

Port      Vlans allowed on trunk
Gi1/0/1   none

Port      Vlans allowed and active in management domain
Gi1/0/1   none

Port      Vlans in spanning tree forwarding state and not pruned
Gi1/0/1   none
```

show interfaces counters

To display various counters for the switch or for a specific interface, use the **show interfaces counters** command in privileged EXEC mode.

show interfaces [*interface-id*] **counters** [{**errors** | **etherchannel** | **module** *stack-member-number* | **protocol status** | **trunk**}]

Syntax Description

<i>interface-id</i>	(Optional) ID of the physical interface, including type, stack member (stacking-capable switches only) module, and port number.
errors	(Optional) Displays error counters.
etherchannel	(Optional) Displays EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.
module <i>stack-member-number</i>	(Optional) Displays counters for the specified stack member. The range is 1 to 8. Note In this command, the module keyword refers to the stack member number. The module number that is part of the interface ID is always zero.
protocol status	(Optional) Displays the status of protocols enabled on interfaces.
trunk	(Optional) Displays trunk counters.



Note

Though visible in the command-line help string, the **vlan** *vlan-id* keyword is not supported.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

If you do not enter any keywords, all counters for all interfaces are included.

This is an example of partial output from the **show interfaces counters** command. It displays all counters for the switch.

```
Device# show interfaces counters
Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Gi1/0/1      0           0            0            0
Gi1/0/2      0           0            0            0
Gi1/0/3     95285341    43115        1178430      1950
Gi1/0/4      0           0            0            0
```

<output truncated>

This is an example of partial output from the **show interfaces counters module** command for stack member 2. It displays all counters for the specified switch in the stack.

```
Device# show interfaces counters module 2
Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Gi1/0/1       520         2            0            0
Gi1/0/2       520         2            0            0
Gi1/0/3       520         2            0            0
Gi1/0/4       520         2            0            0
```

<output truncated>

This is an example of partial output from the **show interfaces counters protocol status** command for all interfaces:

```
Device# 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
GigabitEthernet1/0/1: Other, IP, ARP, CDP
GigabitEthernet1/0/2: Other, IP
GigabitEthernet1/0/3: Other, IP
GigabitEthernet1/0/4: Other, IP
GigabitEthernet1/0/5: Other, IP
GigabitEthernet1/0/6: Other, IP
GigabitEthernet1/0/7: Other, IP
GigabitEthernet1/0/8: Other, IP
GigabitEthernet1/0/9: Other, IP
GigabitEthernet1/0/10: 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.

```
Device# show interfaces counters trunk
Port          TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi1/0/1       0              0              0
Gi1/0/2       0              0              0
Gi1/0/3       80678         0              0
Gi1/0/4       82320         0              0
Gi1/0/5       0              0              0
```

<output truncated>

show interfaces switchport

To display the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings, use the **show interfaces switchport** command in privileged EXEC mode.

show interfaces [*interface-id*] **switchport** [{**backup** [**detail**] | **module** *number*}]

Syntax Description	
<i>interface-id</i>	(Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member for stacking-capable switches, module, and port number) and port channels. The port channel range is 1 to 48.
backup	(Optional) Displays Flex Link backup interface configuration for the specified interface or all interfaces.
detail	(Optional) Displays detailed backup information for the specified interface or all interfaces on the switch or the stack.
module <i>number</i>	(Optional) Displays switchport configuration of all interfaces on the switch or specified stack member. The range is 1 to 8. This option is not available if you entered a specific interface ID.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines Use the **show interface switchport module** *number* command to display the switch port characteristics of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, there is no output.

This is an example of output from the **show interfaces switchport** command for a port. The table that follows describes the fields in the display.



Note Private VLANs are not supported in this release, so those fields are not applicable.

```
Device# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 10 (VLAN0010)
```



```

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: 11-20
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

```

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	Displays whether or not protected port is enabled (True) or disabled (False) on the interface.
Unknown unicast blocked Unknown multicast blocked	Displays whether or not unknown multicast and unknown unicast traffic is blocked on the interface.
Voice VLAN	Displays the VLAN ID on which voice VLAN is enabled.

Field	Description
Appliance trust	Displays the class of service (CoS) setting of the data packets of the IP phone.

This is an example of output from the **show interfaces switchport backup** command:

```
Device# show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
Gi1/0/1              Gi1/0/2              Active Up/Backup Standby
Gi3/0/3              Gi4/0/5              Active Down/Backup Up
Po1                  Po2                  Active Standby/Backup Up
```

In this example of output from the **show interfaces switchport backup** command, VLANs 1 to 50, 60, and 100 to 120 are configured on the switch:

```
Device(config)# interface gigabitethernet 2/0/6
Device(config-if)# switchport backup interface gigabitethernet 2/0/8
prefer vlan 60,100-120
```

When both interfaces are up, Gi2/0/8 forwards traffic for VLANs 60, 100 to 120, and Gi2/0/6 will forward traffic for VLANs 1 to 50.

```
Device# show interfaces switchport backup

Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
GigabitEthernet2/0/6  GigabitEthernet2/0/8  Active Up/Backup Up
Vlans on Interface Gi 2/0/6: 1-50
Vlans on Interface Gi 2/0/8: 60, 100-120
```

When a Flex Link interface goes down (LINK_DOWN), VLANs preferred on this interface are moved to the peer interface of the Flex Link pair. In this example, if interface Gi2/0/6 goes down, Gi2/0/8 carries all VLANs of the Flex Link pair.

```
Device# show interfaces switchport backup

Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
GigabitEthernet2/0/6  GigabitEthernet2/0/8  Active Down/Backup Up
Vlans on Interface Gi 2/0/6:
Vlans on Interface Gi 2/0/8: 1-50, 60, 100-120
```

When a Flex Link interface comes up, VLANs preferred on this interface are blocked on the peer interface and moved to the forwarding state on the interface that has just come up. In this example, if interface Gi2/0/6 comes up, then VLANs preferred on this interface are blocked on the peer interface Gi2/0/8 and forwarded on Gi2/0/6.

```
Device# show interfaces switchport backup

Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
GigabitEthernet2/0/6  GigabitEthernet2/0/8  Active Up/Backup Up
Vlans on Interface Gi 2/0/6: 1-50
```

```
Vlans on Interface Gi 2/0/8: 60, 100-120
```

show interfaces transceiver

To display the physical properties of a small form-factor pluggable (SFP) module interface, use the **show interfaces transceiver** command in EXEC mode.

show interfaces [*interface-id*] **transceiver** [{**detail** | **module number** | **properties** | **supported-list** | **threshold-table**}]

Syntax Description	
<i>interface-id</i>	(Optional) ID of the physical interface, including type, stack member (stacking-capable switches only) module, and port number.
detail	(Optional) Displays 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.
module number	(Optional) Limits display to interfaces on module on the switch. The range is 1 to 8. This option is not available if you entered a specific interface ID.
properties	(Optional) Displays speed, duplex, and inline power settings on an interface.
supported-list	(Optional) Lists all supported transceivers.
threshold-table	(Optional) Displays alarm and warning threshold table.

Command Modes	
	User EXEC
	Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Examples

This is an example of output from the **show interfaces *interface-id* transceiver properties** command:

```
Device# show interfaces gigabitethernet1/0/50 transceiver properties
Diagnostic Monitoring is not implemented.
Name : Gi1/0/50
Administrative Speed: auto
Administrative Duplex: auto
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
Operational Speed: 1000
Operational Duplex: full
Operational Auto-MDIX: on
Media Type: 10/100/1000BaseTX
```

This is an example of output from the **show interfaces *interface-id* transceiver detail** command:

```

Device# show interfaces gigabitethernet1/1/1 transceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is internally 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.

```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi1/1/1	29.9	74.0	70.0	0.0	-4.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi1/1/1	3.28	3.60	3.50	3.10	3.00

Port	Optical Transmit Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1/1	1.8	7.9	3.9	0.0	-4.0

Port	Optical Receive Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1/1	-23.5	-5.0	-9.0	-28.2	-32.2

This is an example of output from the **show interfaces transceiver threshold-table** command:

```

Device# show interfaces transceiver threshold-table

```

	Optical Tx	Optical Rx	Temp	Laser Bias current	Voltage

DWDM GBIC					
Min1	-4.00	-32.00	-4	N/A	4.65
Min2	0.00	-28.00	0	N/A	4.75
Max2	4.00	-9.00	70	N/A	5.25
Max1	7.00	-5.00	74	N/A	5.40
DWDM SFP					
Min1	-4.00	-32.00	-4	N/A	3.00
Min2	0.00	-28.00	0	N/A	3.10
Max2	4.00	-9.00	70	N/A	3.50
Max1	8.00	-5.00	74	N/A	3.60
RX only WDM GBIC					
Min1	N/A	-32.00	-4	N/A	4.65
Min2	N/A	-28.30	0	N/A	4.75
Max2	N/A	-9.00	70	N/A	5.25
Max1	N/A	-5.00	74	N/A	5.40
DWDM XENPAK					
Min1	-5.00	-28.00	-4	N/A	N/A
Min2	-1.00	-24.00	0	N/A	N/A
Max2	3.00	-7.00	70	N/A	N/A
Max1	7.00	-3.00	74	N/A	N/A
DWDM X2					
Min1	-5.00	-28.00	-4	N/A	N/A
Min2	-1.00	-24.00	0	N/A	N/A
Max2	3.00	-7.00	70	N/A	N/A

show interfaces transceiver

Max1	7.00	-3.00	74	N/A	N/A
DWDM XFP					
Min1	-5.00	-28.00	-4	N/A	N/A
Min2	-1.00	-24.00	0	N/A	N/A
Max2	3.00	-7.00	70	N/A	N/A
Max1	7.00	-3.00	74	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

<output truncated>

show ip ports all

To display all the open ports on the device, use the **show ip ports all** command in EXEC or User EXEC mode.

show ip ports all

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes User EXEC, Privileged EXEC

Command History	Release	Modification
	15.2(5) E1	This command was introduced.

The following is a sample output from **show ip ports all** command:

```
switch# show ip ports all
TCB Proto Local Address Foreign Address State PID/Program Name
Local Address Foreign Address (state)
tcp *:4786 *: * LISTEN 224/[IOS]SMI IBC server process
tcp *:443 *: * LISTEN 286/[IOS]HTTP CORE
tcp *:443 *: * LISTEN 286/[IOS]HTTP CORE
tcp *:80 *: * LISTEN 286/[IOS]HTTP CORE
tcp *:80 *: * LISTEN 286/[IOS]HTTP CORE
udp *:10002 *: * 0/[IOS] Unknown
udp *:2228 0.0.0.0:0 318/[IOS]L2TRACE SERVER
```

switch#

The table below shows the field descriptions.

Field	Description
Protocol	Transport protocol used
Foreign Address	Remote / peer address
State	State of connection : listen / establishment / connected
PID/Program Name	Process id / process name
Local Address	Device IP address

Related Commands **show tcp brief all**
show ip sockets

show network-policy profile

To display the network-policy profiles, use the **show network policy profile** command in privileged EXEC mode.

show network-policy profile [*profile-number*]

Syntax Description	<i>profile-number</i> (Optional) Displays the network-policy profile number. If no profile is entered, all network-policy profiles appear.	
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

This is an example of output from the **show network-policy profile** command:

```
Device# show network-policy profile
Network Policy Profile 60
  Interface:
    none
```


show power inline

To display the Power over Ethernet (PoE) status for the specified PoE port, the specified stack member, or for all PoE ports in the switch stack, use the **show power inline** command in EXEC mode.

show power inline [{**police** | **priority**}] [{*interface-id* | **module** *stack-member-number*}] [**detail**]

Syntax Description		
police	(Optional) Displays the power policing information about real-time power consumption.	
priority	(Optional) Displays the power inline port priority for each port.	
<i>interface-id</i>	(Optional) ID of the physical interface.	
module <i>stack-member-number</i>	(Optional) Limits the display to ports on the specified stack member. The range is 1 to 8. This keyword is supported only on stacking-capable switches.	
detail	(Optional) Displays detailed output of the interface or module.	

Command Modes	
	User EXEC
	Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Examples

This is an example of output from the **show power inline** command. The table that follows describes the output fields.

```
Device> show power inline
Module   Available   Used   Remaining
         (Watts)    (Watts) (Watts)
-----
1         n/a        n/a    n/a
2         n/a        n/a    n/a
3         1440.0    15.4   1424.6
4         720.0     6.3    713.7
Interface Admin  Oper   Power   Device   Class Max
         (Watts)
-----
Gi3/0/1  auto  off    0.0    n/a      n/a    30.0
Gi3/0/2  auto  off    0.0    n/a      n/a    30.0
Gi3/0/3  auto  off    0.0    n/a      n/a    30.0
Gi3/0/4  auto  off    0.0    n/a      n/a    30.0
Gi3/0/5  auto  off    0.0    n/a      n/a    30.0
Gi3/0/6  auto  off    0.0    n/a      n/a    30.0
Gi3/0/7  auto  off    0.0    n/a      n/a    30.0
Gi3/0/8  auto  off    0.0    n/a      n/a    30.0
```

```

Gi3/0/9   auto   off      0.0    n/a          n/a    30.0
Gi3/0/10  auto   off      0.0    n/a          n/a    30.0
Gi3/0/11  auto   off      0.0    n/a          n/a    30.0
Gi3/0/12  auto   off      0.0    n/a          n/a    30.0
<output truncated>

```

This is an example of output from the **show power inline interface-id** command on a switch port:

This is an example of output from the **show power inline module switch-number** command on stack member 3. The table that follows describes the output fields.

```

Device> show power inline module 3
Module   Available      Used      Remaining
         (Watts)        (Watts)   (Watts)
-----
3        865.0          864.0     1.0
Interface Admin  Oper      Power    Device   Class Max
         (Watts)
-----
Gi3/0/1  auto  power-deny 4.0     n/a      n/a    15.4
Gi3/0/2  auto  off        0.0     n/a      n/a    15.4
Gi3/0/3  auto  off        0.0     n/a      n/a    15.4
Gi3/0/4  auto  off        0.0     n/a      n/a    15.4
Gi3/0/5  auto  off        0.0     n/a      n/a    15.4
Gi3/0/6  auto  off        0.0     n/a      n/a    15.4
Gi3/0/7  auto  off        0.0     n/a      n/a    15.4
Gi3/0/8  auto  off        0.0     n/a      n/a    15.4
Gi3/0/9  auto  off        0.0     n/a      n/a    15.4
Gi3/0/10 auto  off        0.0     n/a      n/a    15.4
<output truncated>

```

Table 8: show power inline Field Descriptions

Field	Description
Available	The total amount of configured power ¹ on the PoE switch in watts (W).
Used	The amount of configured power that is allocated to PoE ports in watts.
Remaining	The amount of configured power in watts that is not allocated to ports in the system. (Available – Used = Remaining)
Admin	Administration mode: auto, off, static.
Oper	Operating mode: <ul style="list-style-type: none"> • on—The powered device is detected, and power is applied. • off—No PoE is applied. • faulty—Device detection or a powered device is in a faulty state. • power-deny—A powered device is detected, but no PoE is available, or the maximum wattage exceeds the detected powered-device maximum.
Power	The maximum amount of power that is allocated to the powered device in watts. This value is the same as the value in the <i>Cutoff Power</i> field in the show power inline police command output.

Field	Description
Device	The device type detected: n/a, unknown, Cisco powered-device, IEEE powered-device, or the name from CDP.
Class	The IEEE classification: n/a or a value from 0 to 4.
Max	The maximum amount of power allocated to the powered device in watts.
AdminPowerMax	The maximum amount power allocated to the powered device in watts when the switch polices the real-time power consumption. This value is the same as the <i>Max</i> field value.
AdminConsumption	The power consumption of the powered device in watts when the switch polices the real-time power consumption. If policing is disabled, this value is the same as the <i>AdminPowerMax</i> field value.

- ¹ The configured power is the power that you manually specify or that the switch specifies by using CDP power negotiation or the IEEE classification, which is different than the real-time power that is monitored with the power sensing feature.

This is an example of output from the **show power inline police** command on a stacking-capable switch:

```
Device> show power inline police
Module   Available   Used         Remaining
         (Watts)    (Watts)     (Watts)
-----
1        370.0      0.0         370.0
3        865.0     864.0       1.0

Interface Admin Oper   Admin   Oper   Cutoff Oper
         State State  Police  Police Power  Power
-----
Gi1/0/1  auto  off   none    n/a    n/a    0.0
Gi1/0/2  auto  off   log     n/a    5.4    0.0
Gi1/0/3  auto  off   errdisable n/a    5.4    0.0
Gi1/0/4  off   off   none    n/a    n/a    0.0
Gi1/0/5  off   off   log     n/a    5.4    0.0
Gi1/0/6  off   off   errdisable n/a    5.4    0.0
Gi1/0/7  auto  off   none    n/a    n/a    0.0
Gi1/0/8  auto  off   log     n/a    5.4    0.0
Gi1/0/9  auto  on    none    n/a    n/a    5.1
Gi1/0/10 auto  on    log     ok     5.4    4.2
Gi1/0/11 auto  on    log     log    5.4    5.9
Gi1/0/12 auto  on    errdisable ok     5.4    4.2
Gi1/0/13 auto  errdisable errdisable n/a    5.4    0.0
<output truncated>
```

In the previous example:

- The Gi1/0/1 port is shut down, and policing is not configured.
- The Gi1/0/2 port is shut down, but policing is enabled with a policing action to generate a syslog message.
- The Gi1/0/3 port is shut down, but policing is enabled with a policing action is to shut down the port.
- Device detection is disabled on the Gi1/0/4 port, power is not applied to the port, and policing is disabled.

- Device detection is disabled on the Gi1/0/5 port, and power is not applied to the port, but policing is enabled with a policing action to generate a syslog message.
- Device detection is disabled on the Gi1/0/6 port, and power is not applied to the port, but policing is enabled with a policing action to shut down the port.
- The Gi1/0/7 port is up, and policing is disabled, but the switch does not apply power to the connected device.
- The Gi1/0/8 port is up, and policing is enabled with a policing action to generate a syslog message, but the switch does not apply power to the powered device.
- The Gi1/0/9 port is up and connected to a powered device, and policing is disabled.
- The Gi1/0/10 port is up and connected to a powered device, and policing is enabled with a policing action to generate a syslog message. The policing action does not take effect because the real-time power consumption is less than the cutoff value.
- The Gi1/0/11 port is up and connected to a powered device, and policing is enabled with a policing action to generate a syslog message.
- The Gi1/0/12 port is up and connected to a powered device, and policing is enabled with a policing action to shut down the port. The policing action does not take effect because the real-time power consumption is less than the cutoff value.
- The Gi1/0/13 port is up and connected to a powered device, and policing is enabled with a policing action to shut down the port.

This is an example of output from the **show power inline police** *interface-id* command on a standalone switch. The table that follows describes the output fields.

Table 9: show power inline police Field Descriptions

Field	Description
Available	The total amount of configured power ² on the switch in watts (W).
Used	The amount of configured power allocated to PoE ports in watts.
Remaining	The amount of configured power in watts that is not allocated to ports in the system. (Available – Used = Remaining)
Admin State	Administration mode: auto, off, static.
Oper State	<p>Operating mode:</p> <ul style="list-style-type: none"> • errdisable—Policing is enabled. • faulty—Device detection on a powered device is in a faulty state. • off—No PoE is applied. • on—The powered device is detected, and power is applied. • power-deny—A powered device is detected, but no PoE is available, or the real-time power consumption exceeds the maximum power allocation. <p>Note The operating mode is the current PoE state for the specified PoE port, the specified stack member, or for all PoE ports on the switch.</p>

Field	Description
Admin Police	Status of the real-time power-consumption policing feature: <ul style="list-style-type: none"> errdisable—Policing is enabled, and the switch shuts down the port when the real-time power consumption exceeds the maximum power allocation. log—Policing is enabled, and the switch generates a syslog message when the real-time power consumption exceeds the maximum power allocation. none—Policing is disabled.
Oper Police	Policing status: <ul style="list-style-type: none"> errdisable—The real-time power consumption exceeds the maximum power allocation, and the switch shuts down the PoE port. log—The real-time power consumption exceeds the maximum power allocation, and the switch generates a syslog message. n/a—Device detection is disabled, power is not applied to the PoE port, or no policing action is configured. ok—Real-time power consumption is less than the maximum power allocation.
Cutoff Power	The maximum power allocated on the port. When the real-time power consumption is greater than this value, the switch takes the configured policing action.
Oper Power	The real-time power consumption of the powered device.

² The configured power is the power that you manually specify or that the switch specifies by using CDP power negotiation or the IEEE classification, which is different than the real-time power that is monitored with the power sensing feature.

show system mtu

To display the global maximum transmission unit (MTU) or maximum packet size set for the switch, use the **show system mtu** command in privileged EXEC mode.

show system mtu

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	This command was introduced.
	Cisco IOS Release 15.2(5)E	

Usage Guidelines For information about the MTU values and the stack configurations that affect the MTU values, see the **system mtu** command.

Examples

This is an example of output from the **show system mtu** command:

```
Device# show system mtu

System MTU size is 1500 bytes
System Jumbo MTU size is 1500 bytes
System Alternate MTU size is 1500 bytes
Routing MTU size is 1500 bytes
```

speed

To specify the speed of a 10/100/1000/2500/5000 Mbps port, use the **speed** command in interface configuration mode. To return to the default value, use the **no** form of this command.

```
speed {10 | 100 | 1000 | 2500 | 5000 | auto [{10 | 100 | 1000 | 2500 | 5000}] | nonegotiate}
no speed
```

Syntax Description	
10	Specifies that the port runs at 10 Mbps.
100	Specifies that the port runs at 100 Mbps.
1000	Specifies that the port runs at 1000 Mbps. This option is valid and visible only on 10/100/1000 Mb/s ports.
2500	Specifies that the port runs at 2500 Mbps. This option is valid and visible only on multi-Gigabit-supported Ethernet ports.
5000	Specifies that the port runs at 5000 Mbps. This option is valid and visible only on multi-Gigabit-supported Ethernet ports.
auto	Detects the speed at which the port should run, automatically, based on the port at the other end of the link. If you use the 10 , 100 , 1000 , 1000 , 2500 , or 5000 keyword with the auto keyword, the port autonegotiates only at the specified speeds.
nonegotiate	Disables autonegotiation, and the port runs at 1000 Mbps.

Command Default The default is **auto**.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.
	Cisco IOS XE Denali 16.3.1	This command was modified. The following keywords were added: 2500 and 5000 . These keywords are visible only on multi-Gigabit Ethernet port supporting devices.

Usage Guidelines You cannot configure speed on 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.

The new keywords, **2500** and **5000** are visible only on multi-Gigabit (m-Gig) Ethernet supporting devices.

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 configured on each end of the link, which might 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, 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.

Verify your settings using the **show interfaces** privileged EXEC command.

Examples

The following example shows how to set speed on a port to 100 Mbps:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed 100
```

The following example shows how to set a port to autonegotiate at only 10 Mbps:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto 10
```

The following example shows how to set a port to autonegotiate at only 10 or 100 Mbps:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto 10 100
```


switchport backup interface

To configure Flex Links, use the **switchport backup interface** command in interface configuration mode on a Layer 2 interface on the switch stack or on a standalone switch. To remove the Flex Links configuration, use the **no** form of this command.

```
switchport backup interface interface-id [{mmu primary vlan vlan-id|multicast fast-convergence
|preemption {delay seconds|mode {bandwidth|forced|off}}|prefer vlan vlan-id}]
no switchport backup interface interface-id [{mmu primary vlan|multicast fast-convergence|
preemption {delay|mode}|prefer vlan}]
```

Syntax Description		
	<i>interface-id</i>	ID of the physical interface.
	mmu	(Optional) Configures the MAC move update (MMU) for a backup interface pair.
	primary vlan <i>vlan-id</i>	(Optional) VLAN ID of the primary VLAN. The range is 1 to 4094.
	multicast fast-convergence	(Optional) Configures multicast fast convergence on the backup interface.
	preemption	(Optional) Configures a preemption scheme for a backup interface pair.
	delay <i>seconds</i>	Specifies a preemption delay. The range is 1 to 300 seconds. The default is 35 seconds.
	mode	Specifies the preemption mode.
	bandwidth	Specifies that a higher bandwidth interface is preferred.
	forced	Specifies that an active interface is preferred.
	off	Specifies that no preemption occurs from backup to active.
	prefer vlan <i>vlan-id</i>	(Optional) Specifies that VLANs are carried on the backup interfaces of a Flex Link pair. VLAN ID range is 1 to 4094.

Command Default The default is to have no Flex Links defined. The preemption mode is off. No preemption occurs. Preemption delay is set to 35 seconds.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines Flex Links are a pair of interfaces that provide backup to each other. With Flex Links configured, one link acts as the primary interface and forwards traffic, while the other interface is in standby mode, ready to begin forwarding traffic if the primary link shuts down. The interface being configured is referred to as the active link; the specified interface is identified as the backup link. The feature provides an alternative to the Spanning Tree Protocol (STP), allowing users to turn off STP and still retain basic link redundancy.

This command is available only for Layer 2 interfaces.

You can configure only one Flex Link backup link for any active link, and it must be a different interface from the active interface.

- An interface can belong to only one Flex Link pair. An interface can be a backup link for only one active link. An active link cannot belong to another Flex Link pair.
- A backup link does not have to be the same type (Fast Ethernet or Gigabit Ethernet, for instance) as the active link. However, you should configure both Flex Links with similar characteristics so that there are no loops or changes in behavior if the standby link begins to forward traffic.
- Neither of the links can be a port that belongs to an EtherChannel. However, you can configure two port channels (EtherChannel logical interfaces) as Flex Links, and you can configure a port channel and a physical interface as Flex Links, with either the port channel or the physical interface as the active link.
- If STP is configured on the switch, Flex Links do not participate in STP in all valid VLANs. If STP is not running, be sure that there are no loops in the configured topology.

This example shows how to configure two interfaces as Flex Links:

```
Device# configure terminal
Device(conf)# interface gigabitethernet1/0/1
Device(conf-if)# switchport backup interface gigabitethernet1/0/2
Device(conf-if)# end
```

This example shows how to configure the Gigabit Ethernet interface to always preempt the backup:

```
Device# configure terminal
Device(conf)# interface gigabitethernet1/0/1
Device(conf-if)# switchport backup interface gigabitethernet1/0/2 preempt forced
Device(conf-if)# end
```

This example shows how to configure the Gigabit Ethernet interface preemption delay time:

```
Device# configure terminal
Device(conf)# interface gigabitethernet1/0/1
Device(conf-if)# switchport backup interface gigabitethernet1/0/2 preempt delay 150
Device(conf-if)# end
```

This example shows how to configure the Gigabit Ethernet interface as the MMU primary VLAN:

```
Device# configure terminal
Device(conf)# interface gigabitethernet1/0/1
Device(conf-if)# switchport backup interface gigabitethernet1/0/2 mmu primary vlan 1021
Device(conf-if)# end
```

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

switchport block

To prevent unknown multicast or unicast packets from being forwarded, use the **switchport block** command in interface configuration mode. To allow forwarding unknown multicast or unicast packets, use the **no** form of this command.

```
switchport block {multicast | unicast}
no switchport block {multicast | unicast}
```

Syntax Description	<p>multicast Specifies that unknown multicast traffic should be blocked.</p> <p>Note Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.</p> <p>unicast Specifies that unknown unicast traffic should be blocked.</p>						
Command Default	Unknown multicast and unicast traffic is not blocked.						
Command Modes	Interface configuration						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E</td> </tr> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E		This command was introduced.
Release	Modification						
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E						
	This command was introduced.						
Usage Guidelines	<p>By default, all traffic with unknown MAC addresses is sent to all ports. You can block unknown multicast or unicast traffic on protected or nonprotected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.</p> <p>With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.</p> <p>Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.</p> <p>For more information about blocking packets, see the software configuration guide for this release.</p> <p>This example shows how to block unknown unicast traffic on an interface:</p> <pre>Device(config-if)# switchport block unicast</pre> <p>You can verify your setting by entering the show interfaces interface-id switchport privileged EXEC command.</p>						

system mtu

system mtu {*bytes* | **jumbo** *bytes*}

no system mtu

Syntax Description	<i>bytes</i>	Set the system MTU for ports that are set to 10 or 100 Mb/s. The range is 1500 to 1998 bytes. This is the maximum MTU received at 10/100-Mb/s Ethernet switch ports.
	jumbo <i>bytes</i>	Set the system jumbo MTU for Gigabit Ethernet ports operating at 1000 Mb/s or greater. The range is 1500 to 9000 bytes. This is the maximum MTU received at the physical port for Gigabit Ethernet ports.

Command Default The default MTU size for all ports is 1500 bytes.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines The switch does not support the MTU on a per-interface basis.

When you use this command to change the system MTU or 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 you enter with the **system mtu** and **system mtu jumbo** commands are not saved in the switch 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** and **system mtu jumbo** settings on the new switch and then reload the switch.

Gigabit Ethernet ports operating at 1000 Mb/s are not affected by the **system mtu** command, and 10/100-Mb/s ports are not affected by the **system mtu jumbo** command.

If you enter a value that is outside the range for the specific type of switch, the value is not accepted.

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

This example shows how to set the global system MTU size to 1600 bytes:

```
Device(config)# system mtu 1600
Changes to the system MTU will not take effect until the next reload is done

Device(config)#
```

This example shows how to set the global system MTU size to 6000 bytes:

```
Device(config)# system mtu jumbo 6000
Changes to the system jumbo MTU will not take effect until the next reload is done

Device(config)#
```

voice-signaling vlan (network-policy configuration)

To create a network-policy profile for the voice-signaling application type, use the **voice-signaling vlan** command in network-policy configuration mode. To delete the policy, use the **no** form of this command.

```
voice-signaling vlan {vlan-id [{cos cos-value | dscp dscp-value}] | dot1p [{cos l2-priority | dscp dscp}] | none | untagged}
```

Syntax Description	
vlan-id	(Optional) The VLAN for voice traffic. The range is 1 to 4094.
cos <i>cos-value</i>	(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5.
dscp <i>dscp-value</i>	(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46.
dot1p	(Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).
none	(Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.
untagged	(Optional) Configures the phone to send untagged voice traffic. This is the default for the phone.

Command Default No network-policy profiles for the voice-signaling application type are defined.
 The default CoS value is 5.
 The default DSCP value is 46.
 The default tagging mode is untagged.

Command Modes Network-policy profile configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines Use the **network-policy profile** global configuration command to create a profile and to enter network-policy profile configuration mode.

The voice-signaling application type is for network topologies that require a different policy for voice signaling than for voice media. This application type should not be advertised if all of the same network policies apply as those advertised in the voice policy TLV.

When you are in network-policy profile configuration mode, you can create the profile for voice-signaling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.

These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).

To return to privileged EXEC mode from the network-policy profile configuration mode, enter the **exit** command.

This example shows how to configure voice-signaling for VLAN 200 with a priority 2 CoS:

```
Device(config)# network-policy profile 1  
Device(config-network-policy)# voice-signaling vlan 200 cos 2
```

This example shows how to configure voice-signaling for VLAN 400 with a DSCP value of 45:

```
Device(config)# network-policy profile 1  
Device(config-network-policy)# voice-signaling vlan 400 dscp 45
```

This example shows how to configure voice-signaling for the native VLAN with priority tagging:

```
Device(config-network-policy)# voice-signaling vlan dot1p cos 4
```

voice vlan (network-policy configuration)

To create a network-policy profile for the voice application type, use the **voice vlan** command in network-policy configuration mode. To delete the policy, use the **no** form of this command.

```
voice vlan {vlan-id [{cos cos-value | dscp dscp-value}] | dot1p [{cos l2-priority | dscp dscp}] | none | untagged}
```

Syntax Description	
vlan-id	(Optional) The VLAN for voice traffic. The range is 1 to 4094.
cos <i>cos-value</i>	(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5.
dscp <i>dscp-value</i>	(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46.
dot1p	(Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).
none	(Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.
untagged	(Optional) Configures the phone to send untagged voice traffic. This is the default for the phone.

Command Default No network-policy profiles for the voice application type are defined.
 The default CoS value is 5.
 The default DSCP value is 46.
 The default tagging mode is untagged.

Command Modes Network-policy profile configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines Use the **network-policy profile** global configuration command to create a profile and to enter network-policy profile configuration mode.

The voice application type is for dedicated IP telephones and similar devices that support interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security through isolation from data applications.

When you are in network-policy profile configuration mode, you can create the profile for voice by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.

These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).

To return to privileged EXEC mode from the network-policy profile configuration mode, enter the **exit** command.

This example shows how to configure the voice application type for VLAN 100 with a priority 4 CoS:

```
Device(config)# network-policy profile 1  
Device(config-network-policy)# voice vlan 100 cos 4
```

This example shows how to configure the voice application type for VLAN 100 with a DSCP value of 34:

```
Device(config)# network-policy profile 1  
Device(config-network-policy)# voice vlan 100 dscp 34
```

This example shows how to configure the voice application type for the native VLAN with priority tagging:

```
Device(config-network-policy)# voice vlan dot1p cos 4
```




PART **III**

Layer 2

- [Layer 2 Commands, on page 121](#)



Layer 2 Commands

- [channel-group](#), on page 123
- [channel-protocol](#), on page 127
- [clear lacp](#), on page 128
- [clear pagp](#), on page 129
- [clear spanning-tree counters](#), on page 130
- [clear spanning-tree detected-protocols](#), on page 131
- [debug etherchannel](#), on page 132
- [debug lacp](#), on page 133
- [debug pagp](#), on page 134
- [debug platform etherchannel](#), on page 135
- [debug platform pm](#), on page 136
- [debug spanning-tree](#), on page 138
- [debug platform udd](#), on page 140
- [interface port-channel](#), on page 141
- [lacp port-priority](#), on page 143
- [lacp system-priority](#), on page 145
- [link state group](#), on page 146
- [link state track](#), on page 147
- [pagp learn-method](#), on page 148
- [pagp port-priority](#), on page 150
- [pagp timer](#), on page 151
- [port-channel load-balance](#), on page 152
- [rep admin vlan](#), on page 153
- [rep block port](#), on page 154
- [rep lsl-age-timer](#), on page 156
- [rep preempt delay](#), on page 157
- [rep preempt segment](#), on page 158
- [rep segment](#), on page 159
- [rep stcn](#), on page 161
- [show etherchannel](#), on page 162
- [show interfaces rep detail](#), on page 165
- [show lacp](#), on page 166
- [show link state group](#), on page 170

- show pagp, on page 171
- show platform backup interface, on page 173
- show platform etherchannel, on page 174
- show platform pm, on page 175
- show platform spanning-tree, on page 176
- show rep topology, on page 177
- show spanning-tree, on page 179
- show uddl, on page 183
- spanning-tree backbonefast, on page 186
- spanning-tree bpdupfilter, on page 187
- spanning-tree bpduguard, on page 188
- spanning-tree bridge assurance, on page 189
- spanning-tree cost, on page 191
- spanning-tree etherchannel guard misconfig, on page 192
- spanning-tree extend system-id, on page 193
- spanning-tree guard, on page 194
- spanning-tree link-type, on page 196
- spanning-tree loopguard default, on page 197
- spanning-tree mode, on page 198
- spanning-tree mst configuration, on page 199
- spanning-tree mst cost, on page 201
- spanning-tree mst forward-time, on page 202
- spanning-tree mst hello-time, on page 203
- spanning-tree mst max-age, on page 204
- spanning-tree mst max-hops, on page 205
- spanning-tree mst port-priority, on page 206
- spanning-tree mst pre-standard, on page 207
- spanning-tree mst priority, on page 208
- spanning-tree mst root, on page 209
- spanning-tree mst simulate pvst (global configuration), on page 210
- spanning-tree mst simulate pvst (interface configuration) , on page 212
- spanning-tree pathcost method, on page 214
- spanning-tree port-priority, on page 215
- spanning-tree portfast edge (global configuration), on page 216
- spanning-tree portfast edge (interface configuration), on page 218
- spanning-tree transmit hold-count, on page 220
- spanning-tree uplinkfast, on page 221
- spanning-tree vlan, on page 223
- switchport access vlan, on page 225
- switchport mode, on page 227
- switchport nonegotiate, on page 229
- uddl, on page 230
- uddl port, on page 232
- uddl reset, on page 234

channel-group

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

```
channel-group { auto | channel-group-number mode {active | auto [non-silent] | desirable
[non-silent] | on | passive} }
no channel-group
```

Syntax Description		
auto		Enables auto-LAG feature on individual port interface. By default, the auto-LAG feature is enabled on the port.
<i>channel-group-number</i>		Channel group number. The range is 1 to 24.
mode		Specifies the EtherChannel mode.
active		Unconditionally enables Link Aggregation Control Protocol (LACP).
auto		Enables the Port Aggregation Protocol (PAgP) only if a PAgP device is detected.
non-silent		(Optional) Configures the interface for nonsilent operation when connected to a partner that is PAgP-capable. Use in PAgP mode with the auto or desirable keyword when traffic is expected from the other device.
desirable		Unconditionally enables PAgP.
on		Enables the on mode.
passive		Enables LACP only if a LACP device is detected.

Command Default No channel groups are assigned.
No mode is configured.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

The LAN Lite feature set supports up to six EtherChannels.

The LAN Base feature set supports up to 24 EtherChannels; however, in mixed stack configurations, only six EtherChannels are supported.

For Layer 2 EtherChannels, the **channel-group** command automatically creates the port-channel interface when the channel group gets its first physical port. You do not have to use the **interface port-channel** command in global configuration mode to manually create a port-channel interface. 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.

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

You create Layer 3 port channels by using the **interface port-channel** command followed by the **no switchport** interface configuration command. Manually configure the port-channel logical interface before putting the interface into the channel group.

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.

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 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 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.

If you do not specify non-silent with the auto or desirable mode, silent is assumed. The silent mode is used when the device is connected to a device that is not PAgP-capable and rarely, if ever, sends packets. An 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 on mode, a usable EtherChannel exists only when both connected port groups are in the on mode.



Caution

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.

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.

Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same device or on different devices in the stack (but not in a cross-stack configuration). 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.

Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x authentication on an EtherChannel port, an error message appears, and IEEE 802.1x authentication is not enabled.

Do not configure a secure port as part of an EtherChannel or configure an EtherChannel port as a secure port.

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


Caution

Do not enable Layer 3 addresses on the physical EtherChannel ports. Do not assign bridge groups on the physical EtherChannel ports because it creates loops.

This example shows how to configure an EtherChannel on a single device in the stack. It assigns two static-access ports in VLAN 10 to channel 5 with the PAgP mode desirable:

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/1 - 2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode desirable
Device(config-if-range)# end
```

This example shows how to configure an EtherChannel on a single device in the stack. It assigns two static-access ports in VLAN 10 to channel 5 with the LACP mode active:

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/1 - 2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode active
Device(config-if-range)# end
```

This example shows how to configure a cross-stack EtherChannel in a device stack. It uses LACP passive mode and assigns two ports on stack member 2 and one port on stack member 3 as static-access ports in VLAN 10 to channel 5:

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/4 - 5
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode passive
Device(config-if-range)# exit
Device(config)# interface GigabitEthernet 3/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 10
Device(config-if)# channel-group 5 mode passive
Device(config-if)# exit
```

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

Related Topics

[channel-protocol](#), on page 127

[interface port-channel](#), on page 141

[show etherchannel](#), on page 162

[show lacp](#), on page 166

[show pagp](#), on page 171

channel-protocol

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

```
channel-protocol {lACP | pagp}
no channel-protocol
```

Syntax Description

lACP Configures an EtherChannel with the Link Aggregation Control Protocol (LACP).

pagp Configures an EtherChannel with the Port Aggregation Protocol (PAgP).

Command Default

No protocol is assigned to the EtherChannel.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	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.

You cannot configure PAgP on cross-stack configurations.

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

```
Device(config-if)# channel-protocol lACP
```

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

Related Topics

[channel-group](#), on page 123

[show etherchannel](#), on page 162

clear lacp

To clear Link Aggregation Control Protocol (LACP) channel-group counters, use the **clear lacp** command in privileged EXEC mode.

clear lacp [*channel-group-number*] **counters**

Syntax Description	
<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 24.
counters	Clears traffic counters.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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.

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

```
Device# clear lacp counters
```

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

```
Device# clear lacp 4 counters
```

You can verify that the information was deleted by entering the **show lacp counters** or the **show lacp channel-group-number counters** privileged EXEC command.

Related Topics

[show lacp](#), on page 166

[debug lacp](#), on page 133

clear pagp

To clear the Port Aggregation Protocol (PAgP) channel-group information, use the **clear pagp** command in privileged EXEC mode.

```
clear pagp [channel-group-number] counters
```

Syntax Description	<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 24.
	counters	Clears traffic counters.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		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.

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

```
Device# clear pagp counters
```

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

```
Device# clear pagp 10 counters
```

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

Related Topics

[show pagp](#), on page 171

[debug pagp](#), on page 134

clear spanning-tree counters

To clear the spanning-tree counters, use the **clear spanning-tree counters** command in privileged EXEC mode.

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

Syntax Description	interface <i>interface-id</i>	(Optional) Clears 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 24.
---------------------------	--------------------------------------	---

Command Default	None
------------------------	------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines	If the <i>interface-id</i> value is not specified, spanning-tree counters are cleared for all interfaces.
-------------------------	---

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

```
Device# clear spanning-tree counters
```

clear spanning-tree detected-protocols

To restart the protocol migration process and force renegotiation with neighboring devices on the interface, use the **clear spanning-tree detected-protocols** command in privileged EXEC mode.

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

Syntax Description	interface <i>interface-id</i>	(Optional) Restarts 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 24.
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

A device running the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol or the Multiple Spanning Tree Protocol (MSTP) supports a built-in protocol migration method that enables it to interoperate with legacy IEEE 802.1D devices. If a rapid-PVST+ or an MSTP device receives a legacy IEEE 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, the device sends only IEEE 802.1D BPDUs on that port. A multiple spanning-tree (MST) device 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).

The device 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.

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

```
Device# clear spanning-tree detected-protocols interface gigabitethernet2/0/1
```

debug etherchannel

To enable debugging of EtherChannels, use the **debug etherchannel** command in privileged EXEC mode. To disable debugging, use the **no** form of the command.

```
debug etherchannel [{all | detail | error | event | idb}]
no debug etherchannel [{all | detail | error | event | idb}]
```

Syntax Description

all	(Optional) Displays all EtherChannel debug messages.
detail	(Optional) Displays detailed EtherChannel debug messages.
error	(Optional) Displays EtherChannel error debug messages.
event	(Optional) Displays EtherChannel event messages.
idb	(Optional) Displays PAgP interface descriptor block debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	This command was introduced.

Usage Guidelines

The **undebug etherchannel** command is the same as the **no debug etherchannel** command.



Note

Although the **linecard** keyword is displayed in the command-line help, it is not supported.

When you enable debugging on a stack, it is enabled only on the stack's active switch. To enable debugging on a stack member, start a session from the stack's active switch by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member.

To enable debugging on a stack member without first starting a session on the stack's active switch, use the **remote command switch-number LINE** command in privileged EXEC mode.

This example shows how to display all EtherChannel debug messages:

```
Device# debug etherchannel all
```

This example shows how to display debug messages related to EtherChannel events:

```
Device# debug etherchannel event
```

Related Topics

[show etherchannel](#), on page 162

debug lacp

To enable debugging of Link Aggregation Control Protocol (LACP) activity, use the **debug lacp** command in privileged EXEC mode. To disable LACP debugging, use the **no** form of this command.

```
debug lacp [{all | event | fsm | misc | packet}]
```

```
no debug lacp [{all | event | fsm | misc | packet}]
```

Syntax Description

all	(Optional) Displays all LACP debug messages.
event	(Optional) Displays LACP event debug messages.
fsm	(Optional) Displays messages about changes within the LACP finite state machine.
misc	(Optional) Displays miscellaneous LACP debug messages.
packet	(Optional) Displays the receiving and transmitting LACP control packets.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

The **undebug etherchannel** command is the same as the **no debug etherchannel** command.

When you enable debugging on a stack, it is enabled only on the stack's active switch. To enable debugging on a stack member, start a session from the stack's active switch by using the **session *switch-number*** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member.

To enable debugging on a stack member without first starting a session on the stack's active switch, use the **remote command *switch-number* *LINE*** command in privileged EXEC mode.

This example shows how to display all LACP debug messages:

```
Device# debug LACP all
```

This example shows how to display debug messages related to LACP events:

```
Device# debug LACP event
```

debug pagp

To enable debugging of Port Aggregation Protocol (PAgP) activity, use the **debug pagp** command in privileged EXEC mode. To disable PAgP debugging, use the **no** form of this command.

```
debug pagp [{all | dual-active | event | fsm | misc | packet}]
no debug pagp [{all | dual-active | event | fsm | misc | packet}]
```

Syntax Description	
all	(Optional) Displays all PAgP debug messages.
dual-active	(Optional) Displays dual-active detection messages.
event	(Optional) Displays PAgP event debug messages.
fsm	(Optional) Displays messages about changes within the PAgP finite state machine.
misc	(Optional) Displays miscellaneous PAgP debug messages.
packet	(Optional) Displays the receiving and transmitting PAgP control packets.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines The **undebug pagp** command is the same as the **no debug pagp** command.

When you enable debugging on a stack, it is enabled only on the stack's active switch. To enable debugging on a stack member, start a session from the stack's active switch by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member.

To enable debugging on a stack member without first starting a session on the stack's active switch, use the **remote command switch-number LINE** command in privileged EXEC mode.

This example shows how to display all PAgP debug messages:

```
Device# debug pagp all
```

This example shows how to display debug messages related to PAgP events:

```
Device# debug pagp event
```


debug platform etherchannel

To enable debugging of platform-dependent EtherChannel events, use the **debug platform etherchannel** command in EXEC mode. To disable debugging, use the **no** form of this command.

```
debug platform etherchannel {init | link-up | rpc | warnings}
no debug platform etherchannel {init | link-up | rpc | warnings}
```

Syntax Description	
init	Displays EtherChannel module initialization debug messages.
link-up	Displays EtherChannel link-up and link-down related debug messages.
rpc	Displays EtherChannel remote procedure call (RPC) debug messages.
warnings	Displays EtherChannel warning debug messages.

Command Default Debugging is disabled.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines The **undebug platform etherchannel** command is the same as the **no debug platform etherchannel** command. When you enable debugging on a stack, it is enabled only on the stack's active switch. To enable debugging on a stack member, start a session from the stack's active switch by using the **session** *switch-number* command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member.

To enable debugging on a stack member without first starting a session on the stack's active switch, use the **remote command** *switch-number* *LINE* command in privileged EXEC mode.

This example shows how to display debug messages related to Etherchannel initialization:

```
Device# debug platform etherchannel init
```

debug platform pm

To enable debugging of the platform-dependent port manager software module, use the **debug platform pm** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug platform pm {all | atom | counters | errdisable | etherchnl | exceptions | gvi | 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 | stack-manager | 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 | stack-manager | sync | vlans}
```

Syntax Description

all	Displays all port manager debug messages.
atom	Displays ATOM related events.
counters	Displays counters for remote procedure call (RPC) debug messages.
errdisable	Displays error-disabled-related events debug messages.
etherchnl	Displays EtherChannel-related events debug messages.
exceptions	Displays system exception debug messages.
gvi	Displays IPe GVI-related messages.
hpm-events	Displays platform port manager event debug messages.
idb-events	Displays interface descriptor block (IDB)-related events debug messages.
if-numbers	Displays interface-number translation event debug messages.
ios-events	Displays Cisco IOS software events.
link-status	Displays interface link-detection event debug messages.
platform	Displays port manager function event debug messages.
pm-events	Displays port manager event debug messages.
pm-span	Displays port manager Switched Port Analyzer (SPAN) event debug messages.
pm-vectors	Displays port manager vector-related event debug messages.
detail	(Optional) Displays vector-function details.
rpc	Displays RPC-related messages.

general	(Optional) Displays general RPC-related messages.
oper-info	(Optional) Displays operational- and informational-related RPC messages.
state	(Optional) Displays administrative- and operational-related RPC messages.
vectors	(Optional) Displays vector-related RPC messages.
vp-events	(Optional) Displays virtual ports-related RPC messages.
soutput-vectors	Displays IDB output vector event debug messages.
stack-manager	Displays stack manager-related events debug messages. This keyword is supported only on stacking-capable switches.
sync	Displays operational synchronization and VLAN line-state event debug messages.
vlangs	Displays VLAN creation and deletion event debug messages.

Command Default Debugging is disabled

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines The **undebg platform pm** command is the same as the **no debug platform pm** command.

When you enable debugging on a stack, it is enabled only on the stack's active switch. To enable debugging on a stack member, start a session from the stack's active switch by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member.

To enable debugging on a stack member without first starting a session on the stack's active switch, use the **remote command switch-number LINE** command in privileged EXEC mode.

This example shows how to display debug messages related to the creation and deletion of VLANs:

```
Device# debug platform pm vlangs
```

debug spanning-tree

To enable debugging of spanning-tree activities, use the **debug spanning-tree** command in EXEC mode. To disable debugging, use the **no** form of this command.

```
debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | csuf/csrt | etherchannel | events
| exceptions | general | mstp | pvst+ | root | snmp | synchronization | switch | uplinkfast}
no debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | csuf/csrt | etherchannel |
events | exceptions | general | mstp | pvst+ | root | snmp | synchronization | switch | uplinkfast}
```

Syntax Description

all	Displays all spanning-tree debug messages.
backbonefast	Displays BackboneFast-event debug messages.
bpdu	Displays spanning-tree bridge protocol data unit (BPDU) debug messages.
bpdu-opt	Displays optimized BPDU handling debug messages.
config	Displays spanning-tree configuration change debug messages.
csuf/csrt	Displays cross-stack UplinkFast and cross-stack rapid transition activity debug messages.
etherchannel	Displays EtherChannel-support debug messages.
events	Displays spanning-tree topology event debug messages.
exceptions	Displays spanning-tree exception debug messages.
general	Displays general spanning-tree activity debug messages.
mstp	Displays Multiple Spanning Tree Protocol (MSTP) events.
pvst+	Displays per-VLAN spanning-tree plus (PVST+) event debug messages.
root	Displays spanning-tree root-event debug messages.
snmp	Displays spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.
switch	Displays device 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 device platforms.
synchronization	Displays the spanning-tree synchronization event debug messages.
uplinkfast	Displays UplinkFast-event debug messages.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines The **undebg spanning-tree** command is the same as the **no debug spanning-tree** command.

When you enable debugging on a stack, it is enabled only on the stack's active switch. To enable debugging on a stack member, start a session from the stack's active switch by using the **session** *switch-number* command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member.

To enable debugging on a stack member without first starting a session on the stack's active switch, use the **remote command** *switch-number* *LINE* command in privileged EXEC mode.

This example shows how to display all spanning-tree debug messages:

```
Device# debug spanning-tree all
```

debug platform udd

To enable debugging of the platform-dependent UniDirectional Link Detection (UDLD) software, use the **debug platform udd** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug platform udd [{all | error | switch | rpc} {events | messages}]
no platform udd [{all | error | rpc} {events | messages}]
```

Syntax Description	
all	(Optional) Displays all UDLD debug messages.
error	(Optional) Displays error condition debug messages.
rpc {events messages}	(Optional) Displays UDLD remote procedure call (RPC) debug messages. The keywords have these meanings: <ul style="list-style-type: none"> • events—Displays UDLD RPC events. • messages—Displays UDLD RPC messages.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines The **undebug platform udd** command is the same as the **no debug platform udd** command.

When you enable debugging on a stack, it is enabled only on the stack's active switch. To enable debugging on a stack member, start a session from the stack's active switch by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the stack member.

To enable debugging on a stack member without first starting a session on the stack's active switch, use the **remote command switch-number LINE** command in privileged EXEC mode.

interface port-channel

To access or create a port channel, use the **interface port-channel** command in global configuration mode. Use the **no** form of this command to remove the port channel.

```
interface port-channel port-channel-number
no interface port-channel
```

Syntax Description

port-channel-number (Optional) Channel group number. The range is 1 to 24.

Command Default

No port channel logical interfaces are defined.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	This command was introduced.

Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface before assigning physical ports to a channel group. Instead, you can use the **channel-group** interface configuration command, which automatically creates the port-channel interface when the channel group obtains 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.

You create Layer 3 port channels by using the **interface port-channel** command followed by the **no switchport** interface configuration command. You should manually configure the port-channel logical interface before putting the interface into the channel group.

Only one port channel in a channel group is allowed.



Caution

When using a port-channel interface as a routed port, do not assign Layer 3 addresses on the physical ports that are assigned to the channel group.



Caution

Do not assign bridge groups on the physical ports in a channel group used as a Layer 3 port channel interface because it creates loops. You must also disable spanning tree.

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 on the physical port and not on the port channel interface.
- Do not configure a port that is an active member of an EtherChannel as an IEEE 802.1x port. If IEEE 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

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

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

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

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

Related Topics

[channel-group](#), on page 123

[show etherchannel](#), on page 162

lACP port-priority

To configure the port priority for the Link Aggregation Control Protocol (LACP), use the **lACP port-priority** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

lACP port-priority *priority*
no lACP port-priority

Syntax Description

priority Port priority for LACP. The range is 1 to 65535.

Command Default

The default is 32768.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	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), then an internal value for the port number determines the priority.



Note

The LACP port priorities are only effective if the ports are on the device that controls the LACP link. See the **lACP system-priority** global configuration command for determining which device 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 configuration guide for this release.

This example shows how to configure the LACP port priority on a port:

```
Device# interface gigabitEthernet2/0/1
Device(config-if)# lACP port-priority 1000
```

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

Related Topics

[channel-group](#), on page 123

[lACP system-priority](#), on page 145

[show lACP](#), on page 166

lACP system-priority

To configure the system priority for the Link Aggregation Control Protocol (LACP), use the **lACP system-priority** command in global configuration mode on the device. To return to the default setting, use the **no** form of this command.

lACP system-priority *priority*
no lACP system-priority

Syntax Description	<i>priority</i> System priority for LACP. The range is 1 to 65535.	
Command Default	The default is 32768.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines

The **lACP system-priority** command determines which device 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 device 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 device (the noncontrolling end of the link) are ignored.

In priority comparisons, numerically lower values have a higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both devices have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the device MAC address) determines which device is in control.

The **lACP system-priority** command applies to all LACP EtherChannels on the device.

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).

This example shows how to set the LACP system priority:

```
Device(config)# lACP system-priority 20000
```

You can verify your settings by entering the **show lACP sys-id** privileged EXEC command.

Related Topics

- [channel-group](#), on page 123
- [lACP port-priority](#), on page 143
- [show lACP](#), on page 166

link state group

To configure an interface as a member of a link-state group, use the **link state group** command in interface configuration mode. Use the **no** form of this command to remove an interface from a link-state group.

```
link state group [{number}]{downstream | upstream}
no link state group [{number}]{downstream | upstream}
```

Syntax Description		
	<i>number</i>	(Optional) Specifies the number of the link-state group. The range is 1 to 2. The default group number is 1.
	downstream	Configures the interface as a downstream interface in the group.
	upstream	Configures the interface as an upstream interface in the group.

Command Default No link-state group is configured.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines This command is supported only on the LAN Base image.

Add upstream interfaces to the link-state group before adding downstream interfaces, otherwise, the downstream interfaces move into error-disable mode. These are the limitations:

- An interface can be an upstream interface or a downstream interface.
- An interface can belong to only one link-state group.
- Only two link-state groups can be configured on a switch.

This example shows how to configure the interfaces as upstream in group 2:

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/1 -2
Device(config-if-range)# link state group 2 upstream
Device(config-if-range)# end
```

Related Topics

- [link state track](#), on page 147
- [show link state group](#), on page 170

link state track

To enable a link-state group, use the **link state track** command in global configuration mode. 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) Specifies the number of the link-state group. The range is 1 to 2. The default is 1.

Command Default

Link-state tracking is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

This command is supported only on the LAN Base image.

Use the **link state group** command to create and configure the link-state group. You then can use this command to enable the link-state group.

This example shows how to enable link-state group 2:

```
Device# configure terminal
Device(config)# link state track 2
Device(config)# end
```

Related Topics

[link state group](#) , on page 146

[show link state group](#) , on page 170

pagp learn-method

To learn the source address of incoming packets received from an EtherChannel port, use the **pagp learn-method** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
pagp learn-method {aggregation-port | physical-port}
no pagp learn-method
```

Syntax Description	<p>aggregation-port Specifies address learning on the logical port channel. The device sends packets to the source using any port in the EtherChannel. This setting is the default. With aggregation-port learning, it is not important on which physical port the packet arrives.</p> <p>physical-port Specifies address learning on the physical port within the EtherChannel. The device 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.</p>						
Command Default	The default is aggregation-port (logical port channel).						
Command Modes	Interface configuration						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)E</td> <td>Cisco IOS Release 15.2(5)E</td> </tr> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E		This command was introduced.
Release	Modification						
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E						
	This command was introduced.						

Usage Guidelines

The learn method must be configured the same at both ends of the link.

The device 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 device hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports.

When the link partner to the device is a physical learner, we recommend that you configure the device as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command. We also recommend that you 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.

This example shows how to set the learning method to learn the address on the physical port within the EtherChannel:

```
Device(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:

```
Device(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 Topics

[pagp port-priority](#), on page 150

[show pagp](#), on page 171

pagp port-priority

To select a port over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent, use the **pagp port-priority** command in interface configuration mode. 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. To return to the default setting, use the **no** form of this command.

pagp port-priority *priority*
no pagp port-priority

Syntax Description

priority Priority number. The range is from 0 to 255.

Command Default

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

The physical port with the highest priority that is operational and has membership in the same EtherChannel is the one selected for PAgP transmission.

The device 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 device 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 device is a physical learner, we recommend that you configure the device as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command. We also recommend that you 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.

This example shows how to set the port priority to 200:

```
Device(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 Topics

[pagp learn-method](#), on page 148

[port-channel load-balance](#), on page 152

[show pagp](#), on page 171

pagp timer

To set the PAgP timer expiration, use the **pagp timer** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
pagp timer time
no pagp timer
```

Syntax Description	<i>time</i> Specifies the number of seconds after which PAgP informational packets are timed-out. The range is 45 to 90.				
Command Default	None				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS 15.0(2)EX</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS 15.0(2)EX	This command was introduced.
Release	Modification				
Cisco IOS 15.0(2)EX	This command was introduced.				
Usage Guidelines	<p>This command is available for all interfaces configured as part of a PAgP port channel.</p> <p>This example shows how to set the PAgP timer expiration to 50 seconds:</p> <pre>Switch(config-if)# pagp timer 50</pre>				

port-channel load-balance

To set the load-distribution method among the ports in the EtherChannel, use the **port-channel load-balance** command in global configuration mode. To reset the load-balancing function to the default setting, use the **no** form of this command.

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	Specifies load distribution based on the destination host IP address.
dst-mac	Specifies load distribution 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	Specifies load distribution based on the source and destination host IP address.
src-dst-mac	Specifies load distribution based on the source and destination host MAC address.
src-ip	Specifies load distribution based on the source host IP address.
src-mac	Specifies load distribution 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.

Command Default The default is **src-mac**.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines You can verify your setting by entering the **show running-config** privileged EXEC command or the **show etherchannel load-balance** privileged EXEC command.

Examples This example shows how to set the load-distribution method to **dst-mac**:

```
Device(config)# port-channel load-balance dst-mac
```

rep admin vlan

To configure a Resilient Ethernet Protocol (REP) administrative VLAN for REP to transmit hardware flood layer (HFL) messages, use the **rep admin vlan** command in global configuration mode. To return to the default configuration with VLAN 1 as the administrative VLAN, use the **no** form of this command.

```
rep admin vlan vlan-id [segment segment-id]
no rep admin vlan vlan-id [segment segment-id]
```

Syntax Description	<i>vlan-id</i>	The REP administrative VLAN. This is a 48-bit static MAC address.
	segment <i>segment-id</i>	Configures the administrative VLAN for the specified segment. The segment ID range is from 1 to 1024.
Command Default	The default value of the administrative VLAN is VLAN 1.	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS Release 15.2(6)E1	This command was introduced.

Usage Guidelines

The range of the REP administrative VLAN is from 2 to 4094.

If you do not configure an administrative VLAN, the default VLAN is VLAN 1. There can be only one administrative VLAN on a device and on a segment.

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

The following example shows how to configure VLAN 100 as the REP administrative VLAN:

```
Device(config)# rep admin vlan 100
```

This example shows how to create an administrative VLAN per segment. Here VLAN 2 is configured as the administrative VLAN only for REP segment 2. All remaining segments that are not configured otherwise will, by default, have VLAN 1 as the administrative VLAN.

```
Device(config)# rep admin vlan 2 segment 2
```

Related Commands	Command	Description
	show interfaces rep detail	Displays detailed REP configuration and status for all interfaces or the specified interface, including the administrative VLAN.

rep block port

To configure a Resilient Ethernet Protocol (REP) VLAN load balancing on the REP primary edge port, use the **rep block port** command in interface configuration mode. To return to the default configuration with VLAN 1 as the administrative VLAN, use the **no** form of this command.

```
rep block port {id port-id | neighbor-offset | preferred} vlan {vlan-list | all}
no rep block port {id port-id | neighbor-offset | preferred}
```

Syntax Description

id <i>port-id</i>	Specifies the VLAN blocking alternate port by entering the unique port ID, which is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value.
<i>neighbor-offset</i>	Identifies the VLAN blocking alternate port by entering the offset number of a neighbor. The range is from -256 to +256; a value of 0 is invalid.
preferred	Selects the regular segment port previously identified as the preferred alternate port for VLAN load balancing.
vlan	Identifies the VLANs to be blocked.
<i>vlan-list</i>	VLAN ID or range of VLAN IDs to be displayed. Enter a VLAN ID from 1 to 4094 or a range or sequence of VLANs (such as 1-3, 22, 41-44) to be blocked.
all	Blocks all VLANs.

Command Default

The default behavior after you enter the **rep preempt segment** command in privileged EXEC (for manual preemption) is to block all VLANs at the primary edge port. This behavior remains until you configure the **rep block port** command.

If the primary edge port cannot determine which port is to be the alternate port, the default action is no preemption and no VLAN load balancing.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS Release 15.2(6)E1	This command was introduced.

Usage Guidelines

You must enter this command on the REP primary edge port.

When you select an alternate port by entering an offset number, this number identifies the downstream neighbor port of an edge port. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors. Do not enter an offset value of 1 because that is the offset number of the primary edge port itself.

If you have configured a preempt delay time by entering the **rep preempt delay seconds** command in interface configuration mode and a link failure and recovery occurs, VLAN load balancing begins after the configured preemption time period elapses without another link failure. The alternate port specified in the load-balancing

configuration blocks the configured VLANs and unblocks all other segment ports. If the primary edge port cannot determine the alternate port for VLAN balancing, the default action is no preemption.

Each port in a segment has a unique port ID. To determine the port ID of a port, enter the **show interfaces interface-id rep detail** command in privileged EXEC mode.

The following example shows how to configure REP VLAN load balancing.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep block port id 0009001818D68700 vlan 1-100
```

Related Commands

Command	Description
show interfaces rep detail	Displays detailed REP configuration and status for all interfaces or the specified interface, including the administrative VLAN.

rep lsl-age-timer

To configure the Resilient Ethernet Protocol (REP) link status layer (LSL) age-out timer value, use the **rep lsl-age-timer** command in interface configuration mode. To restore the default age-out timer value, use the **no** form of this command.

```
rep lsl-age-timer milliseconds
no rep lsl-age-timer milliseconds
```

Syntax Description	<i>milliseconds</i> REP LSL age-out timer value in milliseconds (ms). The range is from 120 ms to 10000 ms in multiples of 40 ms.
---------------------------	---

Command Default	The default LSL age-out timer value is 5 ms.
------------------------	--

Command Modes	Interface configuration (config-if)
----------------------	-------------------------------------

Command History	Release	Modification
	Cisco IOS Release 15.2(6)E1	This command was introduced.

Usage Guidelines	The rep lsl-age-timer command is used to configure the REP LSL age-out timer value. While configuring REP configurable timers, we recommend that you configure the REP LSL number of retries first and then configure the REP LSL age-out timer value.
-------------------------	---

The following example shows how to configure REP LSL age-out timer value.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 1 edge primary
Device(config-if)# rep lsl-age-timer 2000
```

Related Commands	Command	Description
	interface interface-type interface-name	Specifies a physical interface or port channel to receive STCNs.
	rep segment	Enables REP on an interface and assigns a segment ID.

rep preempt delay

To configure a waiting period after a segment port failure and recovery before Resilient Ethernet Protocol (REP) VLAN load balancing is triggered, use the **rep preempt delay** command in interface configuration mode. To remove the configured delay, use the **no** form of this command.

rep preempt delay *seconds*
no rep preempt delay

Syntax Description	<i>seconds</i> Number of seconds to delay REP preemption. The range is from 15 to 300 seconds. The default is manual preemption without delay.				
Command Default	REP preemption delay is not set. The default is manual preemption without delay.				
Command Modes	Interface configuration (config-if)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.2(6)E1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.2(6)E1	This command was introduced.
Release	Modification				
Cisco IOS Release 15.2(6)E1	This command was introduced.				

Usage Guidelines

You must enter this command on the REP primary edge port.

You must enter this command and configure a preempt time delay for VLAN load balancing to automatically trigger after a link failure and recovery.

If VLAN load balancing is configured, after a segment port failure and recovery, the REP primary edge port starts a delay timer before VLAN load balancing occurs. Note that the timer restarts after each link failure. When the timer expires, the REP primary edge port alerts the alternate port to perform VLAN load balancing (configured by using the **rep block port** interface configuration command) and prepares the segment for the new topology. The configured VLAN list is blocked at the alternate port, and all other VLANs are blocked at the primary edge port.

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

The following example shows how to configure a REP preemption time delay of 100 seconds on the primary edge port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep preempt delay 100
```

Related Commands

Command	Description
rep block port	Configures VLAN load balancing.
show interfaces rep detail	Displays detailed REP configuration and status for all interfaces or the specified interface, including the administrative VLAN.

rep preempt segment

To manually start Resilient Ethernet Protocol (REP) VLAN load balancing on a segment, use the **rep preempt segment** command in privileged EXEC mode.

rep preempt segment *segment-id*

Syntax Description	<i>segment-id</i> ID of the REP segment. The range is from 1 to 1024.
---------------------------	---

Command Default	Manual preemption is the default behavior.
------------------------	--

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	Cisco IOS Release 15.2(6)E1	This command was introduced.

Usage Guidelines

Enter this command on the segment, which has the primary edge port on the device.

Ensure that all the other segment configuration is completed before setting preemption for VLAN load balancing. When you enter the **rep preempt segment** *segment-id* command, a confirmation message appears before the command is executed because preemption for VLAN load balancing can disrupt the network.

If you do not enter the **rep preempt delay** *seconds* command in interface configuration mode on the primary edge port to configure a preemption time delay, the default configuration is to manually trigger VLAN load balancing on the segment. Use the **show rep topology** privileged EXEC command to see which port in the segment is the primary edge port.

If you do not configure VLAN load balancing, entering this command results in the default behavior; the primary edge port blocks all VLANs.

You configure VLAN load balancing by entering the **rep block port** command in interface configuration mode on the REP primary edge port before you manually start preemption.

The following example shows how to manually trigger REP preemption on segment 100.

```
Device# rep preempt segment 100
```

Related Commands	Command	Description
	rep block port	Configures VLAN load balancing.
	show rep topology	Displays REP topology information for a segment or for all segments.
	rep preempt delay	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.

rep segment

To enable Resilient Ethernet Protocol (REP) on an interface and to assign a segment ID to the interface, use the **rep segment** command in interface configuration mode. To disable REP on the interface, use the **no** form of this command.

```
rep segment segment-id [edge [no-neighbor] [primary] ] [preferred]
no rep segment
```

Syntax Description

<i>segment-id</i>	Segment for which REP is enabled. Assign a segment ID to the interface. The range is from 1 to 1024.
edge	(Optional) Configures the port as an edge port. Each segment has only two edge ports.
no-neighbor	(Optional) Specifies the segment edge as one with no external REP neighbor.
primary	(Optional) Specifies that the port is the primary edge port where you can configure VLAN load balancing. A segment has only one primary edge port.
preferred	(Optional) Specifies that the port is the preferred alternate port or the preferred port for VLAN load balancing.
Note	Configuring a port as a preferred port does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.

Command Default

REP is disabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS Release 15.2(6)E1	This command was introduced.

Usage Guidelines

REP ports must be a Layer 2 IEEE 802.1Q port or 802.1AD port. You must configure two edge ports on each REP segment, a primary edge port and a port to act as a secondary edge port.

If REP is enabled on two ports on a device, both ports must be either regular segment ports or edge ports. REP ports follow these rules:

- If only one port on a device is configured in a segment, the port should be an edge port.
- If two ports on a device belong to the same segment, both ports must be regular segment ports.
- If two ports on a device belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

REP interfaces come up in a blocked state and remain in a blocked state until notified that it is safe to unblock. Be aware of this to avoid sudden connection losses.

When REP is enabled on an interface, the default is for the port to be a regular segment port.

The following example shows how to enable REP on a regular (nonedge) segment port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100
```

The following example shows how to enable REP on a port and identify the port as the REP primary edge port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100 edge primary
```

The following example shows how to enable REP on a port and identify the port as the REP secondary edge port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100 edge
```

The following example shows how to enable REP as an edge no-neighbor port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 1 edge no-neighbor primary
```

rep stcn

To configure a Resilient Ethernet Protocol (REP) edge port to send segment topology change notifications (STCNs) to another interface or to other segments, use the **rep stcn** command in interface configuration mode. To disable the sending of STCNs to the interface or to the segment, use the **no** form of this command.

```
rep stcn {interface interface-id | segment segment-id-list}
no rep stcn {interface | segment}
```

Syntax Description

interface *interface-id* Specifies a physical interface or port channel to receive STCNs.

segment *segment-id-list* Specifies one REP segment or a list of segments to receive STCNs. The segment range is from 1 to 1024. You can also configure a sequence of segments (for example 3 to 5, 77, 100).

Command Default

Transmission of STCNs to other interfaces or segments is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS Release 15.2(6)E1	This command was introduced.

Usage Guidelines

Enter this command on a segment edge port to send STCNs to one or more segments or to an interface. You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

The following example shows how to configure a REP edge port to send STCNs to segments 25 to 50.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep stcn segment 25-50
```

show etherchannel

To display EtherChannel information for a channel, use the **show etherchannel** command in user EXEC mode.

```
show etherchannel [{channel-group-number} | {detail | port | port-channel | protocol | summary}]
| [{auto | detail | load-balance | port | port-channel | protocol | summary}]
```

Syntax Description		
	<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 24.
	auto	(Optional) Displays that Etherchannel is created automatically.
	detail	(Optional) Displays detailed EtherChannel information.
	load-balance	(Optional) Displays the load-balance or frame-distribution scheme among ports in the port channel.
	port	(Optional) Displays EtherChannel port information.
	port-channel	(Optional) Displays port-channel information.
	protocol	(Optional) Displays the protocol that is being used in the channel.
	summary	(Optional) Displays a one-line summary per channel group.

Command Default None

Command Modes User EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines If you do not specify a channel group number, all channel groups are displayed.

In the output, the passive port list field is displayed only for Layer 3 port channels. This field means that the physical port, which is still not up, is configured to be in the channel group (and indirectly is in the only port channel in the channel group).

This is an example of output from the **show etherchannel auto** command:

```
device# show etherchannel auto
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
```

A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1

```
Group Port-channel Protocol Ports
-----+-----+-----+-----
1      Po1(SUA)         LACP   Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

This is an example of output from the **show etherchannel channel-group-number detail** command:

```
Device> 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: Gi1/0/1
-----
Port state      = Up Mstr In-Bndl
Channel group = 1      Mode = Active      Gcchange = -
Port-channel   =      Po1GC = -      Pseudo port-channel = Po1
Port index     =      0Load = 0x00      Protocol = LACP

Flags: S - Device is sending Slow LACPDU      F - Device is sending fast LACPDU
      A - Device is in active mode.            P - Device is in passive mode.

Local information:

Port      Flags  State  LACP port  Admin  Oper  Port  Port
          1    2    3    4    5    6    7    8
Gi1/0/1  SA    bndl  32768     0x1   0x1   0x101 0x3D
Gi1/0/2  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    Gi1/0/1   Active    0
0      00    Gi1/0/2   Active    0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2
```

This is an example of output from the **show etherchannel channel-group-number summary** command:

```
Device> 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	Pol(SU)	LACP	Gi1/0/1(P) Gi1/0/2(P)

This is an example of output from the **show etherchannel *channel-group-number* port-channel** command:

```

Device> 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
Logical slot/port = 10/1 Number of ports = 2
Port state = Port-channel Ag-Inuse
Protocol = LACP

Ports in the Port-channel:

Index  Load  Port  EC state  No of bits
-----+-----+-----+-----+-----
0      00    Gi1/0/1 Active      0
0      00    Gi1/0/2 Active      0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2

```

This is an example of output from **show etherchannel protocol** command:

```

Device# show etherchannel protocol
Channel-group listing:
-----
Group: 1
-----
Protocol: LACP
Group: 2
-----
Protocol: PAgP

```

Related Topics

- [channel-group](#), on page 123
- [channel-protocol](#), on page 127
- [interface port-channel](#), on page 141

show interfaces rep detail

To display detailed Resilient Ethernet Protocol (REP) configuration and status for all interfaces or a specified interface, including the administrative VLAN, use the **show interfaces rep detail** command in privileged EXEC mode.

show interfaces [*interface-id*] **rep detail**

Syntax Description	<i>interface-id</i> (Optional) Physical interface used to display the port ID.	
Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS Release 15.2(6)E1	This command was introduced.
Usage Guidelines	Enter this command on a segment edge port to send STCNs to one or more segments or to an interface. You can verify your settings by entering the show interfaces rep detail privileged EXEC command.	

The following example shows how to display the REP configuration and status for a specified interface.

```
Device# show interfaces TenGigabitEthernet4/1 rep detail

TenGigabitEthernet4/1 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

Related Commands	Command	Description
	rep admin vlan	Configures a REP administrative VLAN for REP to transmit HFL messages.

show lacp

To display Link Aggregation Control Protocol (LACP) channel-group information, use the **show lacp** command in user EXEC mode.

show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor** | **sys-id**}

Syntax Description	
<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 24.
counters	Displays traffic information.
internal	Displays internal information.
neighbor	Displays neighbor information.
sys-id	Displays the system identifier that is being used by LACP. The system identifier consists of the LACP system priority and the device MAC address.

Command Default None

Command Modes User EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E
		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* to specify a channel group for all keywords except **sys-id**.

This is an example of output from the **show lacp counters** user EXEC command. The table that follows describes the fields in the display.

```
Device> show lacp counters
          LACPDU      Marker      Marker Response      LACPDU
Port      Sent  Recv      Sent  Recv      Sent  Recv      Pkts  Err
-----
Channel group:1
Gi2/0/1      19   10         0    0         0    0         0
Gi2/0/2      14    6         0    0         0    0         0
```

Table 10: show lacp counters Field Descriptions

Field	Description
LACPDU Sent and Recv	The number of LACP packets sent and received by a port.

Field	Description
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:

```
Device> 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

Port      Flags   State   LACP port   Admin   Oper   Port   Port
Port      Flags   State   Priority    Key     Key   Number State
Gi2/0/1   SA     bndl   32768      0x3    0x3   0x4   0x3D
Gi2/0/2   SA     bndl   32768      0x3    0x3   0x5   0x3D
```

The following table describes the fields in the display:

Table 11: show lacp internal Field Descriptions

Field	Description
State	<p>State of the specific port. These are the allowed values:</p> <ul style="list-style-type: none"> • ——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 handle 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 in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Field	Description
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	<p>State variables for the port, encoded as individual bits within a single octet with these meanings:</p> <ul style="list-style-type: none"> • bit0: LACP_Activity • bit1: LACP_Timeout • bit2: Aggregation • bit3: Synchronization • bit4: Collecting • bit5: Distributing • bit6: Defaulted • bit7: Expired <p>Note In the list above, bit7 is the MSB and bit0 is the LSB.</p>

This is an example of output from the **show lacp neighbor** command:

```

Device> 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:

Port      Partner          Partner          Partner
         System ID    Port Number     Age           Flags
Gi2/0/1   32768,0007.eb49.5e80  0xC             19s          SP

         LACP Partner    Partner          Partner
         Port Priority   Oper Key         Port State
         32768          0x3              0x3C

Partner's information:

```

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Gi2/0/2	32768,0007.eb49.5e80	0xD	15s	SP
	LACP Partner Port Priority	Partner Oper Key	Partner Port State	
	32768	0x3	0x3C	

This is an example of output from the **show lacp sys-id** command:

```
Device> 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 Topics

[clear lacp](#), on page 128

[debug lacp](#), on page 133

[lacp port-priority](#), on page 143

[lacp system-priority](#), on page 145

show link state group

To display link-state group information, use the **show link state group** command in privileged EXEC mode.

```
show link state group [{number}] [{detail}]
```

Syntax Description	<i>number</i> (Optional) Specifies the number of the link-state group number. The range is 1 to 2.
	<i>detail</i> (Optional) Displays detailed information about the link-state group.

Command Default	None
------------------------	------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

This command is supported only on the LAN Base image.

To display information about all link-state groups, enter this command without keywords. To display information about a specific link-state group enter the link-state group number.

The output for the **show link state group detail** displays information for only those link-state groups that have link-state tracking enabled or that have upstream or downstream interfaces configured. If the group does not have a configuration, the group is not shown as enabled or disabled.

This example shows the output from the **show link state group *number*** command:

```
Device# show link state group 1

Link State Group: 1      Status: Enabled. Down
```

This example shows the output from the **show link state group detail** command:

```
Device# show link state group detail

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi1/0/15(Dwn) Gi1/0/16(Dwn)
Downstream Interfaces : Gi1/0/11(Dis) Gi1/0/12(Dis) Gi1/0/13(Dis) Gi1/0/14(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi1/0/15(Dwn) Gi1/0/16(Dwn) Gi1/0/17(Dwn)
Downstream Interfaces : Gi1/0/11(Dis) Gi1/0/12(Dis) Gi1/0/13(Dis) Gi1/0/14(Dis)
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

Related Topics

[link state group](#), on page 146

[link state track](#), on page 147

show pagp

To display Port Aggregation Protocol (PAgP) channel-group information, use the **show pagp** command in EXEC mode.

```
show pagp [channel-group-number] {counters | dual-active | internal | neighbor}
```

Syntax Description	
	<i>channel-group-number</i> (Optional) Channel group number. The range is 1 to 24.
counters	Displays traffic information.
dual-active	Displays the dual-active status.
internal	Displays internal information.
neighbor	Displays neighbor information.

Command Default None

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		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.

Examples

This is an example of output from the **show pagp 1 counters** command:

```
Device> show pagp 1 counters
          Information      Flush
Port      Sent   Recv   Sent   Recv
-----
Channel group: 1
  Gi1/0/1   45    42     0     0
  Gi1/0/2   45    41     0     0
```

This is an example of output from the **show pagp dual-active** command:

```
Device> 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
Gi1/0/1       No               Device    Gi3/0/3   N/A
Gi1/0/2       No               Device    Gi3/0/4   N/A

<output truncated>
```

This is an example of output from the **show pagp 1 internal** command:

```
Device> 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

```

Port	Flags	State	Timers	Hello Interval	Partner Count	PAGP Priority	Learning Method	Group Ifindex
Gi1/0/1	SC	U6/S7	H	30s	1	128	Any	16
Gi1/0/2	SC	U6/S7	H	30s	1	128	Any	16

This is an example of output from the **show pagp 1 neighbor** command:

```
Device> 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

```

Port	Partner Name	Partner Device ID	Partner Port	Age	Flags	Partner Group Cap.
Gi1/0/1	device-p2	0002.4b29.4600	Gi01//1	9s	SC	10001
Gi1/0/2	device-p2	0002.4b29.4600	Gi1/0/2	24s	SC	10001

Related Topics

[clear pagp](#), on page 129

[debug pagp](#), on page 134

show platform backup interface

To display platform-dependent backup information used in a Flex Links configuration, use the **show platform backup interface** privileged EXEC command.

show platform backup interface [*interface-id* | **dummyQ**]

Syntax Description

interface-id (Optional) Backup information for all interfaces or the specified interface. The interface can be a physical interface or a port channel.

dummyQ (Optional) Displays dummy queue information.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

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.

show platform etherchannel

To display platform-dependent EtherChannel information, use the **show platform etherchannel** command in privileged EXEC mode.

show platform etherchannel {**data-structures** | **flags** | **time-stamps**}

Syntax Description		
	data-structures	Displays EtherChannel data structures.
	flags	Displays EtherChannel port flags.
	time-stamps	Displays EtherChannel time stamps.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines 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.

show platform pm

To display platform-dependent port manager information, use the **show platform pm** command in privileged EXEC mode.

```
show platform pm {counters | group-masks | idbs {active-idbs | deleted-idbs} | if-numbers | link-status
| module-info | platform-block | port-info interface-id | stack-view | vlan {info | line-state}}
```

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines The **stack-view** keyword is not supported on switches running the LAN Lite image.

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.

show platform spanning-tree

To display platform-dependent spanning-tree information, use the **show platform spanning-tree** privileged EXEC command.

show platform spanning-tree synchronization [{**detail** | **vlan** *vlan-id*}]

Syntax Description

synchronization	Displays spanning-tree state synchronization information.
detail	(Optional) Displays detailed spanning-tree information.
vlan <i>vlan-id</i>	(Optional) Displays VLAN device spanning-tree information for the specified VLAN. The range is 1 to 4094.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

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.

show rep topology

To display Resilient Ethernet Protocol (REP) topology information for a segment or for all segments, including the primary and secondary edge ports in the segment, use the **show rep topology** command in privileged EXEC mode.

show rep topology [**segment** *segment-id*] [**archive**] [**detail**]

Syntax Description		
segment <i>segment-id</i>		(Optional) Specifies the segment for which to display the REP topology information. The <i>segment-id</i> range is from 1 to 1024.
archive		(Optional) Displays the previous topology of the segment. This keyword is useful for troubleshooting a link failure.
detail		(Optional) Displays detailed REP topology information.
Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS Release 15.2(6)E1	This command was introduced.

The following is sample output from the **show rep topology** command.

```
Device# show rep topology

REP Segment 1
BridgeName      PortName      Edge Role
-----
10.64.106.63    Te5/4         Pri  Open
10.64.106.228  Te3/4         Open
10.64.106.228  Te3/3         Open
10.64.106.67   Te4/3         Open
10.64.106.67   Te4/4         Alt
10.64.106.63   Te4/4         Sec  Open

REP Segment 3
BridgeName      PortName      Edge Role
-----
10.64.106.63    Gi50/1        Pri  Open
SVT_3400_2      Gi0/3         Open
SVT_3400_2      Gi0/4         Open
10.64.106.68   Gi40/2        Open
10.64.106.68   Gi40/1        Open
10.64.106.63   Gi50/2        Sec  Alt
```

The following is sample output from the **show rep topology detail** command.

```
Device# show rep topology detail
```

```
REP Segment 1
10.64.106.63, Te5/4 (Primary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 1 / [-6]
10.64.106.228, Te3/4 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 2 / [-5]
10.64.106.228, Te3/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 00E
  Port Priority: 000
  Neighbor Number: 3 / [-4]
10.64.106.67, Te4/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1800
  Port Number: 008
  Port Priority: 000
  Neighbor Number: 4 / [-3]
10.64.106.67, Te4/4 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 0005.9b2e.1800
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 5 / [-2]
10.64.106.63, Te4/4 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 6 / [-1]
```

show spanning-tree

To display spanning-tree information for the specified spanning-tree instances, use the **show spanning-tree** command in privileged EXEC mode or user EXEC mode.

show spanning-tree [{**active** | **backbonefast** | **blockedports** | **bridge** | **detail** | **inconsistentports** | **interface** *interface-type interface-number* | **mst** | **pathcost** | **root** | **summary** [**totals**] | **uplinkfast** | **vlan** *vlan-id*}]

Syntax Description		
active		(Optional) Displays spanning-tree information on active interfaces only.
backbonefast		(Optional) Displays spanning-tree BackboneFast status.
blockedports		(Optional) Displays blocked port information.
bridge		(Optional) Displays status and configuration of this switch.
detail		(Optional) Displays detailed information.
inconsistentports		(Optional) Displays information about inconsistent ports.
interface <i>interface-type interface-number</i>		(Optional) Specifies the type and number of the interface.
mst		(Optional) Specifies multiple spanning-tree.
pathcost		(Optional) Displays spanning-tree pathcost options.
root		(Optional) Displays root-switch status and configuration.
summary		(Optional) Specifies a summary of port states.
totals		(Optional) Displays the total lines of the spanning-tree state section.
uplinkfast		(Optional) Displays spanning-tree UplinkFast status.
vlan <i>vlan-id</i>		(Optional) Specifies the VLAN ID. The range is 1 to 4094.

Command Modes	
	User EXEC
	Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines If you do not specify a *vlan-id* value when you use the **vlan** keyword, the command applies to spanning-tree instances for all VLANs.

This is an example of output from the **show spanning-tree active** command:

```

Device# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address    0001.42e2.cdd0
             Cost      3038
             Port      24 (GigabitEthernet2/0/1)
             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
-----
Gi2/0/1       Root FWD 3019      128.24  P2p
Gi0/1         Root FWD 3019      128.24  P2p
<output truncated>

```

This is an example of output from the **show spanning-tree detail** command:

```

Device# show spanning-tree detail
  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 1 (GigabitEthernet2/0/1), 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 (GigabitEthernet2/0/1) 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 summary** command:

```

Device# show spanning-tree interface mst configuration
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:

```

Device# show spanning-tree interface 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 interface mst interface interface-id** command:

```

Device# show spanning-tree interface mst configuration
GigabitEthernet2/0/1 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 interface mst instance-id** command:

```

Device# show spanning-tree interface mst 0
GigabitEthernet2/0/1 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

```

show spanning-tree

```
0          root FWD  200000  128  1,12,14-4094
```


show udld

To display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port, use the **show udld** command in user EXEC mode.

```
show udld [{interface_id | neighbors}]
```

Syntax Description	<i>interface-id</i> (Optional) ID of the interface and port number. Valid interfaces include physical ports, VLANs, and port channels.						
	neighbors (Optional) Displays neighbor information only.						
Command Default	None						
Command Modes	User EXEC						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E</td> </tr> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E		This command was introduced.
Release	Modification						
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E						
	This command was introduced.						
Usage Guidelines	<p>If you do not enter an interface ID, administrative and operational UDLD status for all interfaces appear.</p> <p>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. The table that follows describes the fields in this display.</p> <pre>Device> show udld gigabitethernet2/0/1 Interface gi2/0/1 --- 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: Gi2/0/1 Neighbor echo 1 device: Switch-B Neighbor echo 1 port: Gi2/0/2 Message interval: 5 CDP Device name: Switch-A</pre>						

Table 12: show udld Field Descriptions

Field	Description
Interface	The interface on the local device configured for UDLD.

Field	Description
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.

Field	Description
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).

This is an example of output from the **show uddl neighbors** command:

```
Device# show uddl neighbors
Port      Device Name      Device ID  Port-ID  OperState
-----
Gi2/0/1   Switch-A          1          Gi2/0/1  Bidirectional
Gi3/0/1   Switch-A          2          Gi3/0/1  Bidirectional
```

Related Topics

- [uddl](#), on page 230
- [uddl port](#), on page 232
- [uddl reset](#), on page 234

spanning-tree backbonefast

To enable BackboneFast to allow a blocked port on a device to change immediately to a listening mode, use the **spanning-tree backbonefast** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree backbonefast

no spanning-tree backbonefast

Syntax Description This command has no arguments or keywords.

Command Default BackboneFast is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines Enable BackboneFast so that the device detects indirect link failures and starts the spanning-tree reconfiguration sooner than it would under normal spanning-tree rules.

You can configure BackboneFast for rapid PVST+ or for multiple spanning-tree (MST) mode; however, the feature remains disabled until you change the spanning-tree mode to PVST+.

Use the **show spanning-tree** privileged EXEC command to verify your settings.

Examples

The following example shows how to enable BackboneFast on the device:

```
Device(config)# spanning-tree backbonefast
```

Related Topics

[show spanning-tree](#), on page 179

spanning-tree bpdudfilter

To enable bridge protocol data unit (BPDU) filtering on the interface, use the **spanning-tree bpdudfilter** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
spanning-tree bpdudfilter {enable | disable}
no spanning-tree bpdudfilter
```

Syntax Description

enable Enables BPDU filtering on this interface.

disable Disables BPDU filtering on this interface.

Command Default

The setting that is already configured when you enter the **spanning-tree portfast bpdudfilter default** command.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

This command has three states:

- **spanning-tree bpdudfilter enable** —Unconditionally enables BPDU filtering on the interface.
- **spanning-tree bpdudfilter disable** —Unconditionally disables BPDU filtering on the interface.
- **no spanning-tree bpdudfilter** —Enables BPDU filtering on the interface if the interface is in the operational PortFast state and if you configure the **spanning-tree portfast bpdudfilter default** command.



Caution

Be careful when you enter the **spanning-tree bpdudfilter enable** command. Enabling BPDU filtering on an interface is similar to disabling the spanning tree for this interface. If you do not use this command correctly, you might create bridging loops.

You can enable BPDU filtering when the device is operating in the per-VLAN spanning-tree plus (PVST+) mode, the rapid-PVST mode, or the multiple spanning-tree (MST) mode.

You can globally enable BPDU filtering on all Port Fast-enabled interfaces with the **spanning-tree portfast bpdudfilter default** command.

The **spanning-tree bpdudfilter enable** command overrides the PortFast configuration.

Examples

This example shows how to enable BPDU filtering on this interface:

```
Device(config-if) # spanning-tree bpdudfilter enable
Device(config-if) #
```

Related Topics

[spanning-tree portfast edge \(interface configuration\)](#), on page 218

spanning-tree bpduguard

To enable bridge protocol data unit (BPDU) guard on the interface, use the **spanning-tree bpduguard** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
spanning-tree bpduguard {enable | disable}
no spanning-tree bpduguard
```

Syntax Description

enable Enables BPDU guard on this interface.

disable Disables BPDU guard on this interface.

Command Default

The setting that is already configured when you enter the **spanning-tree portfast bpduguard default** command.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

Use the BPDU guard feature in a service-provider environment to prevent an access port from participating in the spanning tree. If the port still receives a BPDU, it is put in the error-disabled state as a protective measure. This command has three states:

- **spanning-tree bpduguard enable** —Unconditionally enables BPDU guard on the interface.
- **spanning-tree bpduguard disable** —Unconditionally disables BPDU guard on the interface.
- **no spanning-tree bpduguard** —Enables BPDU guard on the interface if the interface is in the operational PortFast state and if you configure the **spanning-tree portfast bpduguard default** command.

Examples

This example shows how to enable BPDU guard on an interface:

```
Device(config-if)# spanning-tree bpduguard enable
Device(config-if)#
```

Related Topics

[spanning-tree portfast edge \(interface configuration\)](#), on page 218

spanning-tree bridge assurance

To enable Bridge Assurance on your network, use the **spanning-tree bridge assurance** command. To disable the feature, use the **no** form of the command.

spanning-tree bridge assurance
no spanning-tree bridge assurance

Syntax Description	This command has no arguments or keywords.	
Command Default	Bridge Assurance is enabled	
Command Modes	Global configuration mode	
Command History	Release	Modification
	3.8.0E and 15.2.(4)E	Support for the command was introduced.

Usage Guidelines

This feature protects your network from bridging loops. It monitors the receipt of BPDUs on point-to-point links on all network ports. When a port does not receive BPDUs within the allotted hello time period, the port is put into a blocked state (the same as a port inconsistent state, which stops forwarding of frames). When the port resumes receipt of BPDUs, the port resumes normal spanning tree operations.

By default, Bridge Assurance is enabled on all operational network ports, including alternate and backup ports. If you have configured the **spanning-tree portfast network** command on all the required ports that are connected Layer 2 switches or bridges, Bridge Assurance is automatically effective on all those network ports.

Only Rapid PVST+ and MST spanning tree protocols support Bridge Assurance. PVST+ does not support Bridge Assurance.

For Bridge Assurance to work properly, it must be supported and configured on both ends of a point-to-point link. If the device on one side of the link has Bridge Assurance enabled and the device on the other side does not, then the connecting port is blocked (a Bridge Assurance inconsistent state). We recommend that you enable Bridge Assurance throughout your network.

To enable Bridge Assurance on a port, BPDU filtering and BPDU Guard must be disabled.

You can enable Bridge Assurance in conjunction with Loop Guard.

You can enable Bridge Assurance in conjunction with Root Guard. The latter is designed to provide a way to enforce the root bridge placement in the network.

Disabling Bridge Assurance causes all configured network ports to behave as normal spanning tree ports.

Use the **show spanning-tree summary** command to see if the feature is enabled on a port.

Example

The following example shows how to enable Bridge Assurance on all network ports on the switch, and how to configure a network port:

```
Device(config)# spanning-tree bridge assurance
```

```
Device(config)# interface gigabitethernet 5/8
Device(config-if)# spanning-tree portfast network
Device(config-if)# exit
```

This example show how to display spanning tree information and verify if Bridge Assurance is enabled. Look for these details in the output:

- Portfast Default—Network
- Bridge Assurance—Enabled

```
Device# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0199-VLAN0200, VLAN0128
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is network
Portfast Edge BPDU Guard Default is disabled
Portfast Edge BPDU Filter Default is disabled
Loopguard Default is enabled
PVST Simulation Default is enabled but inactive in rapid-pvst mode
Bridge Assurance is enabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short
Name Blocking Listening Learning Forwarding STP Active
-----
VLAN0199 0 0 0 5 5
VLAN0200 0 0 0 4 4
VLAN0128 0 0 0 4 4
-----
3 vlans 0 0 0 13 13
```

Related Topics

- [spanning-tree portfast edge \(global configuration\)](#), on page 216
- [spanning-tree portfast edge \(interface configuration\)](#), on page 218
- [show spanning-tree](#), on page 179

spanning-tree cost

To set the path cost of the interface for Spanning Tree Protocol (STP) calculations, use the **spanning-tree cost** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

```
spanning-tree [vlan vlan-id] cost cost
no spanning-tree cost
```

Syntax Description

vlan <i>vlan-id</i>	(Optional) Specifies the VLAN range associated with the spanning-tree instance. The range of VLAN IDs is 1 to 4094.
<i>cost</i>	The path cost; valid values are from 1 to 200000000.

Command Default

The default path cost is computed from the bandwidth setting of the interface. Default path costs are:

- 1 Gb/s: 4
- 100 Mb/s: 19
- 10 Mb/s: 100

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

When you specify VLANs associated with a spanning tree instance, you can specify a single VLAN identified by a VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLAN IDs separated by a comma.

When you specify a value for the cost argument, higher values indicate higher costs. This range applies regardless of the protocol type specified.

Examples

This example shows how to set the path cost on an interface to a value of 250:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# spanning-tree cost 250
```

This example shows how to set the path cost to 300 for VLANs 10, 12 to 15, and 20:

```
Device(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

Related Topics

- [show spanning-tree](#), on page 179
- [spanning-tree port-priority](#), on page 215
- [spanning-tree vlan](#), on page 223

spanning-tree etherchannel guard misconfig

To display an error message when the device detects an EtherChannel misconfiguration, use the **spanning-tree etherchannel guard misconfig** command in global configuration mode. To disable the error message, use the **no** form of this command.

spanning-tree etherchannel guard misconfig
no spanning-tree etherchannel guard misconfig

Syntax Description This command has no arguments or keywords.

Command Default Error messages are displayed.

Command Modes Global configuration

Command History

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines When the device detects an EtherChannel misconfiguration, this error message is displayed:

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in err-disable state.
```

To determine which local ports are involved in the misconfiguration, enter the **show interfaces status err-disabled** command. To check the EtherChannel configuration on the remote device, enter the **show etherchannel summary** command on the remote device.

After you correct the configuration, enter the **shutdown** and the **no shutdown** commands on the associated port-channel interface.

Examples

This example shows how to enable the EtherChannel-guard misconfiguration:

```
Device(config)# spanning-tree etherchannel guard misconfig
```

Related Topics

[show etherchannel](#), on page 162

spanning-tree extend system-id

To enable extended system identification, use the **spanning-tree extend system-id** command in global configuration mode. To disable extended system identification, use the **no** form of this command.

spanning-tree extend system-id
no spanning-tree extend system-id

Syntax Description This command has no arguments or keywords.

Command Default The extended system ID is enabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines The spanning tree uses the extended system ID, the device priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN or multiple spanning-tree instance. Because a switch stack appears as a single switch to the rest of the network, all switches in the stack use the same bridge ID for a given spanning tree. If the stack's active switch fails, the stack members recalculate their bridge IDs of all running spanning trees based on the new MAC address of the stack's active switch.

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.

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.

Examples

This example shows how to enable the extended-system ID:

```
Device(config)# spanning-tree extend system-id
```

Related Topics

- [show spanning-tree](#), on page 179
- [spanning-tree mst root](#), on page 209
- [spanning-tree vlan](#), on page 223

spanning-tree guard

To enable or disable root-guard mode or loop-guard mode on the VLANs associated with an interface, use the **spanning-tree guard** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
spanning-tree guard {loop | root | none}
no spanning-tree guard
```

Syntax Description

loop Enables the loop-guard mode on the interface.

root Enables root-guard mode on the interface.

none Sets the guard mode to none.

Command Default

Root-guard mode is disabled.

Loop-guard mode is configured according to the **spanning-tree loopguard default** command in global configuration mode.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

You can enable root guard or loop guard when the device is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

You cannot enable both root guard and loop guard at the same time.

Use the **spanning-tree guard loop** command to override the setting of the spanning-tree loop guard default setting.

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 device from becoming the root switch or from 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 are prevented from reaching the forwarding state. The UplinkFast feature is not available when the device is operating in the rapid-PVST+ or MST mode.

Examples

This example shows how to enable root guard on all the VLANs associated with the specified interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# spanning-tree guard root
```

Related Topics

[spanning-tree loopguard default](#), on page 197

spanning-tree link-type

To configure a link type for a port, use the **spanning-tree link-type** command in the interface configuration mode. To return to the default settings, use the **no** form of this command.

```
spanning-tree link-type {point-to-point | shared}
no spanning-tree link-type
```

Syntax Description

point-to-point Specifies that the interface is a point-to-point link.

shared Specifies that the interface is a shared medium.

Command Default

Link type is automatically derived from the duplex setting unless you explicitly configure the link type.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

Rapid Spanning Tree Protocol Plus (RSTP+) fast transition works only on point-to-point links between two bridges.

By default, the device derives the link type of a port from the duplex mode. A full-duplex port is considered as a point-to-point link while a half-duplex configuration is assumed to be on a shared link.

If you designate a port as a shared link, RSTP+ fast transition is forbidden, regardless of the duplex setting.

Examples

This example shows how to configure the port as a shared link:

```
Device(config-if)# spanning-tree link-type shared
```

Related Topics

[show spanning-tree](#), on page 179

spanning-tree loopguard default

To enable loop guard as a default on all ports of a given bridge, use the **spanning-tree loopguard default** command in global configuration mode. To disable loop guard, use the **no** form of this command.

spanning-tree loopguard default
no spanning-tree loopguard default

Syntax Description This command has no arguments or keywords.

Command Default Loop guard is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines Loop guard provides additional security in the bridge network. Loop guard prevents alternate or root ports from becoming the designated port due to a failure that could lead to a unidirectional link.

Loop guard operates only on ports that are considered point-to-point by the spanning tree.

The individual loop-guard port configuration overrides this command.

Examples This example shows how to enable loop guard:

```
Device(config)# spanning-tree loopguard default
```

Related Topics

[spanning-tree guard](#), on page 194

spanning-tree mode

To switch between per-VLAN Spanning Tree+ (PVST+), Rapid-PVST+, and Multiple Spanning Tree (MST) modes, use the **spanning-tree mode** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mode {**pvst** | **mst** | **rapid-pvst**}
no spanning-tree mode

Syntax Description		
	pvst	Enables PVST+ mode.
	mst	Enables MST mode.
	rapid-pvst	Enables Rapid-PVST+ mode.

Command Default The default mode is PVST+.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines Only one mode can be active at a time.
 All stack members run the same spanning-tree mode.



Caution Be careful when using the **spanning-tree mode** command to switch between PVST+, Rapid-PVST+, and MST modes. When you enter the command, all spanning-tree instances are stopped for the previous mode and are restarted in the new mode. Using this command may cause disruption of user traffic.

Examples This example shows how to enable MST mode:

```
Device(config)# spanning-tree mode mst
```

This example shows how to return to the default mode (PVST+):

```
Device(config)# no spanning-tree mode
```

Related Topics

[show spanning-tree](#), on page 179

spanning-tree mst configuration

To enter MST-configuration mode, use the **spanning-tree mst configuration** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst configuration
no spanning-tree mst configuration

Syntax Description

This command has no arguments or keywords.

Command Default

The default value for the Multiple Spanning Tree (MST) configuration is the default value for all its parameters:

- No VLANs are mapped to any MST instance (all VLANs are mapped to the Common and Internal Spanning Tree [CIST] instance).
- The region name is an empty string.
- The revision number is 0.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	This command was introduced.

Usage Guidelines

You can use these commands for MST configuration:

- **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_id*** Maps VLANs to an MST instance. The range for instance IDs is 1 to 4094. The range for VLANs is 1 to 4094. You can specify a single VLAN identified by a 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 is case sensitive and can be up to 32 characters long.
- **no** Negates the instance, name and revision commands or sets them to their defaults.
- **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, a switch stack supports up to 65 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration name, and the same configuration revision number.

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 this command.

Changing an MST-configuration mode parameter can cause connectivity loss. To reduce service disruptions, when you enter MST-configuration mode, make changes to a copy of the current MST configuration. When you have finished editing the configuration, you can apply all the changes at once by using the **exit** keyword, or you can exit the mode without committing any change to the configuration by using the **abort** keyword.

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 and display the pending configuration:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# instance 1 vlan 10-20
Device(config-mst)# name region1
Device(config-mst)# revision 1
Device(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans  Mapped
-----  -----
0         1-9,21-4094
1         10-20
-----
```

This example shows how to reset the MST configuration to the default settings:

```
Device(config)# no spanning-tree mst configuration
```

Related Topics

[show spanning-tree](#), on page 179

spanning-tree mst cost

To set the path cost of the interface for multiple spanning tree (MST) calculations, use the **spanning-tree mst cost** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

```
spanning-tree mst instance-id cost cost
no spanning-tree mst instance-id cost
```

Syntax Description

instance-id Range of spanning-tree instances. The range is 1 to 4094.

cost Path cost. The range is 1 to 200000000.

Command Default

The default path cost is computed from the bandwidth setting of the interface. Default path costs are:

- 1 Gb/s: 20000
- 100 Mb/s: 200000
- 10 Mb/s: 2000000

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

When you specify a value for the cost argument, higher values indicate higher costs.

Examples

This example shows how to set the path cost for an interface associated with MST instances 2 and 4 to 50:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# spanning-tree mst 2,4 cost 250
```

Related Topics

[show spanning-tree](#), on page 179

spanning-tree mst forward-time

To set the forward-delay timer for MST instances, use the **spanning-tree mst forward-time** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

Syntax Description

seconds Number of seconds to set the forward-delay timer for all the MST instances. The range is 4 to 30.

Command Default

The default is 15 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Examples

This example shows how to set the forward-delay timer for all MST instances:

```
Device(config)# spanning-tree mst forward-time 20
```

Related Topics

[spanning-tree mst hello-time](#), on page 203

[spanning-tree mst max-age](#), on page 204

[spanning-tree mst max-hops](#), on page 205

spanning-tree mst hello-time

To set the hello-time delay timer, use the **spanning-tree mst hello-time** command in global configuration mode. To return to the default settings, use the **no** form of this command.

```
spanning-tree mst hello-time seconds
no spanning-tree mst hello-time
```

Syntax Description

seconds Interval, in seconds, between hello BPDUs. The range is 1 to 10.

Command Default

The default is 2.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

If you do not specify the *hello-time* value, the value is calculated from the network diameter.

Exercise care when using this command. For most situations, we recommend that you use the **spanning-tree vlan *vlan-id* root primary** and the **spanning-tree vlan *vlan-id* root secondary** global configuration commands to modify the hello time.

Examples

This example shows how to set the hello-time delay timer to 3 seconds:

```
Device(config)# spanning-tree mst hello-time 3
```

Related Topics

- [spanning-tree mst forward-time](#), on page 202
- [spanning-tree mst max-age](#), on page 204
- [spanning-tree mst max-hops](#), on page 205

spanning-tree mst max-age

To set the interval between messages that the spanning tree receives from the root switch, use the **spanning-tree mst max-age** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-age *seconds*
no spanning-tree mst max-age

Syntax Description	<i>seconds</i> Interval, in seconds, between messages the spanning tree receives from the root switch. The range is 6 to 40.
---------------------------	--

Command Default	The default is 20.
------------------------	--------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.				

Examples

This example shows how to set the max-age timer to 40 seconds:

```
Device(config)# spanning-tree mst max-age 40
```

Related Topics

- [show spanning-tree](#), on page 179
- [spanning-tree mst forward-time](#), on page 202
- [spanning-tree mst hello-time](#), on page 203
- [spanning-tree mst max-hops](#), on page 205

spanning-tree mst max-hops

To specify the number of possible hops in the region before a bridge protocol data unit (BPDU) is discarded, use the **spanning-tree mst max-hops** command in global configuration mode. To return to the default settings, use the **no** form of this command.

```
spanning-tree mst max-hops hop-count
no spanning-tree mst max-hops
```

Syntax Description	<i>hop-count</i> Number of possible hops in the region before a BPDU is discarded. The range is 1 to 255.						
Command Default	The default is 20.						
Command Modes	Global configuration						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E</td> </tr> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E		This command was introduced.
Release	Modification						
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E						
	This command was introduced.						

Examples

This example shows how to set the number of possible hops to 25:

```
Device(config)# spanning-tree mst max-hops 25
```

Related Topics

- [spanning-tree mst forward-time](#), on page 202
- [spanning-tree mst hello-time](#), on page 203
- [spanning-tree mst max-age](#), on page 204

spanning-tree mst port-priority

To set the priority for an interface, use the **spanning-tree mst port-priority** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

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. The range is 1 to 4094.

priority Priority. The range is 0 to 240 in increments of 16.

Command Default

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	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.

If the switch is a member of a switch stack, you must use the **spanning-tree mst** *instance_id* **cost** *cost* command to select an interface to put in the forwarding state.

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:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# spanning-tree mst 20,24 port-priority 0
```

Related Topics

[spanning-tree mst cost](#), on page 201

[spanning-tree mst priority](#), on page 208

spanning-tree mst pre-standard

To configure a port to transmit only prestandard bridge protocol data units (BPDUs), use the **spanning-tree mst pre-standard** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
spanning-tree mst pre-standard
no spanning-tree mst pre-standard
```

Syntax Description

This command has no arguments or keywords.

Command Default

The default is to automatically detect prestandard neighbors.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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 transmit only prestandard BPDUs:

```
Device(config-if)# spanning-tree mst pre-standard
```

Related Topics

[spanning-tree bpdupfilter](#), on page 187

[spanning-tree bpduguard](#), on page 188

[spanning-tree portfast edge \(interface configuration\)](#), on page 218

spanning-tree mst priority

To set the bridge priority for an instance, use the **spanning-tree mst priority** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree mst *instance* **priority** *priority*

no spanning-tree mst priority

Syntax Description	<i>instance</i>	Instance identification number. The range is 0 to 4094.
	priority <i>priority</i>	Specifies the bridge priority. The range is 0 to 61440 in increments of 4096.

Command Default The default is 32768.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines You can set the bridge priority in increments of 4096 only. Valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344 and 61440.

You can enter *instance* as a single instance or a range of instances, for example, 0-3,5,7-9.

Examples

This example shows how to set the spanning tree priority for MST instance 0 to 4096:

```
Device(config)# spanning-tree mst 0 priority 4096
```

Related Topics

[spanning-tree mst configuration](#), on page 199

[spanning-tree mst root](#), on page 209

spanning-tree mst root

To designate the primary and secondary root switch and set the timer value for an instance, use the **spanning-tree mst root** command in global configuration mode. To return to the default settings, use the **no** form of this command.

```
spanning-tree mst instance root {primary | secondary}
no spanning-tree mst instance root
```

Syntax Description	
<i>instance</i>	Instance identification number. The range is 0 to 4094.
primary	Forces this switch to be the root switch.
secondary	Specifies this switch to act as the root switch, if the primary root fail.

Command Default None

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines Use this command only on backbone switches. You can enter *instance-id* as a single instance or a range of instances, for example, 0-3,5,7-9.

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:

```
Device(config)# spanning-tree mst 10 root primary
```

spanning-tree mst simulate pvst (global configuration)

To enable PVST+ simulation globally, use the **spanning-tree mst simulate pvst global** command. This is enabled by default. To disable PVST+ simulation, use the **no** form of this command.

spanning-tree mst simulate pvst global
no spanning-tree mst simulate pvst global

Syntax Description This command has no arguments or keywords.

Command Default PVST+ simulation is enabled by default.

Command Modes Global configuration mode

Command History	Release	Modification
	3.8.0E and 15.2.(4)E	Support for the command was introduced.

Usage Guidelines This feature configures MST switches (in the same region) to seamlessly interact with PVST+ switches. Use the **show spanning-tree summary** command to see if the feature is enabled.

To enable PVST+ simulation on a port, see **spanning-tree mst simulate pvst (interface configuration)**.

Example

The following example shows the spanning tree summary when PVST+ simulation is enabled in the MSTP mode:

```
Device# show spanning-tree summary
Switch is in mst mode (IEEE Standard)
Root bridge for: MST0
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long
PVST Simulation Default is enabled
Name Blocking Listening Learning Forwarding STP Active
-----
MST0 2 0 0 0 2
-----
1 mst 2 0 0 0 2
```

The following example shows the spanning tree summary when the switch is not in MSTP mode, that is, the switch is in PVST or Rapid-PVST mode. The output string displays the current STP mode:

```
Device# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001, VLAN2001-VLAN2002
EtherChannel misconfig guard is enabled
```

```
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is short
PVST Simulation Default is enabled but inactive in rapid-pvst mode
Name Blocking Listening Learning Forwarding STP Active
```

```
-----
VLAN0001 2 0 0 0 2
VLAN2001 2 0 0 0 2
VLAN2002 2 0 0 0 2
-----
```

```
3 vlans 6 0 0 0 6
```

Related Topics

[spanning-tree mst simulate pvst \(interface configuration\)](#) , on page 212

[show spanning-tree](#), on page 179

spanning-tree mst simulate pvst (interface configuration)

To enable PVST+ simulation on a port, use the **spanning-tree mst simulate pvst** command in the interface configuration mode. This is enabled by default. To disable PVST+ simulation, use the **no** form of this command, or enter the **spanning-tree mst simulate pvst disable** command.

spanning-tree mst simulate pvst [disable]

no spanning-tree mst simulate pvst

Syntax Description	disable Disables the PVST+ simulation feature. This prevents a port from automatically interoperating with a connecting device that is running Rapid PVST+.				
Command Default	PVST+ simulation is enabled by default.				
Command Modes	Interface configuration mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>3.8.0E and 15.2.(4)E</td> <td>Support for the command was introduced.</td> </tr> </tbody> </table>	Release	Modification	3.8.0E and 15.2.(4)E	Support for the command was introduced.
Release	Modification				
3.8.0E and 15.2.(4)E	Support for the command was introduced.				
Usage Guidelines	<p>This feature configures MST switches (in the same region) to seamlessly interact with PVST+ switches. Use the show spanning-tree interface <i>interface-id</i> detail command to see if the feature is enabled.</p> <p>To enable PVST+ simulation globally, see spanning-tree mst simulate pvst global.</p>				

Example

The following example shows the interface details when PVST+ simulation is explicitly enabled on the port:

```
Device# show spanning-tree interface gi3/13 detail
Port 269 (GigabitEthernet3/13) of VLAN0002 is forwarding
Port path cost 4, Port priority 128, Port Identifier 128.297.
Designated root has priority 32769, address 0013.5f20.01c0
Designated bridge has priority 32769, address 0013.5f20.01c0
Designated port id is 128.297, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
PVST Simulation is enabled
BPDU: sent 132, received 1
```

The following example shows the interface details when the PVST+ simulation feature is disabled and a PVST Peer inconsistency has been detected on the port:

```
Device# show spanning-tree interface gi3/13 detail
Port 269 (GigabitEthernet3/13) of VLAN0002 is broken (PVST Peer Inconsistent)
Port path cost 4, Port priority 128, Port Identifier 128.297.
Designated root has priority 32769, address 0013.5f20.01c0
Designated bridge has priority 32769, address 0013.5f20.01c0
Designated port id is 128.297, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
```

```
Number of transitions to forwarding state: 1
Link type is point-to-point by default
PVST Simulation is disabled
BPDU: sent 132, received 1
```

Related Topics

[spanning-tree mst simulate pvst \(global configuration\)](#), on page 210

[show spanning-tree](#), on page 179

spanning-tree pathcost method

To set the default path-cost calculation method, use the **spanning-tree pathcost method** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree pathcost method {long | short}

no spanning-tree pathcost method

Syntax Description

long Specifies the 32-bit based values for default port-path costs.

short Specifies the 16-bit based values for default port-path costs.

Command Default

short

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

The **long** path-cost calculation method utilizes all 32 bits for path-cost calculation and yields values in the range of 1 through 200,000,000.

The **short** path-cost calculation method (16 bits) yields values in the range of 1 through 65535.

Examples

This example shows how to set the default path-cost calculation method to long:

```
Device(config)#spanning-tree pathcost method long
```

This example shows how to set the default path-cost calculation method to short:

```
Device(config)#spanning-tree pathcost method short
```


spanning-tree port-priority

To configure an interface priority when two bridges tie for position as the root bridge, use the **spanning-tree port-priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

```
spanning-tree [{vlan vlan-id} port-priority port-priority
no spanning-tree [{vlan vlan-id} port-priority
```

Syntax Description	
vlan <i>vlan-id</i>	(Optional) Specifies the VLAN range associated with the spanning-tree instance. The range is 1 to 4094.
port-priority	The port priority in increments of sixteen. The range is 0 to 240. The default is 128.

Command Default The port priority is 128.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines The priority you set breaks the tie.

Examples The following example shows how to increase the likelihood that a port will be put in the forwarding state if a loop occurs:

```
Device(config)# interface gigabitethernet2/0/2
Device(config-if)# spanning-tree vlan 20 port-priority 0
```

spanning-tree portfast edge (global configuration)

To enable bridge protocol data unit (BPDU) filtering on PortFast edge-enabled interfaces, the BPDU guard feature on PortFast edge-enabled interfaces, or the PortFast edge feature on all nontrunking interfaces, use the **spanning-tree portfast edge** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree portfast edge {**bpdufilter default** | **bpduguard default** | **default**}

no portfast edge {**bpdufilter default** | **bpduguard default** | **default**}

Syntax Description

bpdufilter default	Enables BPDU filtering on PortFast edge-enabled interfaces and prevents the switch interface connect to end stations from sending or receiving BPDUs.
bpduguard default	Enables the BPDU guard feature on PortFast edge-enabled interfaces and places the interfaces that receive BPDUs in an error-disabled state.
default	Enables the PortFast edge feature on all nontrunking interfaces.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.
Cisco IOS XE 3.8.0E and Cisco IOS 15.2.(4)E	Beginning with this release, if you enter the spanning-tree portfast [trunk] command in the global configuration mode, the system automatically saves it as spanning-tree portfast edge [trunk] .

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 edge bpdufilter default** global configuration command to globally enable BPDU filtering on interfaces that are PortFast edge-enabled (the interfaces are in a PortFast edge-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 PortFast edge-enabled interface, the interface loses its PortFast edge-operational status and BPDU filtering is disabled.

You can override the **spanning-tree portfast edge bpdufilter default** command by using the **spanning-tree portfast edge bpdufilter** interface command.



Caution

Be careful when using this command. 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 edge bpduguard default** global configuration command to globally enable BPDU guard on interfaces that are in a PortFast edge-operational state. In a valid configuration, PortFast edge-enabled interfaces do not receive BPDUs. Receiving a BPDU on a PortFast edge-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 edge bpduguard default** command by using the **spanning-tree portfast edge bpduguard** interface command.

Use the **spanning-tree portfast edge default** command to globally enable the PortFast edge feature on all nontrunking interfaces. Configure PortFast edge 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 PortFast edge-enabled interface moves directly to the spanning-tree forwarding state when linkup occurs; it does not wait for the standard forward-delay time.

You can override the **spanning-tree portfast edge default** global configuration command by using the **spanning-tree portfast edge** interface configuration command. You can use the **no spanning-tree portfast edge default** global configuration command to disable PortFast edge on all interfaces unless they are individually configured with the **spanning-tree portfast edge** interface configuration command.

Examples

This example shows how to globally enable BPDU filtering by default:

```
Device(config)# spanning-tree portfast edge bpdupfilter default
```

This example shows how to globally enable the BPDU guard feature by default:

```
Device(config)# spanning-tree portfast edge bpduguard default
```

This example shows how to globally enable the PortFast feature on all nontrunking interfaces:

```
Device(config)# spanning-tree portfast edge default
```

spanning-tree portfast edge (interface configuration)

To enable PortFast edge mode where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire, use the **spanning-tree portfast edge** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
spanning-tree portfast edge [{disable | trunk}]
no spanning-tree portfast edge
```

Syntax Description

disable (Optional) Disables PortFast edge on the interface.

trunk (Optional) Enables PortFast edge mode on the interface.

Command Default

The settings that are configured by the **spanning-tree portfast edge default** command.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.
Cisco IOS XE 3.8.0E and Cisco IOS 15.2.(4)E	Beginning with this release, if you enter the spanning-tree portfast [trunk] command in the global configuration mode, the system automatically saves it as spanning-tree portfast edge [trunk] .

Usage Guidelines

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.

Use this command only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the switch and network operation.

To enable PortFast edge on trunk ports, you must use the **spanning-tree portfast edge trunk** interface configuration command. The **spanning-tree portfast edge** command is not supported on trunk ports.

An interface with the PortFast edge feature enabled is moved directly to the spanning-tree forwarding state without the standard forward-time delay.

You can use the **spanning-tree portfast edge default** global configuration command to globally enable the PortFast edge feature on all nontrunking interfaces. Use the **spanning-tree portfast edge** interface configuration command to override the global setting.

If you configure the **spanning-tree portfast edge default** global configuration command, you can disable PortFast edge on an interface that is not a trunk interface by using the **spanning-tree portfast edge disable** interface configuration command.

Examples

This example shows how to enable the PortFast edge feature on a port:

```
Device(config)# interface gigabitethernet1/0/2  
Device(config-if)#spanning-tree portfast edge
```

Related Topics

- [spanning-tree bpdupfilter](#), on page 187
- [spanning-tree bpduguard](#), on page 188
- [spanning-tree bridge assurance](#), on page 189
- [spanning-tree portfast edge \(global configuration\)](#), on page 216

spanning-tree transmit hold-count

To specify the transmit hold count, use the **spanning-tree transmit hold-count** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree transmit hold-count *value*

no spanning-tree transmit hold-count

Syntax Description

value Number of bridge protocol data units (BPDUs) sent every second. The range is 1 to 20.

Command Default

The default is 6.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

This command is supported on all spanning-tree modes.

The transmit hold count determines the number of BPDUs that can be sent before pausing for 1 second.



Note

Increasing the transmit-hold count value can have a significant impact on CPU utilization, especially in Rapid Per-VLAN Spanning Tree (PVST+) mode. Decreasing this value might result in slow convergence. We recommend that you used the default setting.

Examples

This example shows how to specify the transmit hold count 8:

```
Device(config)# spanning-tree transmit hold-count 8
```

spanning-tree uplinkfast

To enable UplinkFast, use the **spanning-tree uplinkfast** command in global configuration mode. To disable UplinkFast, use the **no** form of this command.

```
spanning-tree uplinkfast [max-update-rate packets-per-second]
no spanning-tree uplinkfast [max-update-rate]
```

Syntax Description	max-update-rate <i>packets-per-second</i>	(Optional) Specifies the rate (number of packets per second) at which update packets are sent. The range is 0 to 320000. The default is 150.
---------------------------	---	---

Command Default UplinkFast is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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; it cannot be enabled for individual VLANs.

When you enable or disable UplinkFast, cross-stack UplinkFast (CSUF) also is automatically enabled or disabled on all nonstack port interfaces. CSUF accelerates the choice of a new root port when a link or switch fails or when spanning tree reconfigures itself.

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 and set the maximum rate to 200 packets per second:

```
Device(config)# spanning-tree uplinkfast max-update-rate 200
```

Related Topics

[show spanning-tree](#), on page 179

[spanning-tree vlan](#), on page 223

spanning-tree vlan

To configure Spanning Tree Protocol (STP) on a per-virtual LAN (VLAN) basis, use the **spanning-tree vlan** command in global configuration mode. To return to the default settings, use the **no** form of this command.

```
spanning-tree vlan vlan-id [{forward-time seconds | hello-time seconds | max-age seconds | priority
priority | [root {primary | secondary} [diameter net-diameter]}]
no spanning-tree vlan vlan-id [{forward-time | hello-time | max-age | priority | root}]
```

Syntax Description	
<i>vlan-id</i>	VLAN range associated with the spanning-tree instance. The range is 1 to 4094.
forward-time <i>seconds</i>	(Optional) Sets the STP forward delay time in second. The range is 4 to 30. The default is 15.
hello-time <i>seconds</i>	(Optional) Specifies the duration, in seconds, between the generation of configuration messages by the root switch. The range is 1 to 10. The default is 2.
max-age <i>seconds</i>	(Optional) Sets the maximum number of seconds the information in a bridge packet data unit (BPDU) is valid. The range is 6 to 40. The default is 20.
priority <i>priority</i>	(Optional) Sets the STP bridge priority. The range is 0 to 61440 in increments of 4096. The default for the primary root switch is 24576. The default for the secondary root switch is 28672.
root primary	(Optional) Forces this switch to be the root switch.
root secondary	(Optional) Specifies this switch to act as the root switch should the primary root fail.
diameter <i>net-diameter</i>	(Optional) Specifies the maximum number of switches between any two points of attachment of end stations. The range is 2 through 7.

Command Default Spanning tree is enabled on all VLANs.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines If the switch does not hear BPDUs within the time specified by the **max-age** *seconds*- value, it recomputes the spanning-tree topology.

Use the **spanning-tree vlan** *vlan-id* **root** only on backbone switches.

The **spanning-tree vlan *vlan-id* root secondary** command alters this switch's priority from 32768 to 28672. If the root switch should fail, this switch becomes the next root switch.

**Caution**

We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

Examples

The following example shows how to enable spanning tree on VLAN 200:

```
Device(config)# spanning-tree vlan 200
```

The following example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Device(config)# spanning-tree vlan 10 root primary diameter 4
```

The following example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Device(config)# spanning-tree vlan 10 root secondary diameter 4
```

Related Topics

[show spanning-tree](#), on page 179

switchport access vlan

To configure a port as a static-access port, use the **switchport access vlan** command in interface configuration mode. To reset the access mode to the default VLAN mode, use the **no** form of this command.

```
switchport access vlan {vlan-id }
no switchport access vlan
```

Syntax Description

vlan-id (Optional) Number of the VLAN on the interface in access mode. Valid values are from 1 to 4094.

Command Default

The default access VLAN and trunk interface native VLAN is a default VLAN corresponding to the platform or interface hardware.

A dynamic-access port is initially a member of no VLAN and receives its assignment based on the packet it receives.

Command Modes

Interface configuration mode

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

The port must be in access mode before the **switchport access vlan** command can take effect.

If the switchport mode is set to **access vlan** *vlan-id*, the port operates as a member of the specified VLAN. If set to **access vlan dynamic**, the port starts discovery of VLAN assignment based on the incoming packets it receives. An access port can be assigned to only one VLAN.

The **no switchport access** command resets the access mode VLAN to the appropriate default VLAN for the device.

Examples

This example show how to first populate the VLAN database by associating a VLAN ID with a VLAN name, and then configure the VLAN (using the name) on an interface, in the access mode: You can also verify your configuration by entering the **show interfaces interface-id switchport** in privileged EXEC command and examining information in the Access Mode VLAN: row.

Part 1 - Making the entry in the VLAN database:

```
Device# configure terminal
Device(config)# vlan 33
Device(config-vlan)# name test
Device(config-vlan)# end
Device#
```

Part 2 - Checking the VLAN database

```
Device # show vlan id 33
VLAN Name      Status   Ports
-----
33    test       active

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
-----
33    enet  100033   1500    -     -     -     -     -         0      0
```

```
Remote SPAN VLAN
-----
Disabled
```

```
Primary Secondary Type          Ports
-----
```

Part 3 - Setting the VLAN on the interface, by using the vlan_name 'test'.

```
Device # configure terminal
Device(config)# interface GigabitEthernet5/1
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan name test
Device(config-if)# end
Device#
```

Part 4 - Verifying running-config

```
Device # show running-config interface GigabitEthernet5/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet5/1
switchport access vlan 33
switchport mode access
Switch#
```

Part 5 - Also can be verified in interface switchport

```
Device # show interface GigabitEthernet5/1 switchport
Name: Gi5/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 33 (test)
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
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#
```

Related Topics

[switchport mode](#), on page 227

switchport mode

To configure the VLAN membership mode of a port, use the **switchport mode** command in interface configuration mode. To reset the mode to the appropriate default for the device, use the **no** form of this command.

```
switchport mode {access | dynamic | {auto | desirable} | trunk}
noswitchport mode {access | dynamic | {auto | desirable} | trunk}
```

Syntax Description		
access	Sets 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	Sets the port 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	Sets the port trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.	
trunk	Sets 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 devices or between a device and a router.	

Command Default The default mode is **dynamic auto**.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	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 problem, 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.

The IEEE 802.1x feature interacts with switchport modes in these ways:

- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.
- If you try to enable IEEE 802.1x on a port set to **dynamic auto** or **dynamic desirable**, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to **dynamic auto** or **dynamic desirable**, the port mode is not changed.
- If you try to enable IEEE 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

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.

Examples

This example shows how to configure a port for access mode:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode access
```

This example shows how set the port to dynamic desirable mode:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode dynamic desirable
```

This example shows how to configure a port for trunk mode:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode trunk
```

Related Topics

[switchport access vlan](#), on page 225

switchport nonegotiate

To specify that Dynamic Trunking Protocol (DTP) negotiation packets are not sent on the Layer 2 interface, use the **switchport nonegotiate** command in interface configuration mode. 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.

Command Default

The default is to use DTP negotiation to learn the trunking status.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	This command was introduced.

Usage Guidelines

The **no 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 problem, turn off DTP by using the **switchport nonegotiate** 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.

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):

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport nonegotiate
```

You can verify your setting by entering the **show interfaces interface-id switchport** privileged EXEC command.

Related Topics

[switchport mode](#), on page 227

udld

To enable aggressive or normal mode in the UniDirectional Link Detection (UDLD) and to set the configurable message timer time, use the **udld** command in global configuration mode. To disable aggressive or normal mode UDLD on all fiber-optic ports, use the **no** form of the command.

```
udld {aggressive | enable | message time message-timer-interval}
no udld {aggressive | enable | message}
```

Syntax Description		
	aggressive	Enables UDLD in aggressive mode on all fiber-optic interfaces.
	enable	Enables UDLD in normal mode on all fiber-optic interfaces.
	message time <i>message-timer-interval</i>	Configures 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. The default is 15 seconds.

Command Default UDLD is disabled on all interfaces.
The message timer is set at 15 seconds.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E
		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 *Catalyst 2960-X Switch Layer 2 Configuration Guide* and *Catalyst 2960-XR Switch Layer 2 Configuration Guide*.

If you change the message time between probe packets, you are making a compromise 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 reenabling UDLD globally.
- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to reenabling 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.

This example shows how to enable UDLD on all fiber-optic interfaces:

```
Device(config)# udld enable
```

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

Related Topics

[show udld](#), on page 183

[udld port](#), on page 232

[udld reset](#), on page 234

udld port

To enable UniDirectional Link Detection (UDLD) on an individual interface or to prevent a fiber-optic interface from being enabled by the **udld** global configuration command, use the **udld port** command in interface configuration mode. To return to the **udld** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port, use the **no** form of this command.

udld port [**aggressive**]
no udld port [**aggressive**]

Syntax Description

aggressive (Optional) Enables UDLD in aggressive mode on the specified interface.

Command Default

On fiber-optic interfaces, UDLD is disabled and 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
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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 device.

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.

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 resets 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 reenables UDLD globally.
- The **no udld port** interface configuration command, followed by the **udld port** or **udld port aggressive** interface configuration command reenables UDLD on the specified interface.

- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands automatically recover from the UDLD error-disabled state.

This example shows how to enable UDLD on an port:

```
Device(config)# interface gigabitethernet6/0/1  
Device(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:

```
Device(config)# interface gigabitethernet6/0/1  
Device(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 Topics

[show udld](#), on page 183

[udld](#), on page 230

[udld reset](#), on page 234

udld reset

To reset all interfaces disabled by 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), use the **udld reset** command in privileged EXEC mode.

udld reset

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		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.

This example shows how to reset all interfaces disabled by UDLD:

```
Device# udld reset
1 ports shutdown by UDLD were reset.
```

Related Topics

[show udld](#), on page 183

[udld](#), on page 230

[udld port](#), on page 232



PART **IV**

NetFlow Lite

- [NetFlow Lite Commands, on page 237](#)



NetFlow Lite Commands

- [cache](#), on page 239
- [clear flow exporter](#), on page 242
- [clear flow monitor](#), on page 243
- [collect counter](#), on page 245
- [collect flow sampler](#), on page 246
- [collect interface](#), on page 247
- [collect timestamp sys-uptime](#), on page 248
- [collect transport tcp flags](#), on page 249
- [datalink flow monitor](#), on page 251
- [debug flow exporter](#), on page 252
- [debug flow monitor](#), on page 253
- [debug sampler](#), on page 254
- [description](#), on page 255
- [destination](#), on page 256
- [dscp](#), on page 257
- [export-protocol netflow-v9](#), on page 258
- [exporter](#), on page 259
- [flow exporter](#), on page 260
- [flow monitor](#), on page 261
- [flow record](#), on page 262
- [ip flow monitor](#), on page 263
- [ipv6 flow monitor](#), on page 264
- [match datalink ethertype](#), on page 265
- [match datalink mac](#), on page 266
- [match ipv4](#), on page 267
- [match ipv4 destination address](#), on page 268
- [match ipv4 source address](#), on page 269
- [match ipv6](#), on page 270
- [match ipv6 destination address](#), on page 271
- [match ipv6 source address](#), on page 272
- [match transport](#), on page 273
- [mode](#), on page 274
- [option](#), on page 276

- [record](#), on page 278
- [sampler](#), on page 279
- [show flow exporter](#), on page 280
- [show flow interface](#), on page 282
- [show flow monitor](#), on page 284
- [show flow record](#), on page 290
- [show sampler](#), on page 291
- [source](#), on page 293
- [statistics packet protocol](#), on page 295
- [template data timeout](#), on page 296
- [transport](#), on page 297
- [ttl](#), on page 298

cache

To configure a flow cache parameter for a flow monitor, use the **cache** command in flow monitor configuration mode. To remove a flow cache parameter for a flow monitor, use the **no** form of this command.

```
cache {entries number | timeout {active | inactive | update} seconds | type {normal | permanent}}
no cache {entries | timeout {active | inactive | update} | type}
```

Syntax Description		
entries <i>number</i>		Specifies the maximum number of entries in the flow monitor cache. The range is 16 to 1048576. The default is 16640 for each switch in the stack.
timeout		Specifies the flow timeout.
active		Specifies the active flow timeout.
inactive		Specifies the inactive flow timeout.
update		Specifies the update timeout for a permanent flow cache.
<i>seconds</i>		The timeout value in seconds. The range is 30 to 604800 (7 days) for a normal flow cache. For a permanent flow cache the range is 1 to 604800 (7 days).
type		Specifies the type of the flow cache.
normal		Configures a normal cache type. The entries in the flow cache will be aged out according to the timeout active <i>seconds</i> and timeout inactive <i>seconds</i> settings. This is the default cache type.
permanent		Configures a permanent cache type. This cache type disables flow removal from the flow cache.

Command Default The default flow monitor flow cache parameters are used.

The following flow cache parameters for a flow monitor are enabled:

- Cache type: normal
- Maximum number of entries in the flow monitor cache: 16640
- Active flow timeout: 1800 seconds
- Inactive flow timeout: 30 seconds
- Update timeout for a permanent flow cache: 1800 seconds

Command Modes Flow monitor configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Each flow monitor has a cache that it uses to store all the flows it monitors. Each cache has various configurable elements, such as the time that a flow is allowed to remain in it. When a flow times out, it is removed from the cache and sent to any exporters that are configured for the corresponding flow monitor.

If a cache is already active (that is, you have applied the flow monitor to at least one interface in the device), your changes to the parameters will not take effect until you either reboot the device or remove the flow monitor from every interface and then reapply it. Therefore, whenever possible you should customize the parameters for the cache before you apply the flow monitor to an interface. You can modify the timers, flow exporters, and statistics parameters for a cache while the cache is active.

The **cache timeout active** command controls the aging behavior of the normal type of cache. If a flow has been active for a long time, it is usually desirable to age it out (starting a new flow for any subsequent packets in the flow). This age out process allows the monitoring application that is receiving the exports to remain up to date. By default, this timeout is 1800 seconds (30 minutes), but it can be adjusted according to system requirements. A larger value ensures that long-lived flows are accounted for in a single flow record; a smaller value results in a shorter delay between starting a new long-lived flow and exporting some data for it. When you change the active flow timeout, the new timeout value takes effect immediately.

The **cache timeout inactive** command also controls the aging behavior of the normal type of cache. If a flow has not seen any activity for a specified amount of time, that flow will be aged out. By default, this timeout is 30 seconds, but this value can be adjusted depending on the type of traffic expected. If a large number of short-lived flows is consuming many cache entries, reducing the inactive timeout can reduce this overhead. If a large number of flows frequently get aged out before they have finished collecting their data, increasing this timeout can result in better flow correlation. When you change the inactive flow timeout, the new timeout value takes effect immediately.

The **cache timeout update** command controls the periodic updates sent by the permanent type of cache. This behavior is similar to the active timeout, except that it does not result in the removal of the cache entry from the cache. By default, this timer value is 1800 seconds (30 minutes).

The **cache type normal** command specifies the normal cache type. This is the default cache type. The entries in the cache will be aged out according to the **timeout active seconds** and **timeout inactive seconds** settings. When a cache entry is aged out, it is removed from the cache and exported via any exporters configured for the monitor associated with the cache.

To return a cache to its default settings, use the **default cache** flow monitor configuration command.



Note When a cache becomes full, new flows will not be monitored. If this occurs, a Flows not added statistic will appear in the cache statistics.



Note A permanent cache uses update counters rather than delta counters. When a flow is exported, the counters represent the totals seen for the full lifetime of the flow and not the additional packets and bytes seen since the last export was sent.

The following example shows how to configure the active timeout for the flow monitor cache:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout active 4800
```

The following example shows how to configure the inactive timer for the flow monitor cache:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout inactive 30
```

The following example shows how to configure the permanent cache update timeout:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout update 5000
```

The following example shows how to configure a normal cache:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache type normal
```

Related Topics

[flow monitor](#), on page 261

clear flow exporter

To clear the statistics for a Flexible Netflow flow exporter, use the **clear flow exporter** command in privileged EXEC mode.

clear flow exporter *[[name] exporter-name] statistics*

Syntax Description

name	(Optional) Specifies the name of a flow exporter.
<i>exporter-name</i>	(Optional) Name of a flow exporter that was previously configured.
statistics	Clears the flow exporter statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

The **clear flow exporter** command removes all statistics from the flow exporter. These statistics will not be exported and the data gathered in the cache will be lost.

You can view the flow exporter statistics by using the **show flow exporter statistics** privileged EXEC command.

Examples

The following example clears the statistics for all of the flow exporters configured on the device:

```
Device# clear flow exporter statistics
```

The following example clears the statistics for the flow exporter named FLOW-EXPORTER-1:

```
Device# clear flow exporter FLOW-EXPORTER-1 statistics
```

Related Topics

[debug flow exporter](#), on page 252

clear flow monitor

To clear a flow monitor cache or flow monitor statistics and to force the export of the data in the flow monitor cache, use the **clear flow monitor** command in privileged EXEC mode.

```
clear flow monitor [name] monitor-name [{cache] force-export | statistics}]
```

Syntax Description	name	Specifies the name of a flow monitor.
	<i>monitor-name</i>	Name of a flow monitor that was previously configured.
	cache	(Optional) Clears the flow monitor cache information.
	force-export	(Optional) Forces the export of the flow monitor cache statistics.
	statistics	(Optional) Clears the flow monitor statistics.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines The **clear flow monitor cache** command removes all entries from the flow monitor cache. These entries will not be exported and the data gathered in the cache will be lost.



Note The statistics for the cleared cache entries are maintained.

The **clear flow monitor force-export** command removes all entries from the flow monitor cache and exports them using all flow exporters assigned to the flow monitor. This action can result in a short-term increase in CPU usage. Use this command with caution.

The **clear flow monitor statistics** command clears the statistics for this flow monitor.



Note The current entries statistic will not be cleared by the **clear flow monitor statistics** command because this is an indicator of how many entries are in the cache and the cache is not cleared with this command.

You can view the flow monitor statistics by using the **show flow monitor statistics** privileged EXEC command.

Examples

The following example clears the statistics and cache entries for the flow monitor named FLOW-MONITOR-1:

```
Device# clear flow monitor name FLOW-MONITOR-1
```

The following example clears the statistics and cache entries for the flow monitor named FLOW-MONITOR-1 and forces an export:

```
Device# clear flow monitor name FLOW-MONITOR-1 force-export
```

The following example clears the cache for the flow monitor named FLOW-MONITOR-1 and forces an export:

```
Device# clear flow monitor name FLOW-MONITOR-1 cache force-export
```

The following example clears the statistics for the flow monitor named FLOW-MONITOR-1:

```
Device# clear flow monitor name FLOW-MONITOR-1 statistics
```

Related Topics

[debug flow monitor](#), on page 253

collect counter

To configure the number of bytes or packets in a flow as a non-key field for a flow record, use the **collect counter** command in flow record configuration mode. To disable the use of the number of bytes or packets in a flow (counters) as a non-key field for a flow record, use the **no** form of this command.

```
collect counter {bytes | packets} {long | permanent}
no collect counter {bytes | packets} {long | permanent}
```

Syntax Description		
bytes	Configures the number of bytes seen in a flow as a non-key field and enables collecting the total number of bytes from the flow.	
packets	Configures the number of packets seen in a flow as a non-key field and enables collecting the total number of packets from the flow.	
long	Enables collecting the total number of bytes or packets from the flow using a 64-bit counter. After collection the counter resets to 0.	
permanent	Enables collecting the total number of bytes or packets from the flow using a 64-bit counter. After collection the counter does not reset.	

Command Default The number of bytes or packets in a flow is not configured as a non-key field.

Command Modes Flow record configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines Flow packets are exported after cache timeout interval. After they are exported, the count restarts from 0 if the **long** keyword is specified. If the **permanent** keyword is specified, the counter increments for each byte or packet seen in the flow.

To return this command to its default settings, use the **no collect counter** or **default collect counter** flow record configuration command.

The following example configures the total number of bytes in the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#collect counter bytes long
```

The following example configures the total number of packets from the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter packets long
```

Related Topics

[flow record](#), on page 262

collect flow sampler

To configure the flow sampler ID as a non-key field and enable the collection of the ID of the sampler that is assigned to the flow monitor, use the **collect flow sampler** command in flow record configuration mode. To disable the use of the flow sampler ID as a non-key field for a flow record, use the **no** form of this command.

collect flow sampler

no collect flow sampler

Syntax Description

This command has no arguments or keywords.

Command Default

The flow sampler ID is not configured as a non-key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

The NetFlow Lite **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

The **collect flow sampler** command is useful when more than one flow sampler is being used with different sampling rates. The **option sampler-table** flow exporter command exports options records with mappings of the flow sampler ID to sampling rate so the collector can calculate the scaled counters for each flow.

To return this command to its default settings, use the **no collect flow sampler** or **default collect flow sampler** flow record configuration command.

The following example configures the ID of the flow sampler that is assigned to the flow as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect flow sampler
```

Related Topics

[flow exporter](#), on page 260

[flow record](#), on page 262

collect interface

To configure the input interface name as a non-key field for a flow record, use the **collect interface** command in flow record configuration mode. To disable the use of the input interface as a non-key field for a flow record, use the **no** form of this command.

collect interface input
no collect interface input

Syntax Description	input Configures the input interface name as a non-key field and enables collecting the input interface from the flows.				
Command Default	The input interface name is not configured as a non-key field.				
Command Modes	Flow record configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)E</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.				
Usage Guidelines	<p>The NetFlow Lite collect commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.</p> <p>To return this command to its default settings, use the no collect interface or default collect interface flow record configuration command.</p> <p>The following example configures the input interface as a non-key field:</p> <pre>Device(config)# flow record FLOW-RECORD-1 Device(config-flow-record)# collect interface input</pre>				

Related Topics

[flow record](#), on page 262

collect timestamp sys-uptime

To configure the system uptime of the first seen or last seen packet in a flow as a nonkey field for a flow record, use the **collect timestamp sys-uptime** command in flow record configuration mode. To disable the use of the first seen or last seen packet in a flow as a nonkey field for a flow record, use the **no** form of this command.

```
collect timestamp sys-uptime {first | last}
no collect timestamp sys-uptime {first | last}
```

Syntax Description

first	Configures the system uptime for the time the first packet was seen from the flows as a nonkey field and enables collecting time stamps based on the system uptime for the time the first packet was seen from the flows.
last	Configures the system uptime for the time the last packet was seen from the flows as a nonkey field and enables collecting time stamps based on the system uptime for the time the most recent packet was seen from the flows.

Command Default

The system uptime field is not configured as a nonkey field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

The NetFlow Lite **collect** commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases, the values for nonkey fields are taken from only the first packet in the flow.

To return this command to its default settings, use the **no collect timestamp sys-uptime** or **default collect timestamp sys-uptime** flow record configuration command.

Examples

The following example configures time stamps based on the system uptime for the time the first packet was seen from the flows as a nonkey field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp sys-uptime first
```

The following example configures the time stamps based on the system uptime for the time the most recent packet was seen from the flows as a nonkey field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp sys-uptime last
```

Related Topics

[flow record](#), on page 262

collect transport tcp flags

To configure one or more TCP flags as a non-key field for a flow record and enable the collecting of values from the flow, use the **collect transport tcp flags** command in flow record configuration mode. To disable the use of one or more of the TCP fields as a non-key field for a flow record and disable collecting the values from the flow, use the **no** form of this command.

```
collect transport tcp flags [{ack | cwr | ece | fin | psh | rst | syn | urg}]
no collect transport tcp flags [{ack | cwr | ece | fin | psh | rst | syn | urg}]
```

Syntax Description

ack	(Optional) Configures the TCP acknowledgment flag as a non-key field.
cwr	(Optional) Configures the TCP congestion window reduced flag as a non-key field.
ece	(Optional) Configures the TCP Explicit Congestion Notification echo (ECE) flag as a non-key field.
fin	(Optional) Configures the TCP finish flag as a non-key field.
psh	(Optional) Configures the TCP push flag as a non-key field.
rst	(Optional) Configures the TCP reset flag as a non-key field.
syn	(Optional) Configures the TCP synchronize flag as a non-key field.
urg	(Optional) Configures the TCP urgent flag as a non-key field.

Command Default

The transport layer fields are not configured as a non-key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

The values of the transport layer fields are taken from all packets in the flow. You cannot specify which TCP flag to collect. You can only specify to collect transport TCP flags. All TCP flags will be collected with this command. The following transport TCP flags are collected:

- **ack**—TCP acknowledgement flag
- **cwr**—TCP congestion window reduced flag
- **ece**—TCP ECN echo flag
- **fin**—TCP finish flag
- **psh**—TCP push flag
- **rst**—TCP reset flag
- **syn**—TCP synchronize flag
- **urg**—TCP urgent flag

To return this command to its default settings, use the **no collect collect transport tcp flags** or **default collect collect transport tcp flags** flow record configuration command.

The following example configures the TCP acknowledgment flag as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect transport tcp flags ack
```

The following example configures the TCP finish flag as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect transport tcp flags fin
```

The following example configures the TCP reset flag as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect transport tcp flags rst
```

Related Topics

[flow record](#), on page 262

datalink flow monitor

To apply a NetFlow Lite flow monitor to an interface, use the **datalink flow monitor** command in interface configuration mode. To disable a NetFlow Lite flow monitor, use the **no** form of this command.

datalink flow monitor *monitor-name* **sampler** *sampler-name* **input**
no datalink flow monitor *monitor-name* **sampler** *sampler-name* **input**

Syntax Description

<i>monitor-name</i>	Name of the flow monitor to apply to the interface.
sampler <i>sampler-name</i>	Enables the specified flow sampler for the flow monitor.
input	Monitors traffic that the switch receives on the interface.

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Before you apply a flow monitor to an interface with the **datalink flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command and the flow sampler using the **sampler** global configuration command.

To enable a flow sampler for the flow monitor, you must have already created the sampler.



Note

The **datalink flow monitor** command only monitors non-IPv4 and non-IPv6 traffic. To monitor IPv4 traffic, use the **ip flow monitor** command. To monitor IPv6 traffic, use the **ipv6 flow monitor** command.

This example shows how to enable NetFlow Lite datalink monitoring on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# datalink flow monitor FLOW-MONITOR-1 sampler FLOW-SAMPLER-1 input
```

Related Topics

[flow monitor](#), on page 261

debug flow exporter

To enable debugging output for Flexible Netflow flow exporters, use the **debug flow exporter** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug flow exporter [[name] exporter-name] [{error | event | packets number}]
no debug flow exporter [[name] exporter-name] [{error | event | packets number}]
```

Syntax Description

name	(Optional) Specifies the name of a flow exporter.
<i>exporter-name</i>	(Optional) The name of a flow exporter that was previously configured.
error	(Optional) Enables debugging for flow exporter errors.
event	(Optional) Enables debugging for flow exporter events.
packets	(Optional) Enables packet-level debugging for flow exporters.
<i>number</i>	(Optional) The number of packets to debug for packet-level debugging of flow exporters. The range is 1 to 65535.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Examples

The following example indicates that a flow exporter packet has been queued for process send:

```
Device# debug flow exporter
May 21 21:29:12.603: FLOW EXP: Packet queued for process send
```

Related Topics

[clear flow exporter](#), on page 242

debug flow monitor

To enable debugging output for Flexible NetFlow flow monitors, use the **debug flow monitor** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug flow monitor [{error | [name] monitor-name [{cache [error] | error | packets packets}]}]
no debug flow monitor [{error | [name] monitor-name [{cache [error] | error | packets packets}]}]
```

Syntax Description	
error	(Optional) Enables debugging for flow monitor errors for all flow monitors or for the specified flow monitor.
name	(Optional) Specifies the name of a flow monitor.
<i>monitor-name</i>	(Optional) Name of a flow monitor that was previously configured.
cache	(Optional) Enables debugging for the flow monitor cache.
cache error	(Optional) Enables debugging for flow monitor cache errors.
packets	(Optional) Enables packet-level debugging for flow monitors.
<i>packets</i>	(Optional) Number of packets to debug for packet-level debugging of flow monitors. The range is 1 to 65535.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Examples

The following example shows that the cache for FLOW-MONITOR-1 was deleted:

```
Device# debug flow monitor FLOW-MONITOR-1 cache
May 21 21:53:02.839: FLOW MON: 'FLOW-MONITOR-1' deleted cache
```

Related Topics

[clear flow monitor](#), on page 243

debug sampler

To enable debugging output for Flexible NetFlow samplers, use the **debug sampler** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug sampler [{detailed | error | [name] sampler-name [{detailed | error | sampling samples}]}]
no debug sampler [{detailed | error | [name] sampler-name [{detailed | error | sampling}]}]
```

Syntax Description

detailed	(Optional) Enables detailed debugging for sampler elements.
error	(Optional) Enables debugging for sampler errors.
name	(Optional) Specifies the name of a sampler.
<i>sampler-name</i>	(Optional) Name of a sampler that was previously configured.
sampling <i>samples</i>	(Optional) Enables debugging for sampling and specifies the number of samples to debug.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Examples

The following sample output shows that the debug process has obtained the ID for the sampler named SAMPLER-1:

```
Device# debug sampler detailed
*May 28 04:14:30.883: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et1/0,0)
get ID succeeded:1
*May 28 04:14:30.971: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et0/0,I)
get ID succeeded:1
```


description

To configure a description for a flow monitor, flow exporter, or flow record, use the **description** command in the appropriate configuration mode. To remove a description, use the **no** form of this command.

description *description*
no description *description*

Syntax Description

description Text string that describes the flow monitor, flow exporter, or flow record.

Command Default

The default description for a flow sampler, flow monitor, flow exporter, or flow record is "User defined."

Command Modes

The following command modes are supported:

Flow exporter configuration

Flow monitor configuration

Flow record configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

To return this command to its default setting, use the **no description** or **default description** command in the appropriate configuration mode.

The following example configures a description for a flow monitor:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# description Monitors traffic to 172.16.0.1 255.255.0.0
```

Related Topics

- [flow exporter](#), on page 260
- [flow monitor](#), on page 261
- [flow record](#), on page 262

destination

To configure an export destination for a flow exporter, use the **destination** command in flow exporter configuration mode. To remove an export destination for a flow exporter, use the **no** form of this command.

destination {*hostnameip-address*}

no destination {*hostnameip-address*}

Syntax Description

hostname Hostname of the device to which you want to send the NetFlow information.

ip-address IPv4 address of the workstation to which you want to send the NetFlow information.

Command Default

An export destination is not configured.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Each flow exporter can have only one destination address or hostname.

When you configure a hostname instead of the IP address for the device, the hostname is resolved immediately and the IPv4 address is stored in the running configuration. If the hostname-to-IP-address mapping that was used for the original Domain Name System (DNS) name resolution changes dynamically on the DNS server, the device does not detect this, and the exported data continues to be sent to the original IP address, resulting in a loss of data.

To return this command to its default setting, use the **no destination** or **default destination** command in flow exporter configuration mode.

The following example shows how to configure the networking device to export the NetFlow Lite cache entry to a destination system:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# destination 10.0.0.4
```

Related Topics

[flow exporter](#), on page 260

dscp

To configure a differentiated services code point (DSCP) value for flow exporter datagrams, use the **dscp** command in flow exporter configuration mode. To remove a DSCP value for flow exporter datagrams, use the **no** form of this command.

```
dscp dscp
no dscp dscp
```

Syntax Description	<i>dscp</i> DSCP to be used in the DSCP field in exported datagrams. The range is 0 to 63. The default is 0.
---------------------------	--

Command Default	The differentiated services code point (DSCP) value is 0.
------------------------	---

Command Modes	Flow exporter configuration
----------------------	-----------------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines	To return this command to its default setting, use the no dscp or default dscp flow exporter configuration command.
-------------------------	---

The following example sets 22 as the value of the DSCP field in exported datagrams:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# dscp 22
```

Related Topics

[flow exporter](#), on page 260

export-protocol netflow-v9

To configure NetFlow Version 9 export as the export protocol for a NetFlow Lite exporter, use the **export-protocol netflow-v9** command in flow exporter configuration mode.

export-protocol netflow-v9

Syntax Description This command has no arguments or keywords.

Command Default NetFlow Version 9 is enabled.

Command Modes Flow exporter configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines The device does not support NetFlow v5 export format, only NetFlow v9 export format is supported.

The following example configures NetFlow Version 9 export as the export protocol for a NetFlow exporter:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# export-protocol netflow-v9
```

Related Topics

[flow exporter](#), on page 260

exporter

To add a flow exporter for a flow monitor, use the **exporter** command in the appropriate configuration mode. To remove a flow exporter for a flow monitor, use the **no** form of this command.

exporter *exporter-name*
no exporter *exporter-name*

Syntax Description

exporter-name Name of a flow exporter that was previously configured.

Command Default

An exporter is not configured.

Command Modes

Flow monitor configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

You must have already created a flow exporter by using the **flow exporter** command before you can apply the flow exporter to a flow monitor with the **exporter** command.

To return this command to its default settings, use the **no exporter** or **default exporter** flow monitor configuration command.

Examples

The following example configures an exporter for a flow monitor:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# exporter EXPORTER-1
```

Related Topics

[flow exporter](#), on page 260

[flow monitor](#), on page 261

flow exporter

To create a NetFlow Lite flow exporter, or to modify an existing NetFlow Lite flow exporter, and enter NetFlow Lite flow exporter configuration mode, use the **flow exporter** command in global configuration mode. To remove a NetFlow Lite flow exporter, use the **no** form of this command.

```
flow exporter exporter-name
no flow exporter exporter-name
```

Syntax Description	<i>exporter-name</i> Name of the flow exporter that is being created or modified.
---------------------------	---

Command Default	NetFlow Lite flow exporters are not present in the configuration.
------------------------	---

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines	Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.
-------------------------	---

Examples	The following example creates a flow exporter named FLOW-EXPORTER-1 and enters NetFlow Lite flow exporter configuration mode:
-----------------	---

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)#
```

Related Topics

- [clear flow exporter](#), on page 242
- [debug flow exporter](#), on page 252
- [show flow exporter](#), on page 280

flow monitor

To create a flow monitor, or to modify an existing flow monitor, and enter flow monitor configuration mode, use the **flow monitor** command in global configuration mode. To remove a flow monitor, use the **no** form of this command.

flow monitor *monitor-name*
no flow monitor *monitor-name*

Syntax Description

monitor-name Name of the flow monitor that is being created or modified.

Command Default

NetFlow Lite flow monitors are not present in the configuration.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Flow monitors are the NetFlow Lite component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a flow record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the flow monitor's record and stored in the flow monitor cache.

Examples

The following example creates a flow monitor named FLOW-MONITOR-1 and enters flow monitor configuration mode:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)#
```

Related Topics

- [clear flow monitor](#), on page 243
- [debug flow monitor](#), on page 253
- [show flow monitor](#), on page 284

flow record

To create a NetFlow Lite flow record, or to modify an existing NetFlow Lite flow record, and enter NetFlow Lite flow record configuration mode, use the **flow record** command in global configuration mode. To remove a NetFlow Lite record, use the **no** form of this command.

flow record *record-name*
no flow record *record-name*

Syntax Description

record-name Name of the flow record that is being created or modified.

Command Default

A NetFlow Lite flow record is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

A flow record defines the keys that NetFlow Lite uses to identify packets in the flow, as well as other fields of interest that NetFlow Lite gathers for the flow. You can define a flow record with any combination of keys and fields of interest. The `flow record` supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 64-bit packet or byte counters.

Examples

The following example creates a flow record named FLOW-RECORD-1, and enters NetFlow Lite flow record configuration mode:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#
```

Related Topics

[show flow record](#), on page 290

ip flow monitor

To enable a NetFlow Lite flow monitor for IPv4 traffic that the device is receiving, use the **ip flow monitor** command in interface configuration mode. To disable a flow monitor, use the **no** form of this command.

ip flow monitor *monitor-name* **sampler** *sampler-name* **input**
no ip flow monitor *monitor-name* **sampler** *sampler-name* **input**

Syntax Description

<i>monitor-name</i>	Name of the flow monitor to apply to the interface.
sampler <i>sampler-name</i>	Enables the specified flow sampler for the flow monitor.
input	Monitors IPv4 traffic that the device receives on the interface.

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Before you can apply a flow monitor to an interface with the **ip flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command.

When you add a sampler to a flow monitor, only packets that are selected by the named sampler will be entered into the cache to form flows. Each use of a sampler causes separate statistics to be stored for that usage.



Note

The statistics for each flow must be scaled to give the expected true usage. For example, with a 1 in 100 sampler it is expected that the packet and byte counters will have to be multiplied by 100.

The following example enables a flow monitor for monitoring input traffic, with a sampler to limit the input packets that are sampled:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

Related Topics

[flow monitor](#), on page 261

[sampler](#), on page 279

ipv6 flow monitor

To enable a flow monitor for IPv6 traffic that the device is receiving, use the **ipv6 flow monitor** command in interface configuration mode. To disable a flow monitor, use the **no** form of this command.

```
ipv6 flow monitor monitor-name sampler sampler-name input
no ipv6 flow monitor monitor-name sampler sampler-name input
```

Syntax Description

<i>monitor-name</i>	Name of the flow monitor to apply to the interface.
sampler <i>sampler-name</i>	Enables the specified flow sampler for the flow monitor.
input	Monitors IPv6 traffic that the device receives on the interface.

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Before you can apply a flow monitor to the interface with the **ipv6 flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command.

When you add a sampler to a flow monitor, only packets that are selected by the named sampler will be entered into the cache to form flows. Each use of a sampler causes separate statistics to be stored for that usage.

You cannot add a sampler to a flow monitor after the flow monitor has been enabled on the interface. You must first remove the flow monitor from the interface and then enable the same flow monitor with a sampler.



Note

The statistics for each flow must be scaled to give the expected true usage. For example, with a 1 in 100 sampler it is expected that the packet and byte counters will have to be multiplied by 100.

The following example enables a flow monitor for monitoring input traffic, with a sampler to limit the input packets that are sampled:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

Related Topics

[flow monitor](#), on page 261

[sampler](#), on page 279

match datalink ethertype

To configure the EtherType of the packet as a key field for a flow record, use the **match datalink ethertype** command in flow record configuration mode. To disable the EtherType of the packet as a key field for a flow record, use the **no** form of this command.

match datalink ethertype
no match datalink ethertype

Syntax Description	This command has no arguments or keywords.				
Command Default	The EtherType of the packet is not configured as a key field.				
Command Modes	Flow record configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)E</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.				

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

When you configure the EtherType of the packet as a key field for a flow record using the **match datalink ethertype** command, the traffic flow that is created is based on the type of flow monitor that is assigned to the interface:

- When a datalink flow monitor is assigned to an interface using the **datalink flow monitor** interface configuration command, it creates unique flows for different Layer 2 protocols.
- When an IP flow monitor is assigned to an interface using the **ip flow monitor** interface configuration command, it creates unique flows for different IPv4 protocols.
- When an IPv6 flow monitor is assigned to an interface using the **ipv6 flow monitor** interface configuration command, it creates unique flows for different IPv6 protocols.

To return this command to its default settings, use the **no match datalink ethertype** or **default match datalink ethertype** flow record configuration command.

The following example configures the EtherType of the packet as a key field for a NetFlow Lite flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink ethertype
```

Related Topics

[flow record](#), on page 262

match datalink mac

To configure the use of MAC addresses as a key field for a flow record, use the **match datalink mac** command in flow record configuration mode. To disable the use of MAC addresses as a key field for a flow record, use the **no** form of this command.

```
match datalink mac {destination address input | source address input}
no match datalink mac {destination address input | source address input}
```

Syntax Description	destination address	Configures the use of the destination MAC address as a key field.
	input	Specifies the MAC address of input packets.
	source address	Configures the use of the source MAC address as a key field.
Command Default	MAC addresses are not configured as a key field.	
Command Modes	Flow record configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The **input** keyword is used to specify the observation point that is used by the **match datalink mac** command to create flows based on the unique MAC addresses in the network traffic.



Note When a datalink flow monitor is assigned to an interface or VLAN record, it creates flows only for non-IPv6 or non-IPv4 traffic.

To return this command to its default settings, use the **no match datalink mac** or **default match datalink mac** flow record configuration command.

The following example configures the use of the destination MAC address of packets that are received by the device as a key field for a flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink mac destination address input
```

Related Topics

[flow record](#), on page 262

match ipv4

To configure one or more of the IPv4 fields as a key field for a flow record, use the **match ipv4** command in flow record configuration mode. To disable the use of one or more of the IPv4 fields as a key field for a flow record, use the **no** form of this command.

```
match ipv4 {destination address | protocol | source address | tos | version}
no match ipv4 {destination address | protocol | source address | tos | version}
```

Syntax Description	Field	Description
	destination address	Configures the IPv4 destination address as a key field. For more information see match ipv4 destination address, on page 268 .
	protocol	Configures the IPv4 protocol as a key field.
	source address	Configures the IPv4 destination address as a key field. For more information see match ipv4 source address, on page 269 .
	tos	Configures the IPv4 ToS as a key field.
	version	Configures the IP version from IPv4 header as a key field.

Command Default The use of one or more of the IPv4 fields as a key field for a user-defined flow record is not enabled.

Command Modes Flow record configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the IPv4 protocol as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 protocol
```

Related Topics

[flow record](#), on page 262

match ipv4 destination address

To configure the IPv4 destination address as a key field for a flow record, use the **match ipv4 destination address** command in flow record configuration mode. To disable the IPv4 destination address as a key field for a flow record, use the **no** form of this command.

match ipv4 destination address
no match ipv4 destination address

Syntax Description

This command has no arguments or keywords.

Command Default

The IPv4 destination address is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv4 destination address** or **default match ipv4 destination address** flow record configuration command.

The following example configures the IPv4 destination address as a key field for a flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 destination address
```

Related Topics

[flow record](#), on page 262

match ipv4 source address

To configure the IPv4 source address as a key field for a flow record, use the **match ipv4 source address** command in flow record configuration mode. To disable the use of the IPv4 source address as a key field for a flow record, use the **no** form of this command.

match ipv4 source address
no match ipv4 source address

Syntax Description This command has no arguments or keywords.

Command Default The IPv4 source address is not configured as a key field.

Command Modes Flow record configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv4 source address** or **default match ipv4 source address** flow record configuration command.

The following example configures the IPv4 source address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 source address
```

Related Topics

[flow record](#), on page 262

match ipv6

To configure one or more of the IPv6 fields as a key field for a flow record, use the **match ipv6** command in flow record configuration mode. To disable the use of one or more of the IPv6 fields as a key field for a flow record, use the **no** form of this command.

```
match ipv6 {destination address | flow-label | protocol | source address}
no match ipv6 {destination address | flow-label | protocol | source address}
```

Syntax Description		
destination address		Configures the IPv4 destination address as a key field. For more information see match ipv6 destination address, on page 271 .
flow-label		Configures the IPv6 flow-label as a key field.
protocol		Configures the IPv6 protocol as a key field.
source address		Configures the IPv4 destination address as a key field. For more information see match ipv6 source address, on page 272 .

Command Default The IPv6 fields are not configured as a key field.

Command Modes Flow record configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the IPv6 protocol field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 protocol
```

Related Topics

[flow record](#), on page 262

match ipv6 destination address

To configure the IPv6 destination address as a key field for a flow record, use the **match ipv6 destination address** command in flow record configuration mode. To disable the IPv6 destination address as a key field for a flow record, use the **no** form of this command.

```
match ipv6 destination address
no match ipv6 destination address
```

Syntax Description This command has no arguments or keywords.

Command Default The IPv6 destination address is not configured as a key field.

Command Modes Flow record configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv6 destination address** or **default match ipv6 destination address** flow record configuration command.

The following example configures the IPv6 destination address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 destination address
```

Related Topics

[flow record](#), on page 262

match ipv6 source address

To configure the IPv6 source address as a key field for a flow record, use the **match ipv6 source address** command in flow record configuration mode. To disable the use of the IPv6 source address as a key field for a flow record, use the **no** form of this command.

match ipv6 source address
no match ipv6 source address

Syntax Description This command has no arguments or keywords.

Command Default The IPv6 source address is not configured as a key field.

Command Modes Flow record configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv6 source address** or **default match ipv6 source address** flow record configuration command.

The following example configures a IPv6 source address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 source address
```

Related Topics

[flow record](#), on page 262

match transport

To configure one or more of the transport fields as a key field for a flow record, use the **match transport** command in flow record configuration mode. To disable the use of one or more of the transport fields as a key field for a flow record, use the **no** form of this command.

```
match transport {destination-port | source-port}
no match transport {destination-port | source-port}
```

Syntax Description

destination-port Configures the transport destination port as a key field.

source-port Configures the transport source port as a key field.

Command Default

The transport fields are not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the destination port as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport destination-port
```

The following example configures the source port as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport source-port
```

Related Topics

[flow record](#), on page 262

mode

To specify the type of sampling and the packet interval for a NetFlow Lite sampler, use the **mode** command in sampler configuration mode. To remove the type of sampling and the packet interval information for a NetFlow Lite sampler, use the **no** form of this command.

```
mode {deterministic | random} 1 out-of window-size
no mode
```

Syntax Description	deterministic	Enables deterministic mode sampling for the sampler.
	random	Enables random mode sampling for the sampler.
	1 out-of <i>window-size</i>	Specifies the window size from which to select packets. The range is 32 to 1022.
Command Default	The mode and the packet interval for a sampler are not configured.	
Command Modes	Sampler configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E

Usage Guidelines

A total of four unique samplers (random or deterministic) are supported on the .

In deterministic mode, packets are chosen periodically based on the configured interval. This mode has less overhead than random mode and can be useful when the device samples traffic that is random in nature.

In random mode, packets are chosen in a manner that should eliminate any bias from traffic patterns and counter any attempt by users to avoid monitoring.

When you attach a monitor using a deterministic sampler, every attachment with the same sampler uses one new free sampler from the out of four available samplers. You cannot attach a monitor with any sampler beyond four attachments. When you attach a monitor using a random sampler, only the first attachment uses a new sampler from the . The remainder of all of the attachments using the same sampler, share the same sampler. Because of this behavior, when using a deterministic sampler, you can always make sure that the correct number of flows are sampled by comparing the sampling rate and what the sends. If the same random sampler is used with multiple interfaces, flows from any interface can always be sampled, and flows from other interfaces can always be skipped.

Examples

The following example enables deterministic sampling with a window size of 1000:

```
Device(config)# sampler SAMPLER-1
Device(config-sampler)# mode deterministic 1 out-of 1000
```

The following example enables random sampling with a window size of 1000:

```
Device(config)# sampler SAMPLER-1
Device(config-sampler)# mode random 1 out-of 1000
```

Related Topics

[debug sampler](#), on page 254

[show sampler](#), on page 291

option

To configure optional data parameters for a flow exporter for NetFlow Lite, use the **option** command in flow exporter configuration mode. To remove optional data parameters for a flow exporter, use the **no** form of this command.

```
option {exporter-stats | interface-table | sampler-table} [{timeout seconds}]
no option {exporter-stats | interface-table | sampler-table}
```

Syntax Description		
	exporter-stats	Configures the exporter statistics option for flow exporters.
	interface-table	Configures the interface table option for flow exporters.
	sampler-table	Configures the export sampler table option for flow exporters.
	timeout <i>seconds</i>	(Optional) Configures the option resend time in seconds for flow exporters. The range is 1 to 86400. The default is 600.

Command Default The timeout is 600 seconds. All other optional data parameters are not configured.

Command Modes Flow exporter configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines The **option exporter-stats** command causes the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent. This command allows the collector to estimate packet loss for the export records it receives. The optional timeout alters the frequency at which the reports are sent.

The **option interface-table** command causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names. The optional timeout can alter the frequency at which the reports are sent.

The **option sampler-table** command causes the periodic sending of an options table, which details the configuration of each sampler and allows the collector to map the sampler ID provided in any flow record to a configuration that it can use to scale up the flow statistics. The optional timeout can alter the frequency at which the reports are sent.

To return this command to its default settings, use the **no option** or **default option** flow exporter configuration command.

The following example shows how to enable the periodic sending of the sampler option table, which allows the collector to map the sampler ID to the sampler type and rate:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option sampler-table
```

The following example shows how to enable the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option exporter-stats
```

The following example shows how to enable the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option interface-table
```

Related Topics

[flow exporter](#), on page 260

record

To add a flow record for a NetFlow Lite flow monitor, use the **record** command in flow monitor configuration mode. To remove a flow record for a NetFlow Lite flow monitor, use the **no** form of this command.

record *record-name*
no record

Syntax Description

record-name Name of a user-defined flow record that was previously configured.

Command Default

A flow record is not configured.

Command Modes

Flow monitor configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Each flow monitor requires a record to define the contents and layout of its cache entries. The flow monitor can use one of the wide range of predefined record formats, or advanced users may create their own record formats.



Note

You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command for the flow monitor.

Examples

The following example configures the flow monitor to use FLOW-RECORD-1:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# record FLOW-RECORD-1
```

Related Topics

[flow monitor](#), on page 261

sampler

To create a NetFlow Lite flow sampler, or to modify an existing NetFlow Lite flow sampler, and to enter NetFlow Lite sampler configuration mode, use the **sampler** command in global configuration mode. To remove a sampler, use the **no** form of this command.

sampler *sampler-name*
no sampler *sampler-name*

Syntax Description

sampler-name Name of the flow sampler that is being created or modified.

Command Default

NetFlow Lite flow samplers are not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Flow samplers are used to reduce the load placed by NetFlow Lite on the networking device to monitor traffic by limiting the number of packets that are analyzed. You configure a rate of sampling that is 1 out of a range of 32 to 1022 packets. Flow samplers are applied to interfaces in conjunction with a flow monitor to implement sampled NetFlow Lite.

To enable flow sampling, you configure the record that you want to use for traffic analysis and assign it to a flow monitor. When you apply a flow monitor with a sampler to an interface, the sampled packets are analyzed at the rate specified by the sampler and compared with the flow record associated with the flow monitor. If the analyzed packets meet the criteria specified by the flow record, they are added to the flow monitor cache.

Examples

The following example creates a flow sampler name SAMPLER-1:

```
Device(config)# sampler SAMPLER-1
Device(config-sampler)#
```

Related Topics

- [debug sampler](#), on page 254
- [mode](#), on page 274
- [show sampler](#), on page 291

show flow exporter

To display flow exporter status and statistics, use the **show flow exporter** command in privileged EXEC mode.

```
show flow exporter [{export-ids netflow-v9} | [name] exporter-name [{statistics | templates}] | statistics | templates}]
```

Syntax Description	
export-ids netflow-v9	(Optional) Displays the NetFlow Version 9 export fields that can be exported and their IDs.
name	(Optional) Specifies the name of a flow exporter.
<i>exporter-name</i>	(Optional) Name of a flow exporter that was previously configured.
statistics	(Optional) Displays statistics for all flow exporters or for the specified flow exporter.
templates	(Optional) Displays template information for all flow exporters or for the specified flow exporter.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

The following example displays the status and statistics for all of the flow exporters configured on a device:

```
Device# show flow exporter
Flow Exporter FLOW-EXPORTER-1:
  Description:           Exports to the datacenter
  Export protocol:       NetFlow Version 9
  Transport Configuration:
    Destination IP address: 192.168.0.1
    Source IP address:     192.168.0.2
    Transport Protocol:    UDP
    Destination Port:      9995
    Source Port:           55864
    DSCP:                  0x0
    TTL:                   255
    Output Features:       Used
```

This table describes the significant fields shown in the display:

Table 13: show flow exporter Field Descriptions

Field	Description
Flow Exporter	The name of the flow exporter that you configured.

Field	Description
Description	The description that you configured for the exporter, or the default description User defined.
Transport Configuration	The transport configuration fields for this exporter.
Destination IP address	The IP address of the destination host.
Source IP address	The source IP address used by the exported packets.
Transport Protocol	The transport layer protocol used by the exported packets.
Destination Port	The destination UDP port to which the exported packets are sent.
Source Port	The source UDP port from which the exported packets are sent.
DSCP	The differentiated services code point (DSCP) value.
TTL	The time-to-live value.
Output Features	Specifies whether the output-features command, which causes the output features to be run on Flexible NetFlow export packets, has been used or not.

The following example displays the status and statistics for all of the flow exporters configured on a device:

```
Device# show flow exporter name FLOW-EXPORTER-1 statistics
Flow Exporter FLOW-EXPORTER-1:
  Packet send statistics (last cleared 2w6d ago):
    Successfully sent:          0                (0 bytes)
```

Related Topics

[clear flow exporter](#), on page 242

[debug flow exporter](#), on page 252

[flow exporter](#), on page 260

show flow interface

To display the NetFlow Lite configuration and status for an interface, use the **show flow interface** command in privileged EXEC mode.

show flow interface [*type number*]

Syntax Description	<i>type</i>	(Optional) The type of interface on which you want to display NetFlow Lite accounting configuration information.
	<i>number</i>	(Optional) The number of the interface on which you want to display NetFlow Lite accounting configuration information.
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Examples

The following example displays the NetFlow Lite accounting configuration on Ethernet interfaces 0/0 and 0/1:

```
Device# show flow interface gigabitethernet1/0/1

Interface Ethernet1/0
  monitor:          FLOW-MONITOR-1
  direction:        Output
  traffic(ip):      on
Device# show flow interface gigabitethernet1/0/2
Interface Ethernet0/0
  monitor:          FLOW-MONITOR-1
  direction:        Input
  traffic(ip):      sampler SAMPLER-2#
```

The table below describes the significant fields shown in the display.

Table 14: show flow interface Field Descriptions

Field	Description
Interface	The interface to which the information applies.
monitor	The name of the flow monitor that is configured on the interface.
direction:	The direction of traffic that is being monitored by the flow monitor. The possible values are: <ul style="list-style-type: none"> • Input—Traffic is being received by the interface. • Output—Traffic is being transmitted by the interface.

Field	Description
traffic(ip)	Indicates if the flow monitor is in normal mode or sampler mode. The possible values are: <ul style="list-style-type: none">• on—The flow monitor is in normal mode.• sampler—The flow monitor is in sampler mode (the name of the sampler will be included in the display).

Related Topics

[show flow monitor](#), on page 284

show flow monitor

To display the status and statistics for a NetFlow Lite flow monitor, use the **show flow monitor** command in privileged EXEC mode.

```
show flow monitor [[name] monitor-name [cache [format {csv | record | table}]] [statistics]]
```

Syntax Description

name	(Optional) Specifies the name of a flow monitor.
<i>monitor-name</i>	(Optional) Name of a flow monitor that was previously configured.
cache	(Optional) Displays the contents of the cache for the flow monitor.
format	(Optional) Specifies the use of one of the format options for formatting the display output.
csv	(Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format.
record	(Optional) Displays the flow monitor cache contents in record format.
table	(Optional) Displays the flow monitor cache contents in table format.
statistics	(Optional) Displays the statistics for the flow monitor.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

The **cache** keyword uses the record format by default.

The uppercase field names in the display output of the **show flowmonitor** *monitor-name* **cache** command are key fields that NetFlow Lite uses to differentiate flows. The lowercase field names in the display output of the **show flow monitor** *monitor-name* **cache** command are nonkey fields from which NetFlow Lite collects values as additional data for the cache.

Examples

The following example displays the status for a flow monitor:

```
Device# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:      Used for basic traffic analysis
  Flow Record:     flow-record-1
  Flow Exporter:   flow-exporter-1
                  flow-exporter-2
  Cache:
    Type:          normal
    Status:        allocated
    Size:          4096 entries / 311316 bytes
    Inactive Timeout: 15 secs
    Active Timeout: 1800 secs
```

Update Timeout: 1800 secs

This table describes the significant fields shown in the display.

Table 15: show flow monitor monitor-name Field Descriptions

Field	Description
Flow Monitor	Name of the flow monitor that you configured.
Description	Description that you configured or the monitor, or the default description User defined.
Flow Record	Flow record assigned to the flow monitor.
Flow Exporter	Exporters that are assigned to the flow monitor.
Cache	Information about the cache for the flow monitor.
Type	Flow monitor cache type. The possible values are: <ul style="list-style-type: none"> • immediate—Flows are expired immediately. • normal—Flows are expired normally. • Permanent—Flows are never expired.
Status	Status of the flow monitor cache. The possible values are: <ul style="list-style-type: none"> • allocated—The cache is allocated. • being deleted—The cache is being deleted. • not allocated—The cache is not allocated.
Size	Current cache size.
Inactive Timeout	Current value for the inactive timeout in seconds.
Active Timeout	Current value for the active timeout in seconds.
Update Timeout	Current value for the update timeout in seconds.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1:

```
Device# show flow monitor FLOW-MONITOR-1 cache
Cache type: Normal
Cache size: 4096
Current entries: 8
High Watermark: 10
Flows added: 1560
Flows aged: 1552
- Active timeout ( 1800 secs) 24
- Inactive timeout ( 15 secs) 1528
- Event aged 0
```

```

- Watermark aged          0
- Emergency aged         0
IP TOS:                   0x00
IP PROTOCOL:              6
IPV4 SOURCE ADDRESS:     10.0.0.1
IPV4 DESTINATION ADDRESS: 172.16.0.1
TRNS SOURCE PORT:        20
TRNS DESTINATION PORT:   20
INTERFACE INPUT:         Et0/0
FLOW SAMPLER ID:         0
ip source as:            0
ip destination as:       0
ipv4 next hop address:   172.16.0.2
ipv4 source mask:        /0
ipv4 destination mask:   /24
tcp flags:               0x00
interface output:        Et1/0
counter bytes:           198520
counter packets:         4963
timestamp first:         10564356
timestamp last:          12154104

```

This table describes the significant fields shown in the display.

Table 16: show flow monitor monitor-name cache Field Descriptions

Field	Description
Cache type	Flow monitor cache type. The possible values are: <ul style="list-style-type: none"> • Immediate—Flows are expired immediately. • Normal—Flows are expired normally. • Permanent—Flows are never expired.
Cache Size	Number of entries in the cache.
Current entries	Number of entries in the cache that are in use.
High Watermark	Highest number of cache entries seen.
Flows added	Flows added to the cache since the cache was created.
Flows aged	Flows expired from the cache since the cache was created.
Active timeout	Current value for the active timeout in seconds.
Inactive timeout	Current value for the inactive timeout in seconds.
Event aged	Number of flows that have been aged by an event such as using the force-export option for the clear flow monitor command.
Watermark aged	Number of flows that have been aged because they exceeded the maximum high watermark value.

Field	Description
Emergency aged	Number of flows that have been aged because the cache size was exceeded.
IP TOS	IP type of service (ToS) value.
IP PROTOCOL	Protocol number.
IPV4 SOURCE ADDRESS	IPv4 source address.
IPV4 DESTINATION ADDRESS	IPv4 destination address.
TRNS SOURCE PORT	Source port for the transport protocol.
TRNS DESTINATION PORT	Destination port for the transport protocol.
INTERFACE INPUT	Interface on which the input is received.
FLOW SAMPLER ID	Flow sampler ID number.
ip source as	Border Gateway Protocol (BGP) source autonomous system number.
ip destination as	BGP destination autonomous system number.
ipv4 next hop address	IPv4 address of the next hop to which the packet is forwarded.
ipv4 source mask	IPv4 source address mask.
ipv4 destination mask	IPv4 destination address mask.
tcp flags	Value of the TCP flags.
interface output	Interface on which the input is transmitted.
counter bytes	Number of bytes that have been counted.
counter packets	Number of packets that have been counted.
timestamp first	Time stamp of the first packet in the flow.
timestamp last	Time stamp of the last packet in the flow.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1 in a table format:

```
Device# show flow monitor FLOW-MONITOR-1 cache format table
```

```
Cache type:                Normal
Cache size:                4096
Current entries:           4
High Watermark:           6
Flows added:               90
Flows aged:               86
- Active timeout ( 1800 secs) 0
- Inactive timeout ( 15 secs) 86
- Event aged                0
- Watermark aged            0
```

```

- Emergency aged                                0
IP TOS  IP PROT  IPV4 SRC ADDR  IPV4 DST ADDR  TRNS SRC PORT  TRNS DST PORT
=====
0x00    1    10.251.10.1    172.16.10.2    0                02
0x00    1    10.251.10.1    172.16.10.2    0                20484
0xC0    17   172.16.6.1     224.0.0.9      520              5202
0x00    6    10.10.11.1     172.16.10.5    25               252

```

The following example displays the status, statistics, and data for the flow monitor named **FLOW-MONITOR-IPv6** (the cache contains IPv6 data) in record format:

```
Device# show flow monitor name FLOW-MONITOR-IPv6 cache format record
```

```

Cache type:                                Normal
Cache size:                                4096
Current entries:                            6
High Watermark:                             8
Flows added:                                1048
Flows aged:                                 1042
- Active timeout ( 1800 secs)                11
- Inactive timeout ( 15 secs)                1031
- Event aged                                  0
- Watermark aged                              0
- Emergency aged                              0
IPV6 FLOW LABEL:                            0
IPV6 EXTENSION MAP:                         0x00000040
IPV6 SOURCE ADDRESS:                        2001:DB8:1:ABCD::1
IPV6 DESTINATION ADDRESS:                   2001:DB8:4:ABCD::2
TRNS SOURCE PORT:                           3000
TRNS DESTINATION PORT:                       55
INTERFACE INPUT:                             Et0/0
FLOW DIRECTION:                              Input
FLOW SAMPLER ID:                             0
IP PROTOCOL:                                 17
IP TOS:                                       0x00
ip source as:                                0
ip destination as:                           0
ipv6 next hop address:                       ::
ipv6 source mask:                            /48
ipv6 destination mask:                       /0
tcp flags:                                   0x00
interface output:                             Null
counter bytes:                               521192
counter packets:                             9307
timestamp first:                             9899684
timestamp last:                              11660744

```

The following example displays the status and statistics for a flow monitor:

```
Device# show flow monitor FLOW-MONITOR-1 statistics
```

```

Cache type:                                Normal
Cache size:                                4096
Current entries:                            4
High Watermark:                             6
Flows added:                                116
Flows aged:                                 112
- Active timeout ( 1800 secs)                0
- Inactive timeout ( 15 secs)                112
- Event aged                                  0
- Watermark aged                              0
- Emergency aged                              0

```

Related Topics

[clear flow monitor](#), on page 243

[debug flow monitor](#), on page 253

show flow record

To display the status and statistics for a NetFlow Lite flow record, use the **show flow record** command in privileged EXEC mode.

```
show flow record [{{name} record-name}]
```

Syntax Description	name (Optional) Specifies the name of a flow record.				
	<i>record-name</i> (Optional) Name of a user-defined flow record that was previously configured.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.				

The following example displays the status and statistics for FLOW-RECORD-1:

```
Device# show flow record FLOW-RECORD-1
flow record FLOW-RECORD-1:
  Description:      User defined
  No. of users:    0
  Total field space: 24 bytes
  Fields:
    match ipv6 destination address
    match transport source-port
    collect interface input
```

Related Topics

[record](#), on page 278

show sampler

To display the status and statistics for a NetFlow Lite sampler, use the **show sampler** command in privileged EXEC mode.

```
show sampler [{[name] sampler-name}]
```

Syntax Description	name (Optional) Specifies the name of a sampler.				
	sampler-name (Optional) Name of a sampler that was previously configured.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.				

The following example displays the status and statistics for all of the flow samplers configured:

```
Device# show sampler
Sampler SAMPLER-1:
  ID:                2083940135
  export ID:         0
  Description:       User defined
  Type:              Invalid (not in use)
  Rate:              1 out of 32
  Samples:           0
  Requests:          0
  Users (0):

Sampler SAMPLER-2:
  ID:                3800923489
  export ID:         1
  Description:       User defined
  Type:              random
  Rate:              1 out of 100
  Samples:           1
  Requests:          124
  Users (1):
    flow monitor FLOW-MONITOR-1 (datalink,vlan1) 0 out of 0
```

This table describes the significant fields shown in the display.

Table 17: show sampler Field Descriptions

Field	Description
ID	ID number of the flow sampler.
Export ID	ID of the flow sampler export.

Field	Description
Description	Description that you configured for the flow sampler, or the default description User defined.
Type	Sampling mode that you configured for the flow sampler.
Rate	Window size (for packet selection) that you configured for the flow sampler. The range is 2 to 32768.
Samples	Number of packets sampled since the flow sampler was configured or the device was restarted. This is equivalent to the number of times a positive response was received when the sampler was queried to determine if the traffic needed to be sampled. See the explanation of the Requests field in this table.
Requests	Number of times the flow sampler was queried to determine if the traffic needed to be sampled.
Users	Interfaces on which the flow sampler is configured.

Related Topics

[debug sampler](#), on page 254

[sampler](#), on page 279

source

To configure the source IP address interface for all of the packets sent by a NetFlow Lite flow exporter, use the **source** command in flow exporter configuration mode. To remove the source IP address interface for all of the packets sent by a NetFlow Lite flow exporter, use the **no** form of this command.

```
source interface-type interface-number
no source
```

Syntax Description

<i>interface-type</i>	Type of interface whose IP address you want to use for the source IP address of the packets sent by a NetFlow Lite flow exporter.
<i>interface-number</i>	Interface number whose IP address you want to use for the source IP address of the packets sent by a NetFlow Lite flow exporter.

Command Default

The IP address of the interface over which the NetFlow Lite datagram is transmitted is used as the source IP address.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

The benefits of using a consistent IP source address for the datagrams that NetFlow Lite sends include the following:

- The source IP address of the datagrams exported by NetFlow Lite is used by the destination system to determine from which device the NetFlow Lite data is arriving. If your network has two or more paths that can be used to send NetFlow Lite datagrams from the device to the destination system and you do not specify the source interface from which the source IP address is to be obtained, the device uses the IP address of the interface over which the datagram is transmitted as the source IP address of the datagram. In this situation the destination system might receive NetFlow Lite datagrams from the same device, but with different source IP addresses. When the destination system receives NetFlow Lite datagrams from the same device with different source IP addresses, the destination system treats the NetFlow Lite datagrams as if they were being sent from different devices. To avoid having the destination system treat the NetFlow Lite datagrams as if they were being sent from different devices, you must configure the destination system to aggregate the NetFlow Lite datagrams it receives from all of the possible source IP addresses in the device into a single NetFlow Lite flow.
- If your device has multiple interfaces that can be used to transmit datagrams to the destination system, and you do not configure the **source** command, you will have to add an entry for the IP address of each interface into any access lists that you create for permitting NetFlow Lite traffic. Creating and maintaining access lists for permitting NetFlow Lite traffic from known sources and blocking it from unknown sources is easier when you limit the source IP address for NetFlow Lite datagrams to a single IP address for each device that is exporting NetFlow Lite traffic.



Caution The interface that you configure as the **source** interface must have an IP address configured, and it must be up.



Tip When a transient outage occurs on the interface that you configured with the **source** command, the NetFlow Lite exporter reverts to the default behavior of using the IP address of the interface over which the datagrams are being transmitted as the source IP address for the datagrams. To avoid this problem, use a loopback interface as the source interface because loopback interfaces are not subject to the transient outages that can occur on physical interfaces.

To return this command to its default settings, use the **no source** or **default source** flow exporter configuration command.

Examples

The following example shows how to configure NetFlow Lite to use a loopback interface as the source interface for NetFlow traffic:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# source loopback 0
```

Related Topics

[flow exporter](#), on page 260

statistics packet protocol

To collect protocol distribution statistics for a flow monitor, use the **statistics packet protocol** command in flow monitor configuration mode. To disable collecting protocol distribution statistics and size distribution statistics for a flow monitor, use the **no** form of this command.

statistics packet protocol
no statistics packet protocol

Syntax Description	This command has no arguments or keywords.				
Command Default	The collection of protocol distribution statistics for a flow monitor is not enabled by default.				
Command Modes	Flow monitor configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)E</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.				

Usage Guidelines Before you can collect protocol distribution statistics for a flow monitor with the **statistics packet protocol** command, you must define the protocol, source and destination ports, first and last time stamps and packet and bytes counters in the flow record. If you do not define these fields, you will get the following warning:

Warning: Cannot set protocol distribution with this Flow Record. Require protocol, source and destination ports, first and last timestamps and packet and bytes counters.

To return this command to its default settings, use the **no statistics packet protocol** or **default statistics packet protocol** flow monitor configuration command.

The following example enables the collection of protocol distribution statistics for flow monitors:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# statistics packet protocol
```

Related Topics

[flow exporter](#), on page 260

template data timeout

To specify a timeout period for resending flow exporter template data, use the **template data timeout** command in flow exporter configuration mode. To remove the template resend timeout for a flow exporter, use the **no** form of this command.

template data timeout *seconds*
no template data timeout *seconds*

Syntax Description	<i>seconds</i> Timeout value in seconds. The range is 1 to 86400. The default is 600.
---------------------------	---

Command Default	The default template resend timeout for a flow exporter is 600 seconds.
------------------------	---

Command Modes	Flow exporter configuration
----------------------	-----------------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines	<p>Flow exporter template data describes the exported data records. Data records cannot be decoded without the corresponding template. The template data timeout command controls how often those templates are exported.</p> <p>To return this command to its default settings, use the no template data timeout or default template data timeout flow record exporter command.</p>
-------------------------	---

The following example configures resending templates based on a timeout of 1000 seconds:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# template data timeout 1000
```

Related Topics

[flow exporter](#), on page 260

transport

To configure the transport protocol for a flow exporter for NetFlow Lite, use the **transport** command in flow exporter configuration mode. To remove the transport protocol for a flow exporter, use the **no** form of this command.

```
transport udp udp-port
no transport udp udp-port
```

Syntax Description	udp <i>udp-port</i> Specifies User Datagram Protocol (UDP) as the transport protocol and the UDP port number.				
Command Default	Flow exporters use UDP on port 9995.				
Command Modes	Flow exporter configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.				
Usage Guidelines	<p>To return this command to its default settings, use the no transport or default transport flow exporter configuration command.</p> <p>The following example configures UDP as the transport protocol and a UDP port number of 250:</p> <pre>Device(config)# flow exporter FLOW-EXPORTER-1 Device(config-flow-exporter)# transport udp 250</pre>				

Related Topics

[flow exporter](#), on page 260

ttl

To configure the time-to-live (TTL) value, use the **ttl** command in flow exporter configuration mode. To remove the TTL value, use the **no** form of this command.

```
ttl ttl
no ttl ttl
```

Syntax Description

ttl Time-to-live (TTL) value for exported datagrams. The range is 1 to 255. The default is 255.

Command Default

Flow exporters use a TTL of 255.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

To return this command to its default settings, use the **no ttl** or **default ttl** flow exporter configuration command.

The following example specifies a TTL of 15:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# ttl 15
```

Related Topics

[flow exporter](#), on page 260



PART **V**

Network Management

- [Network Management](#) , on page 301



Network Management

- [monitor session](#), on page 302
- [monitor session destination](#), on page 304
- [monitor session filter](#), on page 308
- [monitor session source](#), on page 310
- [show monitor](#), on page 313
- [snmp-server enable traps](#), on page 316
- [snmp-server enable traps bridge](#), on page 319
- [snmp-server enable traps cpu](#), on page 320
- [snmp-server enable traps envmon](#), on page 321
- [snmp-server enable traps errdisable](#), on page 322
- [snmp-server enable traps flash](#), on page 323
- [snmp-server enable traps mac-notification](#), on page 324
- [snmp-server enable traps port-security](#), on page 325
- [snmp-server enable traps rtr](#), on page 326
- [snmp-server enable traps snmp](#), on page 328
- [snmp-server enable traps storm-control](#), on page 329
- [snmp-server enable traps stpx](#), on page 330

monitor session

To create a new Ethernet Switched Port Analyzer (SPAN) or a Remote Switched Port Analyzer (RSPAN) session configuration for analyzing traffic between ports or add to an existing session configuration, use the **monitor session** global configuration command. To clear SPAN or RSPAN sessions, use the **no** form of this command.

monitor session *session-number* {**destination** | **filter** | **source**}

no monitor session {*session-number* [**destination** | **filter** | **source**] | **all** | **local** | **range** *session-range* | **remote**}

Syntax Description		
	<i>session-number</i>	The session number identified with the SPAN or RSPAN session. The range is 1 to 68. However if this switch is stacked with Catalyst 2960-S switches, the range is 1 to 66.
	all	Clears all monitor sessions.
	local	Clears all local monitor sessions.
	range <i>session-range</i>	Clears monitor sessions in the specified range.
	remote	Clears all remote monitor sessions.

Command Default No monitor sessions are configured.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines You can set a combined maximum of four local SPAN sessions and RSPAN source sessions. You can have a total of 68 SPAN and RSPAN sessions on a switch or switch stack. However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions, and the range is 1 to 66.

A private-VLAN port cannot be configured as a SPAN destination port.

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.

Example

This example shows how to create a local SPAN session 1 to monitor traffic on Po13 (an EtherChannel port) and limit SPAN traffic in the session only to VLAN 1281. Egress traffic replicates the source; ingress forwarding is not enabled.

```
Device(config)# monitor session 1 source interface Po13
```



```
Device(config)# monitor session 1 filter vlan 1281
Device(config)# monitor session 1 destination interface GigabitEthernet2/0/36 encapsulation
  replicate
Device(config)# monitor session 1 destination interface GigabitEthernet3/0/36 encapsulation
  replicate
```

The following is the output of a **show monitor session all** command after completing these setup instructions:

```
Device# show monitor session all

Session 1
-----
Type                : Local Session
Source Ports        :
  Both              : Po13
Destination Ports   : Gi2/0/36,Gi3/0/36
Encapsulation       : Replicate
  Ingress           : Disabled
Filter VLANs        : 1281
...
```

Related Topics

- [monitor session destination](#), on page 304
- [monitor session filter](#), on page 308
- [monitor session source](#), on page 310
- [show monitor](#), on page 313

monitor session destination

To start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) destination session, to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance), and to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, use the **monitor session destination** global configuration command. To remove the SPAN or RSPAN session or to remove destination interfaces from the SPAN or RSPAN session, use the **no** form of this command.

```
monitor session session-number destination {interface interface-id [, | -] [encapsulation
{replicate | dot1q} ] {ingress [dot1q | untagged] } | {remote} vlan vlan-id
no monitor session session-number destination {interface interface-id [, | -] [encapsulation
{replicate | dot1q} ] {ingress [dot1q | untagged] } | {remote} vlan vlan-id
```

Syntax Description

<i>session-number</i>	The session number identified with the SPAN or RSPAN session. The range is 1 to 68. However if this switch is stacked with Catalyst 2960-S switches, the range is 1 to 66.
interface <i>interface-id</i>	Specifies the destination or source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type, stack member, module, and port number). For source interface, port channel is also a valid interface type, and the valid range is 1 to 128.
,	(Optional) Specifies a series of interfaces or VLANs, or separates a range of interfaces or VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specifies a range of interfaces or VLANs. Enter a space before and after the hyphen.
encapsulation replicate	(Optional) Specifies 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. The encapsulation options are ignored with the no form of the command.

encapsulation dot1q	(Optional) Specifies that the destination interface accepts the source interface incoming packets with IEEE 802.1Q encapsulation. 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. The encapsulation options are ignored with the no form of the command.
ingress	Enables ingress traffic forwarding.
dot1q	(Optional) Accepts incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.
untagged	(Optional) Accepts incoming packets with untagged encapsulation with the specified VLAN as the default VLAN.
isl	Specifies ingress forwarding using ISL encapsulation.
remote	Specifies 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).
vlan <i>vlan-id</i>	Sets the default VLAN for ingress traffic when used with only the ingress keyword.

Command Default

No monitor sessions are configured.

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.

You can specify **all**, **local**, **range** *session-range*, or **remote** with the **no monitor session** command to clear all SPAN and RSPAN, all local SPAN, a range, or all RSPAN sessions.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

You can set a combined maximum of four local SPAN sessions and RSPAN source sessions. You can have a total of 68 SPAN and RSPAN sessions on a switch or switch stack. However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions, and the range is 1 to 66.

A SPAN or RSPAN destination must be a physical port.

You can have a maximum of 64 destination ports on a switch or a switch stack.

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.

A private-VLAN port cannot be configured as a SPAN destination port.

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.

You can enable IEEE 802.1x authentication on a port that is a SPAN or RSPAN destination port; however, IEEE 802.1x authentication is disabled until the port is removed as a SPAN destination. If IEEE 802.1x authentication is not available on the port, the switch returns an error message. You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.

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 function 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** 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.)

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.

Examples

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2:

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

This example shows how to delete a destination port from an existing local SPAN session:

```
Device(config)# no monitor session 2 destination interface gigabitethernet1/0/2
```

This example shows how to configure RSPAN source session 1 to monitor a source interface and to configure the destination RSPAN VLAN 900:

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
Device(config)# monitor session 1 destination remote vlan 900
Device(config)# end
```

This example shows how to configure an RSPAN destination session 10 in the switch receiving the monitored traffic:

```
Device(config)# monitor session 10 source remote vlan 900
Device(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

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.

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 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.

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress untagged
vlan 5
```

Related Topics

- [monitor session](#), on page 302
- [monitor session filter](#), on page 308
- [monitor session source](#), on page 310
- [show monitor](#), on page 313

monitor session filter

To start a new flow-based SPAN (FSPAN) session or flow-based RSPAN (FRSPAN) source or destination session, or to limit (filter) SPAN source traffic to specific VLANs, use the **monitor session filter** global configuration command. To remove filters from the SPAN or RSPAN session, use the **no** form of this command.

monitor session *session-number* **filter** {**vlan** *vlan-id* [, | -] }

no monitor session *session-number* **filter** {**vlan** *vlan-id* [, | -] }

Syntax Description		
<i>session-number</i>		The session number identified with the SPAN or RSPAN session. The range is 1 to 68. However if this switch is stacked with Catalyst 2960-S switches, the range is 1 to 66.
vlan <i>vlan-id</i>		Specifies a list of VLANs as filters on trunk source ports to limit SPAN source traffic to specific VLANs. The <i>vlan-id</i> range is 1 to 4094.
,		(Optional) Specifies a series of VLANs, or separates a range of VLANs from a previous range. Enter a space before and after the comma.
-		(Optional) Specifies a range of VLANs. Enter a space before and after the hyphen.
Command Default	No monitor sessions are configured.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

You can set a combined maximum of four local SPAN sessions and RSPAN source sessions. You can have a total of 68 SPAN and RSPAN sessions on a switch or switch stack. However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions, and the range is 1 to 66.

You can monitor traffic on a single VLAN or on a series or range of ports or VLANs. You select a series or range of VLANs by using the [, | -] options.

If you specify a series of VLANs, you must enter a space before and after the comma. If you specify a range of VLANs, you must enter a space before and after the hyphen (-).

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.

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.

Examples

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 create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2 and to filter IPv4 traffic using access list number 122 in an FSPAN session:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 1 filter ip access-group 122
```

Related Topics

- [monitor session](#), on page 302
- [monitor session destination](#), on page 304
- [monitor session source](#), on page 310
- [show monitor](#), on page 313

monitor session source

To start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) source session, or to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, use the **monitor session source** global configuration command. To remove the SPAN or RSPAN session or to remove source interfaces from the SPAN or RSPAN session, use the **no** form of this command.

```
monitor session session_number source {interface interface-id [, | -] [both | rx | tx] |
[remote] vlan vlan-id [, | -] [both | rx | tx] }
no monitor session session_number source {interface interface-id [, | -] [both | rx | tx] |
[remote] vlan vlan-id [, | -] [both | rx | tx] }
```

Syntax Description

<i>session_number</i>	The session number identified with the SPAN or RSPAN session. The range is 1 to 68. However if this switch is stacked with Catalyst 2960-S switches, the range is 1 to 66.
interface <i>interface-id</i>	Specifies the source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type, stack member, module, and port number). For source interface, port channel is also a valid interface type, and the valid range is 1 to 48.
,	(Optional) Specifies a series of interfaces or VLANs, or separates a range of interfaces or VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specifies a range of interfaces or VLANs. Enter a space before and after the hyphen.
both rx tx	(Optional) Specifies the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.
remote	(Optional) Specifies 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).
vlan <i>vlan-id</i>	When used with only the ingress keyword, sets default VLAN for ingress traffic.

Command Default

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.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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 four local SPAN sessions and RSPAN source sessions. You can have a total of 68 SPAN and RSPAN sessions on a switch or switch stack. However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions, and the range is 1 to 66.

A source can be a physical port, a port channel, or a VLAN.

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 (-).

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.

You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.

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.

Examples

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

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 gigabitethernet1/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

Related Topics

[monitor session](#), on page 302

[monitor session destination](#), on page 304

[monitor session filter](#), on page 308

[show monitor](#), on page 313

show monitor

To display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions, use the **show monitor** command in EXEC mode.

show monitor [**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} [**detail**]

Syntax Description	
session	(Optional) Displays information about specified SPAN sessions.
<i>session_number</i>	The session number identified with the SPAN or RSPAN session. The range is 1 to 68. However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions, and the range is 1 to 66.
all	(Optional) Displays all SPAN sessions.
local	(Optional) Displays only local SPAN sessions.
range <i>list</i>	(Optional) Displays a range of SPAN sessions, where <i>list</i> is the range of valid sessions. The range is 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	(Optional) Displays only remote SPAN sessions.
detail	(Optional) Displays detailed information about the specified sessions.

Command Modes
User EXEC
Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines The output is the same for the **show monitor** command and the **show monitor session all** command.

Maximum number of SPAN source sessions: 4 (applies to source and local sessions) However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions.

Examples

This is an example of output for the **show monitor** user EXEC command:

```
Device# show monitor
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
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:

```
Device# show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
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:

```
Device# show monitor session all
Session 1
-----
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encaps : DOT1Q
Session 2
-----
Type : Local Session
Source Ports :
Both : Gi4/0/8
```

```
Destination Ports : Gi4/012  
Encapsulation : Replicate  
Ingress : Enabled, default VLAN = 4  
Ingress encap : Untagged
```

Related Topics

- [monitor session](#), on page 302
- [monitor session destination](#), on page 304
- [monitor session filter](#), on page 308
- [monitor session source](#), on page 310

snmp-server enable traps

To enable the device to send Simple Network Management Protocol (SNMP) notifications for various traps or inform requests to the network management system (NMS), use the **snmp-server enable traps** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps [bridge | cluster | config | copy-config | cpu threshold | entity
| envmon | errdisable | flash | fru-ctrl | hsrp | ipmulticast | mac-notification | msdp
| ospf | pim | port-security | rtr | snmp | storm-control | stpx | syslog | tty |
vlan-membership | vlancreate | vlandelete | vtp ]
```

```
no snmp-server enable traps [bridge | cluster | config | copy-config | cpu threshold |
entity | envmon | errdisable | flash | fru-ctrl | hsrp | ipmulticast | mac-notification |
msdp | ospf | pim | port-security | rtr | snmp | storm-control | stpx | syslog | tty
| vlan-membership | vlancreate | vlandelete | vtp ]
```

Syntax Description	
bridge	(Optional) Enables SNMP STP Bridge MIB traps.*
cluster	(Optional) Enables SNMP cluster traps.
config	(Optional) Enables SNMP configuration traps.
copy-config	(Optional) Enables SNMP copy-configuration traps.
cpu threshold	(Optional) Enables CPU related traps.*
entity	(Optional) Enables SNMP entity traps.
envmon	(Optional) Enables SNMP environmental monitor traps.*
errdisable	(Optional) Enables SNMP errdisable notification traps.*
flash	(Optional) Enables SNMP FLASH notification traps.*
fru-ctrl	(Optional) Generates entity field-replaceable unit (FRU) control traps. In a device stack, this trap refers to the insertion or removal of a device in the stack.
hsrp	(Optional) Enables Hot Standby Router Protocol (HSRP) traps.
ipmulticast	(Optional) Enables IP multicast routing traps.
mac-notification	(Optional) Enables SNMP MAC Notification traps.*
msdp	(Optional) Enables Multicast Source Discovery Protocol (MSDP) traps.
ospf	(Optional) Enables Open Shortest Path First (OSPF) traps.
pim	(Optional) Enables Protocol-Independent Multicast (PIM) traps.
port-security	(Optional) Enables SNMP port security traps.*
rtr	(Optional) Enables SNMP Response Time Reporter (RTR) traps.

snmp	(Optional) Enables SNMP traps.*
storm-control	(Optional) Enables SNMP storm-control trap parameters.*
stpx	(Optional) Enables SNMP STPX MIB traps.*
syslog	(Optional) Enables SNMP syslog traps.
tty	(Optional) Sends TCP connection traps. This is enabled by default.
vlan-membership	(Optional) Enables SNMP VLAN membership traps.
vlancreate	(Optional) Enables SNMP VLAN-created traps.
vlandelete	(Optional) Enables SNMP VLAN-deleted traps.
vtp	(Optional) Enables VLAN Trunking Protocol (VTP) traps.

Command Default

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	This command was introduced.

Usage Guidelines

The command options marked with an asterisk in the table above have subcommands. For more information on these subcommands, see the Related Commands section below.

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**

Though visible in the command-line help strings, the **fru-ctrl**, **insertion**, and **removal** keywords are not supported on the device. 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.

**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 enable more than one type of SNMP trap:

```
Device(config)# snmp-server enable traps cluster
Device(config)# snmp-server enable traps config
```

```
Device(config)# snmp-server enable traps vtp
```


snmp-server enable traps bridge

To generate STP bridge MIB traps, use the **snmp-server enable traps bridge** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps bridge [newroot] [topologychange]
no snmp-server enable traps bridge [newroot] [topologychange]
```

Syntax Description

newroot (Optional) Enables SNMP STP bridge MIB new root traps.

topologychange (Optional) Enables SNMP STP bridge MIB topology change traps.

Command Default

The sending of bridge SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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.



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 bridge new root traps to the NMS:

```
Device(config)# snmp-server enable traps bridge newroot
```

Related Topics

[snmp-server host](#)

snmp-server enable traps cpu

To enable CPU notifications, use the **snmp-server enable traps cpu** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps cpu [**threshold**]
no snmp-server enable traps cpu [**threshold**]

Syntax Description **threshold** (Optional) Enables CPU threshold notification.

Command Default The sending of CPU notifications is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E
		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.



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 generate CPU threshold notifications:

```
Device(config)# snmp-server enable traps cpu threshold
```

Related Topics

[snmp-server host](#)

snmp-server enable traps envmon

To enable SNMP environmental traps, use the **snmp-server enable traps envmon** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps envmon [fan] [shutdown] [status] [supply] [temperature]
no snmp-server enable traps envmon [fan] [shutdown] [status] [supply] [temperature]
```

Syntax Description

fan	(Optional) Enables fan traps.
shutdown	(Optional) Enables environmental monitor shutdown traps.
status	(Optional) Enables SNMP environmental status-change traps.
supply	(Optional) Enables environmental monitor power-supply traps.
temperature	(Optional) Enables environmental monitor temperature traps.

Command Default

The sending of environmental SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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.



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 generate fan traps:

```
Device(config)# snmp-server enable traps envmon fan
```

Related Topics

[snmp-server host](#)

snmp-server enable traps errdisable

To enable SNMP notifications of error-disabling, use the **snmp-server enable traps errdisable** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]
no snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]

Syntax Description	notification-rate <i>number-of-notifications</i>	(Optional) Specifies number of notifications per minute as the notification rate. Accepted values are from 0 to 10000.
Command Default	The sending of SNMP notifications of error-disabling is disabled.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	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.	



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 set the number SNMP notifications of error-disabling to 2:

```
Device(config)# snmp-server enable traps errdisable notification-rate 2
```

Related Topics

[snmp-server host](#)

snmp-server enable traps flash

To enable SNMP flash notifications, use the **snmp-server enable traps flash** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps flash [insertion] [removal]
no snmp-server enable traps flash [insertion] [removal]
```

Syntax Description

insertion (Optional) Enables SNMP flash insertion notifications.

removal (Optional) Enables SNMP flash removal notifications.

Command Default

The sending of SNMP flash notifications is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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.



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 generate SNMP flash insertion notifications:

```
Device(config)# snmp-server enable traps flash insertion
```

Related Topics

[snmp-server host](#)

snmp-server enable traps mac-notification

To enable SNMP MAC notification traps, use the **snmp-server enable traps mac-notification** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps mac-notification [**change**] [**move**] [**threshold**]
no snmp-server enable traps mac-notification [**change**] [**move**] [**threshold**]

Syntax Description

change (Optional) Enables SNMP MAC change traps.

move (Optional) Enables SNMP MAC move traps.

threshold (Optional) Enables SNMP MAC threshold traps.

Command Default

The sending of SNMP MAC notification traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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.



Note

Inform traps 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 generate SNMP MAC notification change traps:

```
Device(config)# snmp-server enable traps mac-notification change
```

Related Topics

[snmp-server host](#)

snmp-server enable traps port-security

To enable SNMP port security traps, use the **snmp-server enable traps port-security** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps port-security [trap-rate value]
no snmp-server enable traps port-security [trap-rate value]
```

Syntax Description	trap-rate <i>value</i>	(Optional) Sets the maximum number of port-security traps sent per second. The range is from 0 to 1000; the default is 0 (no limit imposed; a trap is sent at every occurrence).
Command Default	The sending of port security SNMP traps is disabled.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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.



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 enable port-security traps at a rate of 200 per second:

```
Device(config)# snmp-server enable traps port-security trap-rate 200
```

Related Topics

[snmp-server host](#)

snmp-server enable traps rtr

To enable the sending of Cisco IOS IP Service Level Agreements (SLAs) Simple Network Management Protocol (SNMP) trap notifications, use the **snmp-server enable traps rtr** command in global configuration mode. To disable IP SLAs SNMP notifications, use the **no** form of this command.

snmp-server enable traps rtr
no snmp-server enable traps rtr

Syntax Description This command has no arguments or keywords.

Command Default SNMP notifications are disabled by default.

Command Modes Global configuration

Release	Modification
Cisco IOS 11.3	This command was introduced.
Cisco IOS 12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS 12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines This command controls (enables or disables) Cisco IOS IP SLAs notifications, as defined in the Response Time Monitor MIB (CISCO-RTTMON-MIB).

The **snmp-server enable traps rtr** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send IP SLAs SNMP traps to the host at the address myhost.cisco.com using the community string defined as public:

```
snmp-server enable traps rtr
snmp-server host myhost.cisco.com informs version 2c public rtr
```

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
snmp-server host	Specifies the destination NMS and transfer parameters for SNMP notifications.

Command	Description
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps snmp

To enable SNMP traps, use the **snmp-server enable traps snmp** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps snmp [authentication] [coldstart] [linkdown] [linkup] [warmstart]
no snmp-server enable traps snmp [authentication] [coldstart] [linkdown] [linkup]
[ warmstart]
```

Syntax Description

authentication (Optional) Enables authentication traps.

coldstart (Optional) Enables cold start traps.

linkdown (Optional) Enables linkdown traps.

linkup (Optional) Enables linkup traps.

warmstart (Optional) Enables warmstart traps.

Command Default

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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.



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 enable a warmstart SNMP trap:

```
Device(config)# snmp-server enable traps snmp warmstart
```

Related Topics

[snmp-server host](#)

snmp-server enable traps storm-control

To enable SNMP storm-control trap parameters, use the **snmp-server enable traps storm-control** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps storm-control {trap-rate number-of-minutes}
no snmp-server enable traps storm-control {trap-rate}
```

Syntax Description	trap-rate <i>number-of-minutes</i>	(Optional) Specifies the SNMP storm-control trap rate in minutes. Accepted values are from 0 to 1000.
Command Default	The sending of SNMP storm-control trap parameters is disabled.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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.



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 set the SNMP storm-control trap rate to 10 traps per minute:

```
Device(config)# snmp-server enable traps storm-control trap-rate 10
```

Related Topics

[snmp-server host](#)

snmp-server enable traps stpx

To enable SNMP STPX MIB traps, use the **snmp-server enable traps stpx** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps stpx [inconsistency] [loop-inconsistency] [root-inconsistency]
no snmp-server enable traps stpx [inconsistency] [loop-inconsistency] [root-inconsistency]
```

Syntax Description

inconsistency (Optional) Enables SNMP STPX MIB inconsistency update traps.

loop-inconsistency (Optional) Enables SNMP STPX MIB loop inconsistency update traps.

root-inconsistency (Optional) Enables SNMP STPX MIB root inconsistency update traps.

Command Default

The sending of SNMP STPX MIB traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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.



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 generate SNMP STPX MIB inconsistency update traps:

```
Device(config)# snmp-server enable traps stpx inconsistency
```

Related Topics

[snmp-server host](#)



PART VI

QoS

- [Auto-QoS, on page 333](#)
- [QoS , on page 359](#)



Auto-QoS

This chapter contains the following auto-QoS commands:

- [auto qos classify](#), on page 334
- [auto qos trust](#), on page 337
- [auto qos video](#), on page 341
- [auto qos voip](#), on page 346
- [debug auto qos](#), on page 351
- [show auto qos](#), on page 354

auto qos classify

To automatically configure quality of service (QoS) classification for untrusted devices within a QoS domain, use the **auto qos classify** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

auto qos classify [police]
no auto qos classify [police]

Syntax Description	police (Optional) Configures QoS policing for untrusted devices.				
Command Default	Auto-QoS classify is disabled on the port.				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.				

Usage Guidelines Use this command to configure the QoS for trusted interfaces within the QoS domain. The QoS domain includes the device, the network interior, and edge devices that can classify incoming traffic for QoS.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

Table 18: Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	15 percent	15 percent
SRR shared	2	2, 3, 6,7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	40 percent	40 percent
SRR shared	4	1	20 percent	20 percent	20 percent

Auto-QoS configures the device for connectivity with a trusted interface. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packets is trusted. For routed ports, the DSCP value of the incoming packet is trusted.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

This is the policy map when the **auto qos classify** command is configured:

```
policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
class AUTOQOS_MULTIENTHANCED_CONF_CLASS
set dscp af41
class AUTOQOS_BULK_DATA_CLASS
set dscp af11
class AUTOQOS_TRANSACTION_CLASS
set dscp af21
class AUTOQOS_SCAVANGER_CLASS
set dscp cs1
class AUTOQOS_SIGNALING_CLASS
set dscp cs3
class AUTOQOS_DEFAULT_CLASS
set dscp default
```

This is the policy map when the **auto qos classify police** command is configured:

```
policy-map AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
class AUTOQOS_MULTIENTHANCED_CONF_CLASS
set dscp af41
police 5000000 8000 exceed-action drop
class AUTOQOS_BULK_DATA_CLASS
set dscp af11
police 10000000 8000 exceed-action policed-dscp-transmit
class AUTOQOS_TRANSACTION_CLASS
set dscp af21
police 10000000 8000 exceed-action policed-dscp-transmit
class AUTOQOS_SCAVANGER_CLASS
set dscp cs1
police 10000000 8000 exceed-action drop
class AUTOQOS_SIGNALING_CLASS
set dscp cs3
police 32000 8000 exceed-action drop
class AUTOQOS_DEFAULT_CLASS
set dscp default
police 10000000 8000 exceed-action policed-dscp-transmit
```



Note The device applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the device without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface and apply the new policy map.



Note To disable auto-QoS, you need remove the auto-QoS commands manually.

Enter the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS 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.

To disable auto-QoS on a port, use the **no auto qos trust** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos trust** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

Examples

This example shows how to enable auto-QoS classification of an untrusted device and police traffic:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# auto qos classify police
```

You can verify your settings by entering the **show auto qos interface interface-id** privileged EXEC command.

Related Commands

Command	Description
debug auto qos, on page 351	Enables debugging of the auto-QoS feature.
mls qos trust, on page 388	Configures the port trust state.
queue-set, on page 396	Maps a port to a queue-set.
show auto qos, on page 354	Displays auto-QoS information.
show mls qos interface, on page 403	Displays QoS information at the port level.
srr-queue bandwidth share, on page 416	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

auto qos trust

To automatically configure quality of service (QoS) for trusted interfaces within a QoS domain, use the **auto qos trust** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
auto qos trust {cos | dscp }
no auto qos trust {cos | dscp }
```

Syntax Description

cos Trusts the CoS packet classification.

dscp Trusts the DSCP packet classification.

Command Default

Auto-QoS trust is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues. For more information, see [Table 19: Traffic Types, Packet Labels, and Queues, on page 337](#)

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Use this command to configure the QoS for trusted interfaces within the QoS domain. The QoS domain includes the device, the network interior, and edge devices that can classify incoming traffic for QoS.

Table 19: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP ³ BPDU ⁴ Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP ⁵	46	24, 26	48	56	34	—	
CoS ⁶	5	3	6	7	3	—	
CoS-to-egress queue map	4, 5 (queue 1)	2, 3, 6, 7 (queue 2)			0 (queue 3)	2 (queue 3)	0, 1 (queue 4)

³ STP = Spanning Tree Protocol

⁴ BPDU = bridge protocol data unit

⁵ DSCP = Differentiated Services Code Point

⁶ CoS = class of service

Table 20: Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	15 percent	15 percent
SRR shared	2	2, 3, 6,7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	40 percent	40 percent
SRR shared	4	1	20 percent	20 percent	20 percent

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

This is the auto-QoS generated configuration for the **auto qos trust cos** command:

```

Device config-if)#
Mar 16 02:57:46.351 PST: mls qos map cos-dscp 0 8 16 24 32 46 48 56
Mar 16 02:57:46.351 PST: mls qos
Mar 16 02:57:46.351 PST: no mls qos srr-queue output cos-map
Mar 16 02:57:46.362 PST: no mls qos queue-set output 2 threshold
Mar 16 02:57:46.379 PST: no mls qos queue-set output 2 buffers
Mar 16 02:57:46.382 PST: mls qos srr-queue output cos-map queue 1 threshold 3 4 5
Mar 16 02:57:46.386 PST: mls qos srr-queue output cos-map queue 2 threshold 1 2
Mar 16 02:57:46.393 PST: mls qos srr-queue output cos-map queue 2 threshold 2 3
Mar 16 02:57:46.403 PST: mls qos srr-queue output cos-map queue 2 threshold 3 6 7
Mar 16 02:57:46.407 PST: mls qos srr-queue output cos-map queue 3 threshold 3 0
Mar 16 02:57:46.410 PST: mls qos srr-queue output cos-map queue 4 threshold 3 1
Mar 16 02:57:46.414 PST: no mls qos srr-queue output dscp-map
Mar 16 02:57:46.417 PST: mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40
41 42 43 44 45
Mar 16 02:57:46.417 PST: mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
Mar 16 02:57:46.421 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18
19 20 21 22 23
Mar 16 02:57:46.421 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28
29 30 31 34
Mar 16 02:57:46.424 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 35 36 37
38 39
Mar 16 02:57:46.428 PST: mls qos srr-queue output dscp-map queue 2 threshold 2 24
Mar 16 02:57:46.431 PST: mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50
51 52 53 54 55
Mar 16 02:57:46.442 PST: mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58
59 60 61 62 63
Mar 16 02:57:46.445 PST: mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4
5 6 7
Mar 16 02:57:46.449 PST: mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
Mar 16 02:57:46.452 PST: mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
Mar 16 02:57:46.456 PST: mls qos queue-set output 1 threshold 1 100 100 50 200
Mar 16 02:57:46.463 PST: mls qos queue-set output 1 threshold 2 125 125 100 400
Mar 16 02:57:46.466 PST: mls qos queue-set output 1 threshold 3 100 100 100 400
Mar 16 02:57:46.470 PST: mls qos queue-set output 1 threshold 4 60 150 50 200
Mar 16 02:57:46.473 PST: mls qos queue-set output 1 buffers 15 25 40 20
Mar 16 02:57:46.484 PST: auto qos srnd4
Mar 16 02:57:46.501 PST: mls qos trust cos
Mar 16 02:57:46.505 PST: no queue-set 1

```

```

Mar 16 02:57:46.505 PST:   queue-set 1
Mar 16 02:57:46.508 PST:   priority-queue out
Mar 16 02:57:46.512 PST:   srr-queue bandwidth share 1 30 35 5

```

This is the auto-QoS generated configuration for the **auto qos trust dscp** command:

```

Device (config-if)#
switch1(config-if)#
Mar 16 02:58:40.430 PST: mls qos map cos-dscp 0 8 16 24 32 46 48 56
Mar 16 02:58:40.433 PST: mls qos
Mar 16 02:58:40.433 PST: no mls qos srr-queue output cos-map
Mar 16 02:58:40.444 PST: no mls qos queue-set output 2 threshold
Mar 16 02:58:40.458 PST: no mls qos queue-set output 2 buffers
Mar 16 02:58:40.461 PST: mls qos srr-queue output cos-map queue 1 threshold 3 4 5
Mar 16 02:58:40.465 PST: mls qos srr-queue output cos-map queue 2 threshold 1 2
Mar 16 02:58:40.468 PST: mls qos srr-queue output cos-map queue 2 threshold 2 3
Mar 16 02:58:40.472 PST: mls qos srr-queue output cos-map queue 2 threshold 3 6 7
Mar 16 02:58:40.482 PST: mls qos srr-queue output cos-map queue 3 threshold 3 0
Mar 16 02:58:40.486 PST: mls qos srr-queue output cos-map queue 4 threshold 3 1
Mar 16 02:58:40.489 PST: no mls qos srr-queue output dscp-map
Mar 16 02:58:40.496 PST: mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40
41 42 43 44 45
Mar 16 02:58:40.496 PST: mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
Mar 16 02:58:40.500 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18
19 20 21 22 23
Mar 16 02:58:40.503 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28
29 30 31 34
Mar 16 02:58:40.503 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 35 36 37
38 39
Mar 16 02:58:40.506 PST: mls qos srr-queue output dscp-map queue 2 threshold 2 24
Mar 16 02:58:40.510 PST: mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50
51 52 53 54 55
Mar 16 02:58:40.513 PST: mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58
59 60 61 62 63
Mar 16 02:58:40.524 PST: mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4
5 6 7
Mar 16 02:58:40.527 PST: mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
Mar 16 02:58:40.531 PST: mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
Mar 16 02:58:40.538 PST: mls qos queue-set output 1 threshold 1 100 100 50 200
Mar 16 02:58:40.541 PST: mls qos queue-set output 1 threshold 2 125 125 100 400
Mar 16 02:58:40.545 PST: mls qos queue-set output 1 threshold 3 100 100 100 400
Mar 16 02:58:40.548 PST: mls qos queue-set output 1 threshold 4 60 150 50 200
Mar 16 02:58:40.562 PST: mls qos queue-set output 1 buffers 15 25 40 20
Mar 16 02:58:40.566 PST: auto qos srnd4
Mar 16 02:58:40.583 PST:   mls qos trust dscp
Mar 16 02:58:40.590 PST:   no queue-set 1
Mar 16 02:58:40.590 PST:   queue-set 1
Mar 16 02:58:40.590 PST:   priority-queue out
Mar 16 02:58:40.601 PST:   srr-queue bandwidth share 1 30 35 5

```



Note The device applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the device without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface and apply the new policy map.



Note To disable auto-QoS, you need to remove the auto-QoS commands manually.

Enter the **no mls qos** global configuration command. With QoS 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).

To disable auto-QoS on a port, use the **no auto qos trust** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos trust** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

Examples

This example shows how to enable auto-QoS for a trusted interface with specific CoS classification:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# auto qos trust cos
```

You can verify your settings by entering the **show auto qos interface interface-id** privileged EXEC command.

Related Commands

Command	Description
debug auto qos, on page 351	Enables debugging of the auto-QoS feature.
mls qos trust, on page 388	Configures the port trust state.
queue-set, on page 396	Maps a port to a queue-set.
show auto qos, on page 354	Displays auto-QoS information.
srr-queue bandwidth share, on page 416	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.
srr-queue bandwidth share, on page 416	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

auto qos video

To automatically configure quality of service (QoS) for video within a QoS domain, use the **auto qos video** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

```
auto qos video {cts | ip-camera | media-player}
no auto qos video {cts | ip-camera | media-player}
```

Syntax Description

cts	Identifies this port as connected to a Cisco TelePresence System and automatically configures QoS for video.
ip-camera	Identifies this port as connected to a Cisco IP camera and automatically configures QoS for video.
media-player	Identifies this port as connected to a CDP-capable Cisco digital media player and automatically configures QoS for video.

Command Default

Auto-QoS video is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

Use this command to configure the QoS appropriate for video traffic within the QoS domain. The QoS domain includes the device, the network interior, and edge devices that can classify incoming traffic for QoS.

Table 21: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP ⁷ BPDUs ⁸ Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP ⁹	46	24, 26	48	56	34	–	
CoS ¹⁰	5	3	6	7	3	–	
CoS-to-egress queue map	4, 5 (queue 1)	2, 3, 6, 7 (queue 2)	2, 3, 6, 7 (queue 2)	2, 3, 6, 7 (queue 2)	0 (queue 3)	2 (queue 3)	0, 1 (queue 4)

⁷ STP = Spanning Tree Protocol

⁸ BPDUs = bridge protocol data unit

⁹ DSCP = Differentiated Services Code Point

¹⁰ CoS = class of service

Table 22: Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	15 percent	15 percent
SRR shared	2	2, 3, 6, 7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	40 percent	40 percent
SRR shared	4	1	20 percent	20 percent	20 percent

Auto-QoS configures the device for video connectivity to a Cisco TelePresence system, a Cisco IP camera, or a Cisco digital media player.

To take advantage of the auto-QoS defaults, enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration after you enable auto-QoS.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

This is the QoS configuration that is automatically generated for the **auto qos video cts** command:

```
Device(config-if)# auto qos video cts

Mar 16 02:54:17.286 PST: mls qos map cos-dscp 0 8 16 24 32 46 48 56
Mar 16 02:54:17.296 PST: mls qos
Mar 16 02:54:17.296 PST: no mls qos srr-queue output cos-map
Mar 16 02:54:17.300 PST: no mls qos queue-set output 2 threshold
Mar 16 02:54:17.324 PST: no mls qos queue-set output 2 buffers
Mar 16 02:54:17.328 PST: mls qos srr-queue output cos-map queue 1 threshold 3 4 5
Mar 16 02:54:17.331 PST: mls qos srr-queue output cos-map queue 2 threshold 1 2
Mar 16 02:54:17.331 PST: mls qos srr-queue output cos-map queue 2 threshold 2 3
Mar 16 02:54:17.338 PST: mls qos srr-queue output cos-map queue 2 threshold 3 6 7
Mar 16 02:54:17.338 PST: mls qos srr-queue output cos-map queue 3 threshold 3 0
Mar 16 02:54:17.342 PST: mls qos srr-queue output cos-map queue 4 threshold 3 1
Mar 16 02:54:17.345 PST: no mls qos srr-queue output dscp-map
Mar 16 02:54:17.349 PST: mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40
41 42 43 44 45
Mar 16 02:54:17.363 PST: mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
Mar 16 02:54:17.366 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18
19 20 21 22 23
Mar 16 02:54:17.370 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28
29 30 31 34
Mar 16 02:54:17.373 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 35 36 37
38 39
Mar 16 02:54:17.380 PST: mls qos srr-queue output dscp-map queue 2 threshold 2 24
Mar 16 02:54:17.384 PST: mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50
51 52 53 54 55
Mar 16 02:54:17.387 PST: mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58
59 60 61 62 63
Mar 16 02:54:17.391 PST: mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4
5 6 7
Mar 16 02:54:17.401 PST: mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
Mar 16 02:54:17.405 PST: mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
```



```

Mar 16 02:54:17.408 PST: mls qos queue-set output 1 threshold 1 100 100 50 200
Mar 16 02:54:17.415 PST: mls qos queue-set output 1 threshold 2 125 125 100 400
Mar 16 02:54:17.419 PST: mls qos queue-set output 1 threshold 3 100 100 100 400
Mar 16 02:54:17.422 PST: mls qos queue-set output 1 threshold 4 60 150 50 200
Mar 16 02:54:17.426 PST: mls qos queue-set output 1 buffers 15 25 40 20
Mar 16 02:54:17.433 PST: auto qos srnd4
Mar 16 02:54:17.454 PST: mls qos trust device cts
Mar 16 02:54:17.457 PST: mls qos trust dscp
Mar 16 02:54:17.464 PST: no queue-set 1
Mar 16 02:54:17.464 PST: queue-set 1
Mar 16 02:54:17.468 PST: priority-queue out
Mar 16 02:54:17.482 PST: srr-queue bandwidth share 1 30 35 5

```

This is the QoS configuration that is automatically generated for the **auto qos video ip-camera** command:

```

Device(config-if)# auto qos video ip-camera
Mar 16 02:55:43.675 PST: mls qos map cos-dscp 0 8 16 24 32 46 48 56
Mar 16 02:55:43.685 PST: mls qos
Mar 16 02:55:43.685 PST: no mls qos srr-queue output cos-map
Mar 16 02:55:43.689 PST: no mls qos queue-set output 2 threshold
Mar 16 02:55:43.703 PST: no mls qos queue-set output 2 buffers
Mar 16 02:55:43.706 PST: mls qos srr-queue output cos-map queue 1 threshold 3 4 5
Mar 16 02:55:43.710 PST: mls qos srr-queue output cos-map queue 2 threshold 1 2
Mar 16 02:55:43.710 PST: mls qos srr-queue output cos-map queue 2 threshold 2 3
Mar 16 02:55:43.724 PST: mls qos srr-queue output cos-map queue 2 threshold 3 6 7
Mar 16 02:55:43.727 PST: mls qos srr-queue output cos-map queue 3 threshold 3 0
Mar 16 02:55:43.731 PST: mls qos srr-queue output cos-map queue 4 threshold 3 1
Mar 16 02:55:43.734 PST: no mls qos srr-queue output dscp-map
Mar 16 02:55:43.741 PST: mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40
41 42 43 44 45
Mar 16 02:55:43.745 PST: mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
Mar 16 02:55:43.748 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18
19 20 21 22 23
Mar 16 02:55:43.762 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28
29 30 31 34
Mar 16 02:55:43.766 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 35 36 37
38 39
Mar 16 02:55:43.769 PST: mls qos srr-queue output dscp-map queue 2 threshold 2 24
Mar 16 02:55:43.773 PST: mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50
51 52 53 54 55
Mar 16 02:55:43.780 PST: mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58
59 60 61 62 63
Mar 16 02:55:43.783 PST: mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4
5 6 7
Mar 16 02:55:43.786 PST: mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
Mar 16 02:55:43.790 PST: mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
Mar 16 02:55:43.793 PST: mls qos queue-set output 1 threshold 1 100 100 50 200
Mar 16 02:55:43.804 PST: mls qos queue-set output 1 threshold 2 125 125 100 400
Mar 16 02:55:43.807 PST: mls qos queue-set output 1 threshold 3 100 100 100 400
Mar 16 02:55:43.811 PST: mls qos queue-set output 1 threshold 4 60 150 50 200
Mar 16 02:55:43.814 PST: mls qos queue-set output 1 buffers 15 25 40 20
Mar 16 02:55:43.818 PST: auto qos srnd4
Mar 16 02:55:43.832 PST: mls qos trust device ip-camera
Mar 16 02:55:43.842 PST: mls qos trust dscp
Mar 16 02:55:43.849 PST: no queue-set 1
Mar 16 02:55:43.849 PST: queue-set 1
Mar 16 02:55:43.849 PST: priority-queue out
Mar 16 02:55:43.853 PST: srr-queue bandwidth share 1 30 35 5

```

This is the QoS configuration that is automatically generated for the **auto qos video media-player** command:

```

Device(config-if)# auto qos video media-player
Mar 16 02:56:39.969 PST: mls qos map cos-dscp 0 8 16 24 32 46 48 56
Mar 16 02:56:39.980 PST: mls qos
Mar 16 02:56:39.980 PST: no mls qos srr-queue output cos-map
Mar 16 02:56:39.987 PST: no mls qos queue-set output 2 threshold
Mar 16 02:56:40.011 PST: no mls qos queue-set output 2 buffers
Mar 16 02:56:40.011 PST: mls qos srr-queue output cos-map queue 1 threshold 3 4 5
Mar 16 02:56:40.015 PST: mls qos srr-queue output cos-map queue 2 threshold 1 2
Mar 16 02:56:40.018 PST: mls qos srr-queue output cos-map queue 2 threshold 2 3
Mar 16 02:56:40.018 PST: mls qos srr-queue output cos-map queue 2 threshold 3 6 7
Mar 16 02:56:40.022 PST: mls qos srr-queue output cos-map queue 3 threshold 3 0
Mar 16 02:56:40.022 PST: mls qos srr-queue output cos-map queue 4 threshold 3 1
Mar 16 02:56:40.029 PST: no mls qos srr-queue output dscp-map
Mar 16 02:56:40.029 PST: mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40
41 42 43 44 45
Mar 16 02:56:40.043 PST: mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
Mar 16 02:56:40.046 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18
19 20 21 22 23
Mar 16 02:56:40.050 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28
29 30 31 34
Mar 16 02:56:40.053 PST: mls qos srr-queue output dscp-map queue 2 threshold 1 35 36 37
38 39
Mar 16 02:56:40.057 PST: mls qos srr-queue output dscp-map queue 2 threshold 2 24
Mar 16 02:56:40.064 PST: mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50
51 52 53 54 55
Mar 16 02:56:40.067 PST: mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58
59 60 61 62 63
Mar 16 02:56:40.071 PST: mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4
5 6 7
Mar 16 02:56:40.081 PST: mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
Mar 16 02:56:40.085 PST: mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
Mar 16 02:56:40.092 PST: mls qos queue-set output 1 threshold 1 100 100 50 200
Mar 16 02:56:40.095 PST: mls qos queue-set output 1 threshold 2 125 125 100 400
Mar 16 02:56:40.099 PST: mls qos queue-set output 1 threshold 3 100 100 100 400
Mar 16 02:56:40.102 PST: mls qos queue-set output 1 threshold 4 60 150 50 200
Mar 16 02:56:40.106 PST: mls qos queue-set output 1 buffers 15 25 40 20
Mar 16 02:56:40.109 PST: auto qos srnd4
Mar 16 02:56:40.130 PST: mls qos trust device media-player
Mar 16 02:56:40.133 PST: mls qos trust dscp
Mar 16 02:56:40.137 PST: no queue-set 1
Mar 16 02:56:40.137 PST: queue-set 1
Mar 16 02:56:40.140 PST: priority-queue out
Mar 16 02:56:40.172 PST: srr-queue bandwidth share 1 30 35 5

```

**Note**

The device applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the device without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

When you enable the auto-QoS feature on the first port, QoS is globally enabled (**mls qos** global configuration command), and other global configuration commands are added.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.



Note To disable auto-QoS, you need to remove the auto-QoS commands manually.

Enter the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS 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).

To disable auto-QoS on a port, use the **no auto qos video** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos video** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

Examples

This example shows how to enable auto-QoS for a Cisco Telepresence interface with conditional trust. The interface is trusted only if a Cisco Telepresence device is detected; otherwise, the port is untrusted.

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# auto qos video cts
```

You can verify your settings by entering the **show auto qos video interface interface-id** privileged EXEC command.

Related Commands

Command	Description
debug auto qos, on page 351	Enables debugging of the auto-QoS feature.
mls qos trust, on page 388	Configures the port trust state.
queue-set, on page 396	Maps a port to a queue-set.
show auto qos, on page 354	Displays auto-QoS information.
show mls qos interface, on page 403	Displays QoS information at the port level.
srr-queue bandwidth share, on page 416	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

auto qos voip

To automatically configure quality of service (QoS) for voice over IP (VoIP) within a QoS domain, use the **auto qos voip** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

```
auto qos voip {cisco-phone | cisco-softphone | trust}
no auto qos voip {cisco-phone | cisco-softphone | trust}
```

Syntax Description

cisco-phone	Identifies this port as connected to a Cisco IP Phone, and automatically configures QoS for VoIP. The QoS labels of incoming packets are trusted only when the telephone is detected.
cisco-softphone	Identifies this port as connected to a device running the Cisco SoftPhone, and automatically configures QoS for VoIP.
trust	Identifies this port as connected to a trusted device, and automatically configures QoS for VoIP. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packet is trusted. For routed ports, the DSCP value of the incoming packet is trusted.

Command Default

Auto-QoS is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, assign packet labels, and configure the ingress and egress queues. For more information, see [Table 23: Traffic Types, Packet Labels, and Queues, on page 346](#)

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

Use this command to configure the QoS appropriate for VoIP traffic within the QoS domain. The QoS domain includes the device, the network interior, and edge devices that can classify incoming traffic for QoS.

Auto-QoS configures the device for VoIP with Cisco IP Phones on device and routed ports and for VoIP with devices running the Cisco SoftPhone application. These releases support only Cisco IP SoftPhone Version 1.3(3) or later. Connected devices must use Cisco Call Manager Version 4 or later.

To take advantage of the auto-QoS defaults, enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration after you enable auto-QoS.

Table 23: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP ¹¹ BPDU ¹² Traffic	Real-Time Video Traffic	All Other Traffic
DSCP ¹³	46	24, 26	48	56	34	–

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP ¹¹ BPDUs ¹² Traffic	Real-Time Video Traffic	All Other Traffic	
CoS ¹⁴	5	3	6	7	3	–	
CoS-to-egress queue map	4, 5 (queue 1)	2, 3, 6, 7 (queue 2)	2, 3, 6, 7 (queue 2)	2, 3, 6, 7 (queue 2)	0 (queue 3)	2 (queue 3)	0, 1 (queue 4)

¹¹ STP = Spanning Tree Protocol

¹² BPDUs = bridge protocol data unit

¹³ DSCP = Differentiated Services Code Point

¹⁴ CoS = class of service

The device configures egress queues on the port according to the settings in this table.

Table 24: Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	15 percent	15 percent
SRR shared	2	2, 3, 6, 7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	40 percent	40 percent
SRR shared	4	1	20 percent	20 percent	20 percent



Note

The device applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the device without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

When you enable the auto-QoS feature on the first port, these automatic actions occur:

- QoS is globally enabled (**mls qos** global configuration command), and other global configuration commands are added.
- When you enter the **auto qos voip cisco-phone** interface configuration command on a port at the edge of the network that is connected to a Cisco IP Phone, the device enables the trusted boundary feature. The device uses the Cisco Discovery Protocol (CDP) to detect the presence of a Cisco IP Phone. When a Cisco IP Phone is detected, the ingress classification on the port is set to trust the QoS label received

in the packet. The device also uses policing to determine whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the device changes the DSCP value to 0. When a Cisco IP Phone is absent, the ingress classification is set to not trust the QoS label in the packet. The policing is applied to the traffic that matches the policy-map classification before the device enables the trust boundary feature.

- When you enter the **auto qos voip cisco-softphone** interface configuration command on a port at the edge of the network that is connected to a device running the Cisco SoftPhone, the device uses policing to decide whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the device changes the DSCP value to 0.
- When you enter the **auto qos voip trust** interface configuration command on a port connected to the network interior, the device trusts the CoS value for nonrouted ports or the DSCP value for routed ports in ingress packets (the assumption is that traffic has already been classified by other edge devices).

You can enable auto-QoS on static, dynamic-access, and voice VLAN access, and trunk ports. When enabling auto-QoS with a Cisco IP Phone on a routed port, you must assign a static IP address to the IP phone.



Note When a device running Cisco SoftPhone is connected to a device or routed port, the device supports only one Cisco SoftPhone application per port.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.



Note To disable auto-QoS, you need to remove the auto-QoS commands manually.

Enter the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS 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.

To disable auto-QoS on a port, use the **no auto qos voip** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos voip** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

This is the enhanced configuration for the **auto qos voip cisco-phone** command:

```
Device(config)# mls qos map policed-dscp 0 10 18 to 8
Device(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Device(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Device(config-cmap)# match ip dscp ef
Device(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
```

```

Device(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Device(config-cmap)# match ip dscp cs3
Device(config)# policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
Device(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Device(config-pmap-c)# set dscp ef
Device(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Device(config-pmap-c)# set dscp cs3
Device(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Device(config-pmap-c)# set dscp default
Device(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
Device(config-if)# service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY

```

This is the enhanced configuration for the `auto qos voip cisco-softphone` command:

```

Device(config)# mls qos map policed-dscp 0 10 18 to 8
Device(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Device(config)# class-map match-all AUTOQOS_MULTIHANCED_CONF_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-MULTIHANCED-CONF
Device(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Device(config-cmap)# match ip dscp ef
Device(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Device(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Device(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Device(config-cmap)# match ip dscp cs3
Device(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Device(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Device(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Device(config)# policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
Device(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Device(config-pmap-c)# set dscp ef
Device(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Device(config-pmap-c)# set dscp cs3
Device(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AUTOQOS_MULTIHANCED_CONF_CLASS
Device(config-pmap-c)# set dscp af41
Device(config-pmap-c)# police 5000000 8000 exceed-action drop
Device(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Device(config-pmap-c)# set dscp af11
Device(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Device(config-pmap-c)# set dscp af21
Device(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Device(config-pmap-c)# set dscp cs1
Device(config-pmap-c)# police 1000000 8000 exceed-action drop
Device(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Device(config-pmap-c)# set dscp cs3
Device(config-pmap-c)# police 32000 8000 exceed-action drop
Device(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Device(config-pmap-c)# set dscp default
Device(config-if)# service-policy input AUTOQOS-SRND4-SOFTPHONE-POLICY

```

Examples

This example shows how to enable auto-QoS and to trust the QoS labels received in incoming packets when the device or router connected to the port is a trusted device:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# auto qos voip trust
```

You can verify your settings by entering the **show auto qos interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
debug auto qos, on page 351	Enables debugging of the auto-QoS feature.
mls qos cos, on page 372	Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port.
mls qos map, on page 376	Defines the CoS-to-DSCP map or the DSCP-to-CoS map.
mls qos queue-set output buffers, on page 377	Allocates buffers to a queue-set.
mls qos srr-queue output cos-map, on page 384	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map, on page 386	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos trust, on page 388	Configures the port trust state.
queue-set, on page 396	Maps a port to a queue-set.
show auto qos, on page 354	Displays auto-QoS information.
show mls qos interface, on page 403	Displays QoS information at the port level.
srr-queue bandwidth shape, on page 414	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
srr-queue bandwidth share, on page 416	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

debug auto qos

To enable debugging of the automatic quality of service (auto-QoS) feature, use the **debug auto qos** command in privileged EXEC mode. Use the **no** form of this command to disable debugging.

debug auto qos
no debug auto qos

Syntax Description	This command has no arguments or keywords.	
Command Default	Auto-QoS debugging is disabled.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. You enable debugging by entering the **debug auto qos** privileged EXEC command.

The **undebug auto qos** command is the same as the **no debug auto qos** command.

When you enable debugging on a device stack, it is enabled only on the active device. To enable debugging on a stack member, you can start a session from the active device by using the **session switch-number** privileged EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command stack-member-number LINE** privileged EXEC command on the active device to enable debugging on a member device without first starting a session.

Examples

This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled:

```
Device# debug auto qos
Auto QoS debugging is on

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface gigabitethernet1/0/1
Device(config-if)#auto qos voip cisco-softphone
May 31 09:03:32.293: no policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
May 31 09:03:32.296: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-SOFTPHONE-POLICY `
May 31 09:03:32.296: no policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
May 31 09:03:32.300: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-CISCOPHONE-POLICY `
May 31 09:03:32.300: no policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
May 31 09:03:32.300: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-CLASSIFY-POLICY `
May 31 09:03:32.303: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY `
May 31 09:03:32.303: no class-map match-all AUTOQOS_DEFAULT_CLASS
May 31 09:03:32.307: no class-map match-all AUTOQOS_MULTIENTHANCED_CONF_CLASS
```

```

May 31 09:03:32.310: no class-map match-all AUTOQOS_TRANSACTION_CLASS
May 31 09:03:32.310: no class-map match-all AUTOQOS_BULK_DATA_CLASS
May 31 09:03:32.314: no class-map match-all AUTOQOS_SCAVANGER_CLASS
May 31 09:03:32.317: no class-map match-all AUTOQOS_SIGNALING_CLASS
May 31 09:03:32.321: no class-map match-all AUTOQOS_VOIP_DATA_CLASS
May 31 09:03:32.324: no class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
May 31 09:03:32.324: no ip access-list extended AUTOQOS-ACL-DEFAULT
May 31 09:03:32.328: no ip access-list extended AUTOQOS-ACL-BULK-DATA
May 31 09:03:32.331: no ip access-list extended AUTOQOS-ACL-SCAVANGER
May 31 09:03:32.335: no ip access-list extended AUTOQOS-ACL-TRANSACTIONAL-DATA
May 31 09:03:32.338: no ip access-list extended AUTOQOS-ACL-SIGNALING
May 31 09:03:32.415: no ip access-list extended AUTOQOS-ACL-MULTIENHANCED-CONF
May 31 09:03:32.419: mls qos map cos-dscp 0 8 16 24 32 46 48 56
May 31 09:03:32.426: mls qos
May 31 09:03:32.426: no mls qos srr-queue output cos-map
May 31 09:03:32.429: no mls qos map policed-dscp
May 31 09:03:32.446: mls qos srr-queue output cos-map queue 1 threshold 3 5
May 31 09:03:32.450: mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
May 31 09:03:32.527: mls qos srr-queue output cos-map queue 3 threshold 3 2 4
May 31 09:03:32.530: mls qos srr-queue output cos-map queue 4 threshold 2 1
May 31 09:03:32.530: mls qos srr-queue output cos-map queue 4 threshold 3 0
May 31 09:03:32.537: no mls qos srr-queue output dscp-map
May 31 09:03:32.541: mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44
45 46 47
May 31 09:03:32.544: mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28
29 30 31
May 31 09:03:32.544: mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52
53 54 55
May 31 09:03:32.544: mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60
61 62 63
May 31 09:03:32.548: mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20
21 22 23
May 31 09:03:32.548: mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36
37 38 39
May 31 09:03:32.621: mls qos srr-queue output dscp-map queue 4 threshold 1 8
May 31 09:03:32.628: mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13
14 15
May 31 09:03:32.751: mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6
7
May 31 09:03:32.761: mls qos queue-set output 1 threshold 1 138 138 92 138
May 31 09:03:32.779: mls qos queue-set output 1 threshold 2 138 138 92 400
May 31 09:03:32.779: mls qos queue-set output 1 threshold 3 36 77 100 318
May 31 09:03:32.782: mls qos queue-set output 1 threshold 4 20 50 67 400
May 31 09:03:32.859: mls qos queue-set output 1 buffers 10 10 26 54
May 31 09:03:33.488: no policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
May 31 09:03:33.492: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-SOFTPHONE-POLICY '
May 31 09:03:33.492: no policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
May 31 09:03:33.495: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-CISCOPHONE-POLICY '
May 31 09:03:33.495: no policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
May 31 09:03:33.495: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-CLASSIFY-POLICY '
May 31 09:03:33.495: no policy-map AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
May 31 09:03:33.499: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY '
May 31 09:03:33.499: no class-map match-all AUTOQOS_DEFAULT_CLASS
May 31 09:03:33.499: no class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
May 31 09:03:33.499: no class-map match-all AUTOQOS_TRANSACTION_CLASS
May 31 09:03:33.502: no class-map match-all AUTOQOS_BULK_DATA_CLASS
May 31 09:03:33.502: no class-map match-all AUTOQOS_SCAVANGER_CLASS
May 31 09:03:33.502: no class-map match-all AUTOQOS_SIGNALING_CLASS
May 31 09:03:33.502: no class-map match-all AUTOQOS_VOIP_DATA_CLASS
May 31 09:03:33.502: no class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS

```

```

May 31 09:03:33.502: no ip access-list extended AUTOQOS-ACL-DEFAULT
May 31 09:03:33.506: no ip access-list extended AUTOQOS-ACL-BULK-DATA
May 31 09:03:33.509: no ip access-list extended AUTOQOS-ACL-SCAVANGER
May 31 09:03:33.513: no ip access-list extended AUTOQOS-ACL-TRANSACTIONAL-DATA
May 31 09:03:33.516: no ip access-list extended AUTOQOS-ACL-SIGNALING
May 31 09:03:33.520: no ip access-list extended AUTOQOS-ACL-MULTIENHANCED-CONF
May 31 09:03:33.523: no mls qos map cos-dscp
May 31 09:03:33.544: no mls qos
May 31 09:03:33.638: no mls qos srr-queue output cos-map
May 31 09:03:33.642: no mls qos map policed-dscp
May 31 09:03:33.642: no mls qos srr-queue output dscp-map
May 31 09:03:33.656: no mls qos queue-set output 1 threshold 1
May 31 09:03:33.659: no mls qos queue-set output 1 threshold 2
May 31 09:03:33.663: no mls qos queue-set output 1 threshold 3
May 31 09:03:33.663: no mls qos queue-set output 1 threshold 4
May 31 09:03:33.663: no mls qos queue-set output 1 buffers
May 31 09:03:33.782: no mls qos queue-set output 2 threshold 1
May 31 09:03:33.785: no mls qos queue-set output 2 threshold 2
May 31 09:03:33.785: no mls qos queue-set output 2 threshold 3
May 31 09:03:33.785: no mls qos queue-set output 2 threshold 4
May 31 09:03:33.789: no mls qos queue-set output 2 buffers
May 31 09:03:33.789: mls qos srr-queue output queues 8
May 31 09:03:33.792: mls qos

```

Related Commands

Command	Description
show auto qos, on page 354	Displays the initial configuration that is generated by the auto-QoS feature.
show debugging	Displays information about the types of debugging that are enabled.

show auto qos

To display the quality of service (QoS) commands entered on the interfaces on which auto-QoS is enabled, use the **show auto qos** command in privileged EXEC mode.

show auto qos [**interface** *[interface-id]*]

Syntax Description	interface <i>[interface-id]</i>	(Optional) Displays auto-QoS information for the specified port or for all ports. Valid interfaces include physical ports.
Command Modes	User EXEC Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.
Usage Guidelines	<p>The show auto qos command output shows only the auto qos command entered on each interface. The show auto qos interface interface-id command output shows the auto qos command entered on a specific interface.</p> <p>Use the show running-config privileged EXEC command to display the auto-QoS configuration and the user modifications.</p> <p>The show auto qos command output shows the service policy information for the Cisco IP phone.</p> <p>To display information about the QoS configuration that might be affected by auto-QoS, use one of these commands:</p> <ul style="list-style-type: none"> • show mls qos • show mls qos maps cos-dscp • show mls qos interface [interface-id] [buffers queueing] • show mls qos maps [cos-dscp cos-input-q cos-output-q dscp-cos dscp-input-q dscp-output-q] • show mls qos input-queue • show running-config 	

Examples

This is an example of output from the **show auto qos** command after the **auto qos voip cisco-phone** and the **auto qos voip cisco-softphone** interface configuration commands are entered:

```
Device# show auto qos
GigabitEthernet2/0/4
auto qos voip cisco-softphone

GigabitEthernet2/0/5
auto qos voip cisco-phone
```

```
GigabitEthernet2/0/6
auto qos voip cisco-phone
```

This is an example of output from the **show auto qos interface *interface-id*** command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Device# show auto qos interface gigabitethernet 2/0/5
GigabitEthernet2/0/5
auto qos voip cisco-phone
```

This is an example of output from the **show running-config** privileged EXEC command when the **auto qos voip cisco-phone** and the **auto qos voip cisco-softphone** interface configuration commands are entered:

```
Device# show running-config
Building configuration...
...
mls qos map policed-dscp 0 10 18 24 46 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
...
!
spanning-tree mode pvst
spanning-tree extend system-id
!
network-policy profile 1
!
vlan access-map vmap4 10
  action forward
!
vlan internal allocation policy ascending
!
class-map match-all paul
class-map match-all cm-1
  match ip dscp af11
class-map match-all AUTOQOS_VOIP_DATA_CLASS
  match ip dscp ef
class-map match-all AUTOQOS_DEFAULT_CLASS
```

```

    match access-group name AUTOQOS-ACL-DEFAULT
class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
    match ip dscp cs3
class-map match-all ftp_class
!
policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
    class AUTOQOS_VOIP_DATA_CLASS
        set dscp ef
        police 128000 8000 exceed-action policed-dscp-transmit
    class AUTOQOS_VOIP_SIGNAL_CLASS
        set dscp cs3
        police 32000 8000 exceed-action policed-dscp-transmit
    class AUTOQOS_DEFAULT_CLASS
        set dscp default
        police 10000000 8000 exceed-action policed-dscp-transmit
policy-map policy_ftp
    class ftp_class
!!
interface FastEthernet0
    no ip address
!
interface GigabitEthernet1/0/1
    srr-queue bandwidth share 1 30 35 5
    priority-queue out
    mls qos trust cos
    auto qos trust
!
interface GigabitEthernet1/0/2
    srr-queue bandwidth share 1 30 35 5
    priority-queue out
    mls qos trust device cisco-phone
    mls qos trust cos
    auto qos voip cisco-phone
    service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
!
<output truncated>

```

These are examples of output from the **show auto qos interface** command:

```

Device# show auto qos interface

!
interface GigabitEthernet2/0/4
    switchport mode access
    switchport port-security maximum 400
    service-policy input AutoQoS-Police-SoftPhone
    speed 100
    duplex half
    srr-queue bandwidth share 10 10 60 20
    priority-queue out
    auto qos voip cisco-softphone
!
interface GigabitEthernet2/0/5
    switchport mode access
    switchport port-security maximum 1999
    speed 100
    duplex full
    srr-queue bandwidth share 10 10 60 20
    priority-queue out
    mls qos trust device cisco-phone
    mls qos trust cos
    auto qos voip cisco-phone

```

```

!
interface GigabitEthernet2/0/6
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 2
 switchport mode access
 speed 10
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
interface GigabitEthernet4/0/1
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 mls qos trust device cisco-phone
 service-policy input AutoQoS-Police-CiscoPhone

```

These are examples of output from the **show auto qos interface *interface-id*** command when auto-QoS is disabled on an interface:

```

Device# show auto qos interface gigabitethernet3/0/1
AutoQoS is disabled

```

Related Commands

Command	Description
debug auto qos, on page 351	Enables debugging of the auto-QoS feature.



QoS

This chapter contains the following QoS commands:

- [class](#), on page 360
- [class-map](#), on page 362
- [debug qos](#), on page 364
- [match \(class-map configuration\)](#), on page 366
- [mls qos](#), on page 368
- [mls qos aggregate-policer](#), on page 370
- [mls qos cos](#), on page 372
- [mls qos dscp-mutation](#), on page 374
- [mls qos map](#), on page 376
- [mls qos queue-set output buffers](#), on page 377
- [mls qos queue-set output threshold](#), on page 379
- [mls qos rewrite ip dscp](#), on page 382
- [mls qos srr-queue output cos-map](#), on page 384
- [mls qos srr-queue output dscp-map](#), on page 386
- [mls qos trust](#), on page 388
- [police](#), on page 390
- [police aggregate](#), on page 392
- [policy map](#), on page 394
- [queue-set](#), on page 396
- [service-policy](#), on page 397
- [set](#), on page 398
- [show class-map](#), on page 400
- [show mls qos](#), on page 401
- [show mls qos aggregate-policer](#), on page 402
- [show mls qos interface](#), on page 403
- [show mls qos maps](#), on page 407
- [show mls qos queue-set](#), on page 410
- [show policy-map](#), on page 411
- [srr-queue bandwidth limit](#), on page 412
- [srr-queue bandwidth shape](#), on page 414
- [srr-queue bandwidth share](#), on page 416
- [trust](#), on page 418

class

To define a traffic classification match criteria for the specified class-map name, use the **class** command in policy-map configuration mode. Use the **no** form of this command to delete an existing class map.

```
class {class-map-name | class-default}
no class {class-map-name | class-default}
```

Syntax Description

class-map-name Assigns a name to the class map.

class-default Refers to a system default class that matches unclassified packets.

Command Default

No policy map class-maps are defined.

Command Modes

Policy-map configuration

Command History

Release

Modification

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

Before using the **class** command, you must use the **policy-map** global configuration command to identify the policy map and enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter policy-map class configuration mode. These configuration commands are available:

- **exit**—Exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no**—Returns a command to its default setting.
- **police**—Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information, see [police, on page 390](#) and [police aggregate, on page 392](#).
- **set**—Specifies a value to be assigned to the classified traffic. For more information, see [set, on page 398](#).
- **trust**—Defines a trust state for traffic classified with the **class** or the **class-map** command. For more information, see [trust, on page 418](#).

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

The **class** command performs the same function as the **class-map** global configuration command. Use the **class** command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.

You can configure a default class by using the **class class-default** policy-map configuration command. Unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as default traffic.

Examples

This example shows how to configure a default traffic class to a policy map:

```

Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# match protocol ipv6
Device(config-cmap)# exit
Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# match protocol ip
Device(config-cmap)# exit
Device(config)# policy-map pm3
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit
Device(config-pmap)# class cm-3
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit
Device(config-pmap)# class cm-4
Device(config-pmap-c)# trust cos
Device(config-pmap-c)# exit
Device(config-pmap)# exit

```

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

This example shows how the default traffic class is automatically placed at the end of policy-map pm3 even though **class-default** was configured first:

```

Device# show policy-map pm3
  Policy Map pm3
    Class cm-3
      set dscp 4
    Class cm-4
      trust cos
    Class class-default
      set dscp 10
Device#

```

Related Commands

Command	Description
class-map, on page 362	Creates a class map to be used for matching packets to the class whose name you specify.
police, on page 390	Defines a policer for classified traffic.
policy map, on page 394	Defines a policer for classified traffic.
set, on page 398	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
show policy-map, on page 411	Displays quality of service (QoS) policy maps.
trust, on page 418	Defines a trust state for the traffic classified through the class policy-map configuration command or the class-map global configuration command.

class-map

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 **class-map** command in global configuration mode. Use the **no** form of this command to delete an existing class map and to return to global or policy map configuration mode.

```
class-map [match-any | type] class-map-name
no class-map [match-any | type] class-map-name
```

Syntax Description	<p>match-any (Optional) Performs a logical-OR of the matching statements under this class map. One or more criteria must be matched.</p> <hr/> <p>type (Optional) Configures the CPL class map.</p> <hr/> <p><i>class-map-name</i> Name of the class for the class map. The class name is used for both the class map and to configure a policy for the class in the policy map.</p> <hr/>				
Command Default	No class maps are defined.				
Command Modes	Global configuration Policy map configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E</td> <td>This command was introduced.</td> </tr> </tbody> </table> <hr/>	Release	Modification	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:</p> <ul style="list-style-type: none"> • 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), on page 366. • no—Removes a match statement from a class map. <p>If you enter the match-any keyword, you can only use it to specify an extended named access control list (ACL) with the match access-group class-map configuration command.</p> <p>To define packet classification on a physical-port basis, only one match command per class map is supported. Only one ACL can be configured in a class map. The ACL can have multiple access control entries (ACEs).</p>				
Examples	<p>This example shows how to configure the class map called <i>class1</i> with one match criterion, which is an access list called <i>103</i>:</p>				

```

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

```

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

```

Device(config)# no class-map class1

```

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

Related Commands

Command	Description
class, on page 360	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), on page 366	Defines the match criteria to classify traffic.
policy map, on page 394	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show class-map, on page 400	Displays QoS class maps.

debug qos

To enable debugging of the quality of service (QoS) software, use the **debug qos** in privileged EXEC mode. Use the **no** form of this command to disable QoS debugging.

debug qos {**capability** | **command-installation-time** | **events** | **index** | **pre-classify** | **provision** | **service-policy** | **set** | **snmp** | **tunnel_marking**}
no debug qos {**capability** | **command-installation-time** | **events** | **index** | **pre-classify** | **provision** | **service-policy** | **set** | **snmp** | **tunnel_marking**}

Syntax Description

capability	Displays all QoS capability debug messages.
command-installation-time	Displays the amount of time the QoS command takes to become effective.
events	Displays QoS MQC events.
index	Displays class-based QoS MIB index persistency.
pre-classify	Displays QoS pre-classify events for VPN.
provision	Displays QoS provisions.
service-policy	Displays QoS service policies.
set	Displays QoS packet marking.
snmp	Displays class-based QoS configuration and statistics information.
tunnel_marking	Displays QoS packet tunnel marking.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

The **undebug qos** command is the same as the **no debug qos** command.

When you enable debugging on a switch stack, it is enabled only on the primary stack. To enable debugging on a stack member, you can start a session from the primary stack by using the **session switch-number** privileged EXEC command, then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command stack-member-number LINE** privileged EXEC command on the primary switch to enable debugging on a member switch without first starting a session.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

match (class-map configuration)

To define the match criteria to classify traffic, use the **match** command in class-map configuration mode. Use the **no** form of this command to remove the match criteria.

```
match {access-group acl-index-or-name | ip {dscp dscp-list | precedence ip-precedence-list} | protocol
{arp | cdp | http | ip | ipv6}}
no match {access-group acl-index-or-name | ip {dscp dscp-list | precedence ip-precedence-list} |
protocol {arp | cdp | http | ip | ipv6}}
```

Syntax Description

access-group <i>acl-index-or-name</i>	Specifies the number or name of an access control list (ACL). The range is from 1 to 2799.
ip	Sets IP specific values. <ul style="list-style-type: none"> • dscp <i>dscp-list</i>—Lists 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. • precedence <i>ip-precedence-list</i>—Lists 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.
protocol	Specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map. The following protocols are supported: arp , cdp , http , ip , and ipv6 .

Command Default

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	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 or the MAC access group matching to the Ether Type/Len are supported.

If you enter the **class-map match-any** *class-map-name* global configuration command, you can enter the following **match** commands:

- **match access-group** *name* *acl-name*
- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

You cannot enter the **match access-group** *acl-index* command.

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.

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

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:

```
Device(config)# class-map class2
Device(config-cmap)# match ip dscp 10 11 12
Device(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:

```
Device(config)# class-map class3
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using *acl1*:

```
Device(config)# class-map class2
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# no match ip precedence
Device(config-cmap)# match access-group acl1
Device(config-cmap)# exit
```

Related Commands

Command	Description
class-map, on page 362	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map, on page 400	Displays quality of service (QoS) class maps.

mls qos

To enable quality of service (QoS) for the entire switch, use the **mls qos** command in global configuration mode. 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.

Command Default

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 egress queue settings are in effect.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

When the **mls qos** command is entered, QoS is enabled with the default parameters on all ports in the system.

QoS must be globally enabled to use QoS classification, policing, marking or dropping, queueing, and traffic shaping features. You can create a policy map and attach it to a port before entering the **mls qos** command. QoS processing is disabled until you enter the **mls qos** command.

When you enter the **no mls qos** command, policy maps and class maps that are used to configure QoS are not deleted from the configuration, but entries corresponding to policy maps are removed from the switch hardware to save system resources. To reenab QoS with the previous configurations, enter 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:

```
Device(config)# mls qos
```

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

Related Commands

Command	Description
show mls qos, on page 401	Displays QoS information.

mls qos aggregate-policer

To define policer parameters that can be shared by multiple classes within the same policy map, use the **mls qos aggregate-policer** command in global configuration mode. Use the **no** form of this command to delete an aggregate policer.

```
mls qos aggregate-policer aggregate-policer-name rate-bps burst-byte exceed-action {drop | policed-dscp-transmit}
no mls qos aggregate-policer aggregate-policer-name rate-bps burst-byte {drop | policed-dscp-transmit}
```

Syntax Description

<i>aggregate-policer-name</i>	The name of the aggregate policer as referenced by the police aggregate policy-map class configuration command.
<i>rate-bps</i>	The average traffic rate in bits per second (b/s). The range is 8000 to 10000000000.
<i>burst-byte</i>	The normal burst size in bytes. The range is 8000 to 1000000.
exceed-action drop	Sets the traffic rate. If the rate is exceeded, the switch drops the packet.
exceed-action policed-dscp-transmit	Sets the traffic rate. If the rate is exceeded, the switch changes the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then sends the packet.

Command Default

No aggregate policers are defined.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

Define an aggregate policer if the policer is shared with multiple classes.

Policers for a port cannot be shared with other policers for another port; traffic from two different ports cannot be aggregated for policing purposes.

The port ASIC device, which controls more than one physical port, supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port (there is no guarantee that a port will be assigned to any policer).

You apply an aggregate policer to multiple classes in the same policy map; you cannot use an aggregate policer across different policy maps.

You cannot delete an aggregate policer if it is being used in a policy map. You must first use the **no police aggregate** *aggregate-policer-name* policy-map class configuration command to delete the aggregate policer from all policy maps before using the **no mls qos aggregate-policer** *aggregate-policer-name* command.

Policing uses a token-bucket algorithm. You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the *burst-byte* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. You configure how fast (the average rate) that the tokens are removed from the bucket by using the *rate-bps* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. For more information, see the software configuration guide for this release.

Examples

This example shows how to define the aggregate policer parameters and how to apply the policer to multiple classes in a policy map:

```
Device(config)# mls qos aggregate-policer agg_policer1 1000000 1000000 exceed-action drop
Device(config)# policy-map policy2
Device(config-pmap)# class class1
Device(config-pmap-c)# police aggregate agg_policer1
Device(config-pmap-c)# exit
Device(config-pmap)# class class2
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police aggregate agg_policer1
Device(config-pmap-c)# exit
Device(config-pmap)# class class3
Device(config-pmap-c)# trust dscp
Device(config-pmap-c)# police aggregate agg_policer2
Device(config-pmap-c)# exit
```

You can verify your settings by entering the **show mls qos aggregate-policer** privileged EXEC command.

Related Commands

Command	Description
police aggregate, on page 392	Creates a policer that is shared by different classes.
show mls qos aggregate-policer, on page 402	Displays the quality of service (QoS) aggregate policer configuration.

mls qos cos

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 **mls qos cos** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

```
mls qos cos {default-cos | override}
no qos mls cos {default-cos | override}
```

Syntax Description

default-cos The default CoS value that is assigned to a port. If packets are untagged, the default CoS value becomes the packet CoS value. The CoS range is 0 to 7.

override Overrides the CoS value of the incoming packets, and apply the default CoS value on the port to all incoming packets.

Command Default

The default CoS value for a port is 0.
CoS override is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# mls qos trust cos
Device(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:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# mls qos cos 4
Device(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, on page 403	Displays quality of service (QoS) information.

mls qos dscp-mutation

To apply a Differentiated Services Code Point (DSCP)-to-DSCP-mutation map to a DSCP-trusted port, use the **mls qos dscp-mutation** command in interface configuration mode. Use the **no** form of this command to return the map to the default settings.

```
mls qos dscp-mutation dscp-mutation-name
no mls qos dscp-mutation dscp-mutation-name
```

Syntax Description	<i>dscp-mutation-name</i> The name of the DSCP-to-DSCP-mutation map. This map was previously defined with the mls qos map dscp-mutation global configuration command.				
Command Default	The default DSCP-to-DSCP-mutation map is a null map, which maps incoming DSCPs to the same DSCP values.				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	This command was introduced.				

Usage Guidelines

If two quality of service (QoS) domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate one set of DSCP values to match the definition of another domain. You apply the DSCP-to-DSCP-mutation map to the receiving port (ingress mutation) at the boundary of a QoS administrative domain.

With ingress mutation, the new DSCP value overwrites the one in the packet, and QoS handles the packet with this new value. The switch sends the packet out the port with the new DSCP value.

You can configure multiple DSCP-to-DSCP-mutation maps on ingress ports.

You apply the map only to DSCP-trusted ports. If you apply the DSCP mutation map to an untrusted port, to CoS or IP-precedence trusted port, the command has no immediate effect until the port becomes DSCP-trusted.

Examples

This example shows how to define the DSCP-to-DSCP mutation map named *dscpmutation1* and to apply the map to a port:

```
Device(config)# mls qos map dscp-mutation dscpmutation1 10 11 12 13 to 30
Device(config)# interface gigabitethernet3/0/1
Device(config-if)# mls qos trust dscp
Device(config-if)# mls qos dscp-mutation dscpmutation1
```

This example shows how to remove the DSCP-to-DSCP mutation map name *dscpmutation1* from the port and to reset the map to the default:

```
Device(config-if)# no mls qos dscp-mutation dscpmutation1
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

Related Commands

Command	Description
mls qos map, on page 376	Defines the DSCP-to-DSCP mutation map.
mls qos trust, on page 388	Configures the port trust state.
show mls qos maps, on page 407	Displays QoS mapping information.

mls qos map

To define the DSCP-to-DSCP-mutation map, use the **mls qos map** command in global configuration mode. Use the **no** form of this command to return to the default map.

```
mls qos map {dscp-mutation dscp-mutation-name in-dscp to out-dscp}
no mls qos map {dscp-mutation dscp-mutation-name in-dscp to out-dscp}
```

Syntax Description

dscp-mutation	Defines the DSCP-to-DSCP-mutation map.
<i>dscp-mutation-name in-dscp to out-dscp</i>	For <i>dscp-mutation-name</i> , enter the mutation map name. For <i>in-dscp</i> , enter up to eight DSCP values, with each value separated by a space, then enter the to keyword. For <i>out-dscp</i> , enter a single DSCP value. The range is 0 to 63.

Command Default

When this command is disabled, the default maps are set.

The default DSCP-to-DSCP-mutation map is a null map, which maps an incoming DSCP value to the same DSCP value.

The default policed-DSCP map is a null map, which maps an incoming DSCP value to the same DSCP value.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.2(6)E1	This command was introduced.

Usage Guidelines

All the maps are globally defined. The DSCP-to-DSCP-mutation map is applied to a specific port.

This example shows how to define the DSCP-to-DSCP-mutation map. All the entries that are not explicitly configured are not modified (remain as specified in the null map):

```
Device# configure terminal
Device(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 10
Device(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Device(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Device(config)# mls qos map dscp-mutation mutation1 0 31 32 33 34 to 30
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.


Related Commands

Command	Description
mls qos dscp-mutation, on page 374	Applies a DSCP-to-DSCP-mutation map to a DSCP-trusted port.
show mls qos maps, on page 407	Displays quality of service (QoS) mapping information.

mls qos queue-set output buffers

To allocate buffers to a queue set of four egress queues per port, use the **mls qos queue-set output buffers** command in global configuration mode. To return to the default setting, use the **no** form of this command.

mls qos queue-set output *qset-id* **buffers** *allocation1* ... *allocation4*
no mls qos queue-set output *qset-id* **buffers**

Syntax Description	<i>qset-id</i>	Queue set ID. 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.
	<i>allocation1</i> ... <i>allocation4</i>	Buffer space allocation (percentage) for each queue (four values for queues 1 to 4). For <i>allocation1</i> , <i>allocation3</i> , and <i>allocation4</i> , the range is 0 to 99. For <i>allocation2</i> , the range is 1 to 100 (including the CPU buffer). Separate each value with a space.
Command Default	All allocation values are equally mapped among the four queues (25, 25, 25, 25). Each queue has 1/4 th of the buffer space.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.
Usage Guidelines	Specify the 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.	
 Note	The egress queue default settings are suitable for most situations. Change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution. To configure different classes of traffic with different characteristics, use this command with the mls qos queue-set output <i>qset-id</i> threshold global configuration command.	
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. Device(config)# mls qos queue-set output 2 buffers 40 20 20 20 Device(config)# interface gigabitethernet2/0/1 Device(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, on page 379	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
queue-set, on page 396	Maps a port to a queue set.
show mls qos interface, on page 403	Displays quality of service (QoS) information at the port level
show mls qos queue-set, on page 410	Displays egress queue settings for the queue set.

mls qos queue-set output threshold

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 **mls qos queue-set output threshold** command in global configuration mode. 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		
<i>qset-id</i>	Queue set ID. 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.	
<i>queue-id</i>	(Optional) The queue in the queue set on which the command is performed. The range is 1 to 4.	
<i>drop-threshold1</i> <i>drop-threshold2</i>	Two WTD thresholds expressed as a percentage of the allocated memory of the queue. The range is 1 to 3200 percent.	
<i>reserved-threshold</i>	The 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.	
<i>maximum-threshold</i>	Queue in the full condition that is enabled 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.	

Command Default When quality of service (QoS) is enabled, WTD is enabled.
For default egress queue WTD threshold values, see [Table 25: Default Egress Queue WTD Threshold Settings, on page 379](#).

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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.

Table 25: 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

Feature	Queue 1	Queue 2	Queue 3	Queue 4
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

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 user-configurable number of packets for each queue is still internally limited to 3200 percent, or 32 times the allocated number of buffers. One packet can use one or more buffers.



Note The egress queue default settings are suitable for most situations. 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:

```
Device(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Device(config)# interface gigabitethernet2/0/1
Device(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, on page 377	Allocates buffers to a queue set.
queue-set, on page 396	Maps a port to a queue set.
show mls qos interface, on page 403	Displays quality of service (QoS) information at the port level.

Command	Description
show mls qos queue-set, on page 410	Displays egress queue settings for the queue-set.

mls qos rewrite ip dscp

To configure the switch to change or rewrite the Differentiated Services Code Point (DSCP) field of an incoming IP packet, use the **mls qos rewrite ip dscp** command in global configuration mode. Use the **no** form of this command to configure the switch to not modify or rewrite the DSCP field of the packet and to enable DSCP transparency.

mls qos rewrite ip dscp
no mls qos rewrite ip dscp

Syntax Description

This command has no arguments or keywords.

Command Default

DSCP transparency is disabled. The switch changes the DSCP field of the incoming IP packet.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

DSCP transparency affects only the DSCP field of a packet at the egress. If DSCP transparency is enabled by using the **no mls qos rewrite ip dscp** command, the switch does not modify the DSCP field in the incoming packet, and the DSCP field in the outgoing packet is the same as that in the incoming packet.



Note

Enabling DSCP transparency does not affect the port trust settings on IEEE 802.1Q tunneling ports.

By default, DSCP transparency is disabled. The switch modifies the DSCP field in an incoming packet, and the DSCP field in the outgoing packet is based on the quality of service (QoS) configuration, including the port trust setting, policing and marking, and the DSCP-to-DSCP mutation map.

Regardless of the DSCP transparency configuration, the switch modifies the internal DSCP value of the packet that the switch uses to generate a class of service (CoS) value representing the priority of the traffic. The switch also uses the internal DSCP value to select an egress queue and threshold.

For example, if QoS is enabled and an incoming packet has a DSCP value of 32, the switch might modify the internal DSCP value based on the policy-map configuration and change the internal DSCP value to 16. If DSCP transparency is enabled, the outgoing DSCP value is 32 (same as the incoming value). If DSCP transparency is disabled, the outgoing DSCP value is 16 because it is based on the internal DSCP value.

Examples

This example shows how to enable DSCP transparency and configure the switch to not change the DSCP value of the incoming IP packet:

```
Device(config)# mls qos
Device(config)# no mls qos rewrite ip dscp
```


This example shows how to disable DSCP transparency and configure the switch to change the DSCP value of the incoming IP packet:

```
Device(config)# mls qos  
Device(config)# mls qos rewrite ip dscp
```

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

Related Commands

Command	Description
mls qos, on page 368	Enables QoS globally.
show mls qos, on page 401	Displays QoS information.
show running-config include rewrite	Displays the DSCP transparency setting.

mls qos srr-queue output cos-map

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 **mls qos srr-queue output cos-map** command global configuration mode. 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*

Specifies a queue number.

For *queue-id*, the range is 1 to 4.

cos1 ... cos8

CoS values that are mapped 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

Maps 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.

Command Default

For default CoS output queue thresholds values, see [Table 26: Default Cos Output Queue Threshold Map, on page 385](#).

Command Modes

Global configuration

Command History

Release

Modification

Cisco IOS Release 15.0(2)EX
Cisco IOS Release 15.2(5)E

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. 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.

Table 26: Default Cos Output Queue Threshold Map

CoS Value	0	1	2	3	4	5	6	7
Queue ID–Threshold ID	2–1	2–1	3–1	3–1	4–1	1–1	4–1	4–1

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.

```
Device(config)# mls qos srr-queue output cos-map queue 1 threshold 1 0 1 2 3
Device(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Device(config)# interface gigabitethernet2/0/1
Device(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 queue-set output threshold, on page 379	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
mls qos srr-queue output dscp-map, on page 386	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
queue-set, on page 396	Maps a port to a queue set.
show mls qos interface, on page 403	Displays quality of service (QoS) information at the port level
show mls qos maps, on page 407	Displays QoS mapping information.
show mls qos queue-set, on page 410	Displays egress queue settings for the queue-set.

mls qos srr-queue output dscp-map

To map Differentiated Services Code Point (DSCP) values to an egress queue or to map DSCP values to a queue and to a threshold ID, use the **mls qos srr-queue output dscp-map** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
mls qos srr-queue output dscp-map queue queue-id { dscp1 ... dscp8 | threshold threshold-id dscp1 ... dscp8 }
```

```
no mls qos srr-queue output dscp-map
```

Syntax Description		
queue <i>queue-id</i>	Specifies a queue number. For <i>queue-id</i> , the range is 1 to 4.	
<i>dscp1 ... dscp8</i>	DSCP values that are mapped to an egress queue. For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63.	
threshold <i>threshold-id</i> <i>dscp1...dscp8</i>	Maps DSCP values to a queue threshold ID. For <i>threshold-id</i> , the range is 1 to 3. For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63.	

Command Default The default DSCP output queue thresholds are set.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.
For default DSCP output queue-threshold map values, see [Table 27: Default DSCP Output Queue Threshold Map, on page 387](#).



Note The egress queue default settings are suitable for most situations. Change them only when you have a thorough understanding of the egress queues and if these settings do not meet your 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 DSCP value to a different queue and threshold combination, allowing the frame to follow different behavior.

You can map up to eight DSCP values per command.

Table 27: Default DSCP Output Queue Threshold Map

DSCP Value	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
Queue ID–Threshold ID	2–1	2–1	3–1	3–1	4–1	1–1	4–1	4–1

Examples

This example shows how to map a port to queue set 1. It maps DSCP 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.

```
Device(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 0 1 2 3
Device(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Device(config)# interface gigabitethernet2/0/1
Device(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 srr-queue output cos-map, on page 384	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos queue-set output threshold, on page 379	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
queue-set, on page 396	Maps a port to a queue set.
show mls qos interface, on page 403	Displays quality of service (QoS) information at the port level
show mls qos maps, on page 407	Displays QoS mapping information.
show mls qos queue-set, on page 410	Displays egress queue settings for the queue set.

mls qos trust

To configure the port trust state, use the **mls qos trust** command in interface configuration mode. Use the **no** form of this command to return a port to its untrusted state.

```
mls qos trust [{cos | device {cisco-phone | cts | ip-camera | media-player} | dscp | ip-precedence}]
no mls qos trust [{cos | device {cisco-phone | cts | ip-camera | media-player} | dscp | ip-precedence}]
```

Syntax Description

cos	(Optional) Classifies an ingress packet by using the packet CoS value. For an untagged packet, use the port default CoS value.
device cisco-phone	(Optional) Classifies an ingress packet by trusting the CoS or DSCP value sent from the Cisco IP Phone (trusted boundary), depending on the trust setting.
device {cts ip-camera media-player}	(Optional) Classifies an ingress packet by trusting the CoS or DSCP value for these video devices: <ul style="list-style-type: none"> • cts—Cisco TelePresence System • ip-camera—Cisco IP camera • media-player—Cisco digital media player For an untagged packet, use the port default CoS value.
dscp	(Optional) Classifies an ingress packet by using the packet DSCP value (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS is used if the packet is tagged. For an untagged packet, the default port CoS value is used.
ip-precedence	(Optional) Classifies an ingress packet by using the packet IP-precedence value (most significant 3 bits of 8-bit service-type field). For a non-IP packet, the packet CoS is used if the packet is tagged. For an untagged packet, the port default CoS value is used.

Command Default

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
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	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.

When a port is configured with trust DSCP or trust IP precedence and the incoming packet is a non-IP packet, the CoS-to-DSCP map is used to derive the corresponding DSCP value from the CoS value. The CoS can be the packet CoS for trunk ports or the port default CoS for nontrunk ports.

If the DSCP is trusted, the DSCP field of the IP packet is not modified. However, it is still possible that the CoS value of the packet is modified (according to DSCP-to-CoS map).

If the CoS is trusted, the CoS field of the packet is not modified, but the DSCP can be modified (according to CoS-to-DSCP map) if the packet is an IP packet.

The trusted boundary feature prevents security problems if users disconnect their PCs from networked Cisco IP Phones and connect them to the switch port to take advantage of trusted CoS or DSCP settings. You must globally enable the Cisco Discovery Protocol (CDP) on the switch and on the port connected to the IP phone. If the telephone is not detected, trusted boundary disables the trusted setting on the switch or routed port and prevents misuse of a high-priority queue.

If you configure the trust setting for DSCP or IP precedence, the DSCP or IP precedence values in the incoming packets are trusted. If you configure the **mls qos cos override** interface configuration command on the switch port connected to the IP phone, the switch overrides the CoS of the incoming voice and data packets and assigns the default CoS value to them.

For an inter-QoS domain boundary, you can configure the port to the DSCP-trusted state and apply the DSCP-to-DSCP-mutation map if the DSCP values are different between the QoS domains.

Classification using a port trust state (for example, **mls qos trust [cos | dscp | ip-precedence]**) and a policy map (for example, **service-policy input policy-map-name**) are mutually exclusive. The last one configured overwrites the previous configuration.

Related Commands

This example shows how to configure a port to trust the IP precedence field in the incoming packet:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# mls qos trust ip-precedence
```

This example shows how to specify that the Cisco IP Phone connected on a port is a trusted device:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# mls qos trust device cisco-phone
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands

Command	Description
mls qos cos, on page 372	Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port.
mls qos dscp-mutation, on page 374	Applies a DSCP-to DSCP-mutation map to a DSCP-trusted port.
mls qos map, on page 376	Defines the CoS-to-DSCP map, DSCP-to-CoS map, the DSCP-to-DSCP-mutation map, the IP-precedence-to-DSCP map, and the policed-DSCP map.
show mls qos interface, on page 403	Displays QoS information.

police

To define a policer for classified traffic, use the **police** command in policy-map class configuration mode. Use the **no** form of this command to remove an existing policer.

```
police rate-bps burst-byte [exceed-action [drop | policed-dscp-transmit ]]  
no police rate-bps burst-byte [exceed-action [drop | policed-dscp-transmit ]]
```

Syntax Description		
<i>rate-bps</i>		Specifies the average traffic rate in bits per second (b/s). The range is 8000 to 10000000000.
<i>burst-byte</i>		Specifies the normal burst size in bytes. The range is 8000 to 1000000.
exceed-action drop		(Optional) Sets the traffic rate. If the rate is exceeded, the switch drops the packet .
exceed-action policed-dscp-transmit		(Optional) Sets the traffic rate. If the rate is exceeded, the switch changes the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then sends the packet.
aggregate		Chooses the aggregate policer for the current class.

Command Default No policers are defined.

Command Modes Policy-map class configuration

Command History	Release	Modification
	Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

The port ASIC device, which controls more than one physical port, supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Policing uses a token-bucket algorithm. You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the *burst-byte* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. You configure how quickly (the average rate) the tokens are removed from the bucket by using the *rate-bps* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. For more information, see the software configuration guide for this release.

Examples

This example shows how to configure a policer that drops packets if traffic exceeds 1 Mb/s average rate with a burst size of 20 KB. The DSCPs of incoming packets are trusted, and there is no packet modification.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# trust dscp
Device(config-pmap-c)# police 1000000 20000 exceed-action drop
Device(config-pmap-c)# exit
```

This example shows how to configure a policer, which marks down the DSCP values with the values defined in policed-DSCP map and sends the packet:

```
Device(config)# policy-map policy2
Device(config-pmap)# class class2
Device(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Device(config-pmap-c)# exit
```

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

Related Commands

Command	Description
class , on page 360	Defines a traffic classification match criteria (through the police , set , and trust policy-map class configuration commands) for the specified class-map name.
class-map , on page 362	Create a class map to be used for matching packets to the class whose name you specify with the class command.
mls qos map , on page 376 policed-dscp	Applies a policed-DSCP map to a DSCP-trusted port.
policy map , on page 394	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
set , on page 398	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
show policy-map , on page 411	Displays QoS policy maps.

police aggregate

To apply an aggregate policer to multiple classes in the same policy map, use the **police aggregate** command in policy-map class configuration mode. Use the **no** form of this command to remove the specified policer.

police aggregate *aggregate-policer-name*
no police aggregate *aggregate-policer-name*

Syntax Description

aggregate-policer-name The name of the aggregate policer.

Command Default

No aggregate policers are defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

The port ASIC device, which controls more than one physical port, supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer.

You set aggregate policer parameters by using the **mls qos aggregate-policer** global configuration command. You apply an aggregate policer to multiple classes in the same policy map; you cannot use an aggregate policer across different policy maps.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

You cannot configure aggregate policers in hierarchical policy maps.

Examples

This example shows how to define the aggregate policer parameters and to apply the policer to multiple classes in a policy map:

```
Device(config)# mls qos aggregate-policer agg_policer1 10000 1000000 exceed-action drop
Device(config)# policy-map policy2
Device(config-pmap)# class class1
Device(config-pmap-c)# police aggregate agg_policer1
Device(config-pmap-c)# exit
Device(config-pmap)# class class2
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police aggregate agg_policer1
Device(config-pmap-c)# exit
Device(config-pmap)# class class3
Device(config-pmap-c)# trust dscp
```

```
Device(config-pmap-c) # police aggregate agg_policer2  
Device(config-pmap-c) # exit
```

You can verify your settings by entering the **show mls qos aggregate-policer** privileged EXEC command.

Related Commands	Command	Description
	mls qos aggregate-policer, on page 370	Defines policer parameters, which can be shared by multiple classes within a policy map.
	show mls qos aggregate-policer, on page 402	Displays the quality of service (QoS) aggregate policer configuration.

policy map

To create or modify a policy map that can be attached to multiple physical ports and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

policy-map *policy-map-name*
no policy-map *policy-map-name*

Syntax Description

policy-map-name The name of the policy map.

Command Default

No policy maps are defined.

The default behavior is to set the Differentiated Services Code Point (DSCP) to 0 if the packet is an IP packet and to set the class of service (CoS) to 0 if the packet is tagged. No policing is performed.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**—Defines the classification match criteria for the specified class map.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

You can configure QoS only on physical ports. Configure the QoS settings, such as classification, queueing, and scheduling, and apply the policy map to a port. When configuring QoS on a physical port, you apply a nonhierarchical policy map to a port. A nonhierarchical policy map is the same as the port-based policy maps in the device.

Examples

This example shows how to create a policy map called *policy1*.

```
Device(config)# policy-map policy1
```

This example shows how to delete *policy1*:

```
Device(config)# no policy-map policy1
```

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

Related Commands

Command	Description
class, on page 360	Defines a traffic classification match criteria (through the police , set , and trust policy-map class configuration command) for the specified class-map name.
class-map, on page 362	Creates a class map to be used for matching packets to the class whose name you specify.
service-policy, on page 397	Applies a policy map to a physical port.
show policy-map, on page 411	Displays QoS policy maps.

queue-set

To map a port to a queue set, use the **queue-set** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

queue-set *qset-id*
no queue-set *qset-id*

Syntax Description

qset-id Queue-set ID. 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.

Command Default

The queue set ID is 1.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E
	This command was introduced.

Usage Guidelines

For information about automatic generation of the queue-set ID with the **auto qos voip** command, see the “Usage Guidelines” section for the [auto qos voip, on page 346](#) command.

Examples

This example shows how to map a port to queue-set 2:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **buffers** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers, on page 377	Allocates buffers to a queue set.
mls qos queue-set output threshold, on page 379	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
show mls qos interface, on page 403	Displays quality of service (QoS) information.

service-policy

To apply a policy map to the input of a physical port, use the **service-policy** command in interface configuration mode. Use the **no** form of this command to remove the policy map and port association.

```
service-policy {input | output} policy-map-name
no service-policy {input | output} policy-map-name
```

Syntax Description

input Applies the specified policy map to the input of a physical port.
policy-map-name

Command Default

No policy maps are attached to the port.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Though visible in the command-line help strings, the **output** keyword is not supported.

Policy maps can be configured on physical ports. A policy map is defined by the **policy map** command.

Only one policy map is supported per port, per direction. In other words, only one input policy and one output policy is allowed on any one port.

You can apply a policy map to incoming traffic on a physical port. .

Classification using a port trust state (for example, **mls qos trust [cos | dscp | ip-precedence]** and a policy map (for example, **service-policy input policy-map-name**) are mutually exclusive. The last one configured overwrites the previous configuration.

Examples

This example shows how to remove *plcmap2* from a physical port:

```
Device(config)# interface gigabitethernet2/0/2
Device(config-if)# no service-policy input plcmap2
```

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

Related Commands

Command	Description
policy map, on page 394	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map, on page 411	Displays QoS policy maps.
show running-config	Displays the operating configuration.

set

To classify IP traffic by setting a Differentiated Services Code Point (DSCP) or an IP-precedence value in the packet, use the **set** command in policy-map class configuration mode. Use the **no** form of this command to remove traffic classification.

```
set {dscp new-dscp | ip {dscp | precedence} | precedence precedence}
no set {dscp new-dscp | ip {dscp | precedence} | precedence precedence}
```

Syntax Description		
dscp <i>new-dscp</i>	Sets the DSCP value in IPv4 and IPv6 packets. The range is 0 to 63.	
ip { dscp precedence }	Sets the IP values.	<ul style="list-style-type: none"> • dscp—Sets the IP DSCP value. • precedence—Sets the IP precedence value.
precedence <i>new-precedence</i>	Sets the precedence in IPv4 and IPv6 packets. The range is 0 to 7.	

Command Default No traffic classification is defined.

Command Modes Policy-map class configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines If you have used the **set ip dscp** policy-map class configuration command, the device changes this command to **set dscp** in the device configuration. If you enter the **set ip dscp** policy-map class configuration command, this setting appears as **set dscp** in the device configuration.

You can use the **set ip precedence** policy-map class configuration command or the **set precedence** policy-map class configuration command. This setting appears as **set ip precedence** in the device configuration.

The **set** command is mutually exclusive with the **trust** policy-map class configuration command within the same policy map.

For the **set dscp new-dscp** or the **set ip precedence new-precedence** command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **set dscp af11** command, which is the same as entering the **set dscp 10** command. You can enter the **set ip precedence critical** command, which is the same as entering the **set ip precedence 5** command. For a list of supported mnemonics, enter the **set dscp ?** or the **set ip precedence ?** command to see the command-line help strings.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to assign DSCP 10 to all FTP traffic without any policers:

```
Device(config)# policy-map policy_ftp
Device(config-pmap)# class-map ftp_class
Device(config-cmap)# exit
Device(config)# policy-map policy_ftp
Device(config-pmap)# class ftp_class
Device(config-pmap-c)# set dscp 10
Device(config-pmap)# exit
```

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

Related Commands

Command	Description
class, on page 360	Defines a traffic classification match criteria (through the police , set , and trust policy-map class configuration commands) for the specified class-map name.
police, on page 390	Defines a policer for classified traffic.
policy map, on page 394	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map, on page 411	Displays QoS policy maps.
trust, on page 418	Defines a trust state for traffic classified through the class policy-map configuration command or the class-map global configuration command.

show class-map

To display quality of service (QoS) class maps, which define the match criteria to classify traffic, use the **show class-map** command in EXEC mode.

```
show class-map [class-map-name | type control subscriber {all | class-map-name}]
```

Syntax Description

class-map-name (Optional) Class map name.

type control subscriber (Optional) Displays information about control class maps.

all (Optional) Displays information about all control class maps.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

This command is supported only on the LAN Base image.

Examples

This is an example of output from the **show class-map** command:

```
Device# show class-map
Class Map match-any 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-any dscp5 (id 3)
  Match ip dscp 5
```

Related Commands

Command	Description
class-map , on page 362	Creates a class map to be used for matching packets to the class whose name you specify.
match (class-map configuration) , on page 366	Defines the match criteria to classify traffic.

show mls qos

To display global quality of service (QoS) configuration information, use the **show mls qos** command in EXEC mode.

show mls qos

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

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:

```
Device# 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:

```
Device# show mls qos
QoS is enabled
QoS ip packet dscp rewrite is enabled
```

Related Commands

Command	Description
mls qos, on page 368	Enables QoS on the entire switch.

show mls qos aggregate-policer

To display the quality of service (QoS) aggregate policer configuration, use the **show mls qos aggregate-policer** command in EXEC mode.

show mls qos aggregate-policer [*aggregate-policer-name*]

Syntax Description	<i>aggregate-policer-name</i> (Optional) Displays the policer configuration for the specified name.
---------------------------	---

Command Modes	User EXEC Privileged EXEC
----------------------	------------------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines	<p>A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.</p> <p>This command is supported only on the LAN Base image.</p>
-------------------------	--

Examples	<p>This is an example of output from the show mls qos aggregate-policer command:</p>
-----------------	---

```
Device# show mls qos aggregate-policer policer1
aggregate-policer policer1 1000000 2000000 exceed-action drop
Not used by any policy map
```

Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>mls qos aggregate-policer, on page 370</td> <td>Defines policer parameters that can be shared by multiple classes within a policy map.</td> </tr> </tbody> </table>	Command	Description	mls qos aggregate-policer, on page 370	Defines policer parameters that can be shared by multiple classes within a policy map.
Command	Description				
mls qos aggregate-policer, on page 370	Defines policer parameters that can be shared by multiple classes within a policy map.				

show mls qos interface

To display quality of service (QoS) information at the port level, use the **show mls qos interface** command in EXEC mode.

show mls qos interface [*interface-id*] [{**buffers** | **queueing** | **statistics**}]

Syntax Description		
	<i>interface-id</i>	(Optional) The QoS information for the specified port. Valid interfaces include physical ports.
	buffers	(Optional) Displays the buffer allocation among the queues.
	queueing	(Optional) Displays the queueing strategy (shared or shaped) and the weights corresponding to the queues.
	statistics	(Optional) Displays 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.

Command Modes	
	User EXEC
	Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines	
	Though visible in the command-line help string, the policers keyword is not supported.
	This command is supported only on the LAN Base image.

Examples

This is an example of output from the **show mls qos interface** *interface-id* command when port-based QoS is enabled:

```
Device# show mls qos interface gigabitethernet1/0/1
GigabitEthernet1/0/1
trust state: trust cos
trust mode: trust cos
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* command when port-based QoS is disabled:

```

Device# show mls qos interface gigabitethernet1/0/1
GigabitEthernet1/0/1
QoS is disabled. When QoS is enabled, following settings will be applied
trust state: trust cos
trust mode: trust cos
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:

```

Device# show mls qos interface gigabitethernet1/0/2 buffers
GigabitEthernet1/0/2
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.

```

Device# show mls qos interface gigabitethernet1/0/2 queueing
GigabitEthernet1/0/2
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

```

This is an example of output from the **show mls qos interface interface-id statistics** command:

```

Device# show mls qos interface gigabitethernet1/0/1 statistics
GigabitEthernet1/0/1 (All statistics are in packets)

dscp: incoming
-----

 0 - 4 :          15233          0          0          0          0
 5 - 9 :           0          0          0          0          0
10 - 14 :          0          0          0          0          0
15 - 19 :          0          0          0          0          0
20 - 24 :          0          0          0          0          0
25 - 29 :          0          0          0          0          0
30 - 34 :          0          0          0          0          0
35 - 39 :          0          0          0          0          0
40 - 44 :          0          0          0          0          0
45 - 49 :          0          0          0          406417         0
50 - 54 :          0          0          0          0          0
55 - 59 :          0          0          0          0          0
60 - 64 :          0          0          0          0          0

dscp: outgoing
-----

 0 - 4 :           337          0          0          0          0
 5 - 9 :           0          0          0          0          0
10 - 14 :          0          0          0          0          0
15 - 19 :          0          0          0          0          0
20 - 24 :          0          0          0          0          0
25 - 29 :          0          0          0          0          0
30 - 34 :          0          0          0          0          0
35 - 39 :          0          0          0          0          0

```

```

40 - 44 :          0          0          0          0          0
45 - 49 :          0          0          0        13866          0
50 - 54 :          0          0          0          0          0
55 - 59 :          0          0          0          0          0
60 - 64 :          0          0          0          0          0
  cos: incoming
-----
 0 -  4 :    1426270          0          0          0          0
 5 -  7 :          0          0          0          0          0
  cos: outgoing
-----
 0 -  4 :    131687          12          0          0          7478
 5 -  7 :    1993          25483          275213
  output queues enqueued:
  queue:  threshold1  threshold2  threshold3
-----
  queue 0:          0          0          0
  queue 1:          0          341          441525
  queue 2:          0          0          0
  queue 3:          0          0          0

  output queues dropped:
  queue:  threshold1  threshold2  threshold3
-----
  queue 0:          0          0          0
  queue 1:          0          0          0
  queue 2:          0          0          0
  queue 3:          0          0          0

Policer: Inprofile:          0 OutofProfile:          0

```

This table describes the fields in this display.

Table 28: show mls qos interface statistics Field Descriptions

Field		Description
DSCP	incoming	Number of packets received for each DSCP value.
	outgoing	Number of packets sent for each DSCP value.
CoS	incoming	Number of packets received for each CoS value.
	outgoing	Number of packets sent for each CoS value.
Output queues	enqueued	Number of packets in the egress queue.
	dropped	Number of packets in the egress queue that are dropped.
Policer	Inprofile	Number of in-profile packets for each policer.
	Outofprofile	Number of out-of-profile packets for each policer.

Related Commands

Command	Description
mls qos queue-set output buffers, on page 377	Allocates buffers to a queue set.
mls qos queue-set output threshold, on page 379	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
mls qos srr-queue output cos-map, on page 384	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map, on page 386	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
policy map, on page 394	Creates or modifies a policy map.
queue-set, on page 396	Maps a port to a queue set.
srr-queue bandwidth limit, on page 412	Limits the maximum output on a port.
srr-queue bandwidth shape, on page 414	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
srr-queue bandwidth share, on page 416	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

show mls qos maps

To display quality of service (QoS) mapping information, use the **show mls qos maps** command in EXEC mode.

```
show mls qos maps [{cos-dscp | cos-output-q | dscp-cos | dscp-mutation dscp-mutation-name |
dscp-output-q | ip-prec-dscp | policed-dscp}]
```

Syntax Description	cos-dscp	(Optional) Displays class of service (CoS)-to-DSCP map.
	cos-output-q	(Optional) Displays the CoS output queue threshold map.
	dscp-cos	(Optional) Displays DSCP-to-CoS map.
	dscp-mutation <i>dscp-mutation-name</i>	(Optional) Displays the specified DSCP-to-DSCP-mutation map.
	dscp-output-q	(Optional) Displays the DSCP output queue threshold map.
	ip-prec-dscp	(Optional) Displays the IP-precedence-to-DSCP map.
	policed-dscp	(Optional) Displays the policed-DSCP map.
Command Default	None	
Command Modes	User EXEC Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	This command was introduced.
Usage Guidelines	<p>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.</p> <p>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.</p> <p>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 output queue threshold map, a DSCP value of 43 corresponds to queue 1 and threshold 3 (01-03).</p> <p>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 output queue threshold map, a CoS value of 5 corresponds to queue 1 and threshold 3 (1-3).</p>	

Examples

This is an example of output from the **show mls qos maps** command:

```
Device# 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 46 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 :    03-03 03-03 03-03 03-03 03-03 03-03 03-03 03-03 03-03 04-01 04-01
1 :    04-02 04-01 04-02 04-01 04-02 04-01 02-01 02-01 02-01 02-01 02-01
2 :    02-01 02-01 02-01 02-01 02-02 03-01 02-01 02-01 02-01 02-01 02-01
3 :    02-01 02-01 01-03 01-03 02-01 02-01 02-01 02-01 02-01 02-01 02-01
4 :    01-03 01-03 01-03 01-03 01-03 01-03 01-03 01-03 01-03 02-03 02-03
5 :    02-03 02-03 02-03 02-03 02-03 02-03 02-03 02-03 02-03 02-03 02-03
6 :    02-03 02-03 02-03 02-03

Cos-outputq-threshold map:
cos:  0 1 2 3 4 5 6 7
-----
queue-threshold: 3-3 4-3 2-1 2-2 1-3 1-3 2-3 2-3

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 map, on page 376	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 srr-queue output cos-map, on page 384	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map, on page 386	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.

show mls qos queue-set

To display quality of service (QoS) settings for the egress queues, use the **show mls qos queue-set** command in EXEC mode.

show mls qos queue-set [*gset-id*]

Syntax Description	<i>gset-id</i> (Optional) Queue set ID. 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.	
Command Modes	User EXEC Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Examples

This is an example of output from the **show mls qos queue-set** command:

```
Device# 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, on page 377	Allocates buffers to the queue set.
	mls qos queue-set output threshold, on page 379	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation of the queue set.

show policy-map

To display quality of service (QoS) policy maps, which define classification criteria for incoming traffic, use the **show policy-map** command in EXEC mode.

```
show policy-map [ policy-map-name ]
```

Syntax Description	<i>policy-map-name</i> (Optional) The policy map name.
---------------------------	--

Command Modes	User EXEC Privileged EXEC
----------------------	------------------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines	Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.
-------------------------	--



Note	Though visible in the command-line help string, the session , type , control-plane , and interface keywords are not supported; statistics shown in the display should be ignored.
-------------	---

Examples

This is an example of output from the **show policy-map** command:

```
Device# show policy-map
Policy Map videowizard_policy2
  class videowizard_10-10-10-10
    set dscp 34
    police 100000000 2000000 exceed-action drop

Policy Map mypolicy
  class dscp5
    set dscp 6
```

Related Commands	Command	Description
	policy map, on page 394	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.

srr-queue bandwidth limit

To limit the maximum output on a port, use the **srr-queue bandwidth limit** command in interface configuration mode. 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 The port speed limit in percentage terms. The range is 10 to 90.

Command Default

The port is not rate limited and is set to 100 percent.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	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.

Examples

This example shows how to limit a port to 800 Mb/s:

```
Device(config)# interface gigabitethernet2/0/1
Device(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, on page 377	Allocates buffers to the queue set.
mls qos srr-queue output dscp-map, on page 386	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold, on page 379	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation for the queue set.
queue-set, on page 396	Maps a port to a queue set.
show mls qos interface, on page 403	Displays QoS information.
srr-queue bandwidth shape, on page 414	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.

Command	Description
srr-queue bandwidth share, on page 416	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

srr-queue bandwidth shape

To assign the shaped weights and to enable bandwidth shaping on the four egress queues mapped to a port, use the **srr-queue bandwidth shape** command in interface configuration mode. 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	<i>weight1 weight2 weight3 weight4</i>	The weights that 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.
---------------------------	--	---

Command Default 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
	Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	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. Queues 2, 3, and 4 operate in the shared mode, because the weight ratios for these queues are set to 0. 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:


```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# srr-queue bandwidth shape 8 0 0 0
Device(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, on page 377	Allocates buffers to a queue set.
mls qos srr-queue output dscp-map, on page 386	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold, on page 379	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
queue-set, on page 396	Maps a port to a queue set.
show mls qos interface, on page 403	Displays QoS information.
srr-queue bandwidth share, on page 416	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

srr-queue bandwidth share

To assign the shared weights and to enable bandwidth sharing on the four egress queues mapped to a port, use the **srr-queue bandwidth share** command in interface configuration mode. 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	<i>weight1 weight2 weight3 weight4</i>	The ratios of <i>weight1</i> , <i>weight2</i> , <i>weight3</i> , and <i>weight4</i> 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.
Command Default	Equal bandwidth is allocated to each queue (Equal bandwidth for weight1, weight2, weight3, and weight4).	
Command Modes	Interface configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)E Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

The ratio of the weights is the ratio of frequency in which the shaped round-robin (SRR) scheduler dequeues packets from each queue.

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. 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.

```
Device(config)# interface gigabitethernet2/0/1
Device(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, on page 377	Allocates buffers to a queue set.
	mls qos queue-set output threshold, on page 379	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
	mls qos srr-queue output dscp-map, on page 386	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
	queue-set, on page 396	Maps a port to a queue set.
	show mls qos interface, on page 403	Displays quality of service (QoS) information.
	srr-queue bandwidth shape, on page 414	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.

trust

To define a trust state for traffic classified through the **class** policy-map configuration or the **class-map** global configuration command, use the **trust** command in policy-map class configuration mode. Use the **no** form of this command to return to the default setting.

```
trust [{cos | dscp | ip-precedence}]
no trust [{cos | dscp | ip-precedence}]
```

Syntax Description	
cos	(Optional) Classifies an ingress packet by using the packet class of service (CoS) value. For an untagged packet, the port default CoS value is used.
dscp	(Optional) Classifies an ingress packet by using the packet Differentiated Services Code Point (DSCP) values (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the default port CoS value is used to map CoS to DSCP.
ip-precedence	(Optional) Classifies an ingress packet by using the packet IP-precedence value (most significant 3 bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the port default CoS value is used to map CoS to DSCP.

Command Default The action is not trusted. If no keyword is specified when the command is entered, the default is **dscp**.

Command Modes Policy-map class configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	This command was introduced.
	Cisco IOS Release 15.2(5)E	

Usage Guidelines Use this command to distinguish the quality of service (QoS) trust behavior for certain traffic from other traffic. For example, incoming traffic with certain DSCP values can be trusted. You can configure a class map to match and trust the DSCP values in the incoming traffic.

Trust values set with this command supersede trust values set with the **mls qos trust** interface configuration command.

The **trust** command is mutually exclusive with **set** policy-map class configuration command within the same policy map.

If you specify **trust cos**, QoS uses the received or default port CoS value and the CoS-to-DSCP map to generate a DSCP value for the packet.

If you specify **trust dscp**, QoS uses the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP value for the packet is derived from the CoS-to-DSCP map.

If you specify **trust ip-precedence**, QoS uses the IP precedence value from the ingress packet and the IP-precedence-to-DSCP map. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP

packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP for the packet is derived from the CoS-to-DSCP map.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to define a port trust state to trust incoming DSCP values for traffic classified with a default class:

```
Device(config)# policy-map policy1
Device(config-pmap)# class class-default
Device(config-pmap-c)# trust dscp
Device(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Device(config-pmap-c)# exit
```

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

Related Commands

Command	Description
class, on page 360	Defines a traffic classification match criteria (through the police , set , and trust policy-map class configuration command) for the specified class-map name.
police, on page 390	Defines a policer for classified traffic.
policy map, on page 394	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
set, on page 398	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
show policy-map, on page 411	Displays QoS policy maps.



PART **VII**

Security

- [Security](#), on page 423



Security

- [aaa accounting dot1x](#), on page 425
- [aaa accounting identity](#), on page 427
- [aaa authentication dot1x](#), on page 429
- [aaa authorization network](#), on page 430
- [aaa new-model](#), on page 431
- [authentication host-mode](#), on page 433
- [authentication mac-move permit](#), on page 435
- [authentication priority](#), on page 436
- [authentication violation](#), on page 439
- [auto security](#), on page 441
- [auto security-port](#), on page 442
- [cisp enable](#), on page 443
- [clear errdisable interface vlan](#), on page 444
- [clear mac address-table](#), on page 445
- [debug ip rip](#), on page 447
- [deny \(MAC access-list configuration\)](#), on page 449
- [device-role \(IPv6 snooping\)](#), on page 453
- [device-role \(IPv6 nd inspection\)](#), on page 454
- [device-tracking policy](#), on page 455
- [dot1x critical \(global configuration\)](#), on page 457
- [dot1x pae](#), on page 458
- [dot1x supplicant force-multicast](#), on page 459
- [dot1x test eapol-capable](#), on page 460
- [dot1x test timeout](#), on page 461
- [dot1x timeout](#), on page 462
- [epm access-control open](#), on page 464
- [ip admission](#), on page 465
- [ip admission name](#), on page 466
- [ip device tracking maximum](#), on page 468
- [ip device tracking probe](#), on page 469
- [ip dhcp snooping database](#), on page 470
- [ip dhcp snooping information option format remote-id](#), on page 472
- [ip dhcp snooping verify no-relay-agent-address](#), on page 473

- ip source binding, on page 474
- ip verify source, on page 475
- ipv6 snooping policy, on page 477
- limit address-count, on page 478
- mab request format attribute 32, on page 479
- match (access-map configuration), on page 481
- mls qos copp protocol, on page 483
- authentication logging verbose, on page 487
- dot1x logging verbose, on page 488
- mab logging verbose, on page 489
- permit (MAC access-list configuration), on page 490
- protocol (IPv6 snooping), on page 494
- radius server, on page 495
- router rip, on page 497
- security level (IPv6 snooping), on page 498
- show aaa acct-stop-cache, on page 499
- show aaa clients, on page 500
- show aaa command handler, on page 501
- **show aaa local**, on page 502
- show aaa servers, on page 503
- show aaa sessions, on page 504
- show authentication sessions, on page 505
- show auto security, on page 508
- show cisp, on page 510
- show dot1x, on page 512
- show eap pac peer, on page 514
- show ip dhcp snooping statistics, on page 515
- show ip rip database, on page 518
- show mls qos copp protocols, on page 520
- show radius server-group, on page 521
- show vlan group, on page 523
- switchport port-security aging, on page 524
- switchport port-security mac-address, on page 526
- switchport port-security maximum, on page 528
- switchport port-security violation, on page 530
- tracking (IPv6 snooping), on page 532
- trusted-port, on page 534
- vlan access-map, on page 535
- vlan filter, on page 537
- vlan group, on page 538

aaa accounting dot1x

To enable authentication, authorization, and accounting (AAA) accounting and to create method lists defining specific accounting methods on a per-line or per-interface basis for IEEE 802.1x sessions, use the **aaa accounting dot1x** command in global configuration mode. To disable IEEE 802.1x accounting, use the **no** form of this command.

```
aaa accounting dot1x {name | default} start-stop {broadcast group {name | radius | tacacs+}
[group {name | radius | tacacs+} ... ] | group {name | radius | tacacs+} [group
{name | radius | tacacs+} ... ]}
no aaa accounting dot1x {name | default}
```

Syntax Description

name	Name of a server group. This is optional when you enter it after the broadcast group and group keywords.
default	Specifies the accounting methods that follow as the default list for accounting services.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting notice was received by the accounting server.
broadcast	Enables accounting records to be sent to multiple AAA servers and sends accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.
group	Specifies the server group to be used for accounting services. These are valid server group names: <ul style="list-style-type: none"> • name — Name of a server group. • radius — Lists of all RADIUS hosts. • tacacs+ — Lists of all TACACS+ hosts. <p>The group keyword is optional when you enter it after the broadcast group and group keywords. You can enter more than optional group keyword.</p>
radius	(Optional) Enables RADIUS accounting.
tacacs+	(Optional) Enables TACACS+ accounting.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

This command requires access to a RADIUS server.

We recommend that you enter the **dot1x reauthentication** interface configuration command before configuring IEEE 802.1x RADIUS accounting on an interface.

This example shows how to configure IEEE 802.1x accounting:

```
Device(config)# aaa new-model  
Device(config)# aaa accounting dot1x default start-stop group radius
```

aaa accounting identity

To enable authentication, authorization, and accounting (AAA) accounting for IEEE 802.1x, MAC authentication bypass (MAB), and web authentication sessions, use the **aaa accounting identity** command in global configuration mode. To disable IEEE 802.1x accounting, use the **no** form of this command.

```
aaa accounting identity {name | default} start-stop {broadcast group {name | radius | tacacs+}
[group {name | radius | tacacs+} ... ] | group {name | radius | tacacs+} [group
{name | radius | tacacs+} ... ]}
no aaa accounting identity {name | default}
```

Syntax Description

name	Name of a server group. This is optional when you enter it after the broadcast group and group keywords.
default	Uses the accounting methods that follow as the default list for accounting services.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested-user process begins regardless of whether or not the start accounting notice was received by the accounting server.
broadcast	Enables accounting records to be sent to multiple AAA servers and send accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.
group	Specifies the server group to be used for accounting services. These are valid server group names: <ul style="list-style-type: none"> • name — Name of a server group. • radius — Lists of all RADIUS hosts. • tacacs+ — Lists of all TACACS+ hosts. <p>The group keyword is optional when you enter it after the broadcast group and group keywords. You can enter more than optional group keyword.</p>
radius	(Optional) Enables RADIUS authorization.
tacacs+	(Optional) Enables TACACS+ accounting.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

To enable AAA accounting identity, you need to enable policy mode. To enable policy mode, enter the **authentication display new-style** command in privileged EXEC mode.

This example shows how to configure IEEE 802.1x accounting identity:

```
Device# authentication display new-style
```

Please note that while you can revert to legacy style configuration at any time unless you have explicitly entered new-style configuration, the following caveats should be carefully read and understood.

- (1) If you save the config in this mode, it will be written to NVRAM in NEW-style config, and if you subsequently reload the router without reverting to legacy config and saving that, you will no longer be able to revert.
- (2) In this and legacy mode, Webauth is not IPv6-capable. It will only become IPv6-capable once you have entered new-style config manually, or have reloaded with config saved in 'authentication display new' mode.

```
Device# configure terminal
```

```
Device(config)# aaa accounting identity default start-stop group radius
```

aaa authentication dot1x

To specify the authentication, authorization, and accounting (AAA) method to use on ports complying with the IEEE 802.1x authentication, use the **aaa authentication dot1x** command in global configuration mode on the switch stack or on a standalone switch. To disable authentication, use the **no** form of this command.

```
aaa authentication dot1x {default} method1
no aaa authentication dot1x {default} method1
```

Syntax Description	default	The default method when a user logs in. Use the listed authentication method that follows this argument.
	<i>method1</i>	Specifies the server authentication. Enter the group radius keywords to use the list of all RADIUS servers for authentication.
	Note	Though other keywords are visible in the command-line help strings, only the default and group radius keywords are supported.
Command Default	No authentication is performed.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E

Usage Guidelines The **method** argument identifies the method that the authentication algorithm tries in the specified sequence to validate the password provided by the client. The only method that is IEEE 802.1x-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command.

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

This example shows how to enable AAA and how to create an IEEE 802.1x-compliant authentication list. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is not allowed access to the network.

```
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
```

aaa authorization network

To configure the switch to use user-RADIUS authorization for all network-related service requests, such as IEEE 802.1x VLAN assignment, use the **aaa authorization network** command in global configuration mode. To disable RADIUS user authorization, use the **no** form of this command

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.
---------------------------	---

Command Default	Authorization is disabled.
------------------------	----------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines	Use the aaa authorization network default group radius global configuration command to allow the switch to download IEEE 802.1x 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.

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

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


aaa new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

aaa new-model
no aaa new-model

Syntax Description This command has no arguments or keywords.

Command Default AAA is not enabled.

Command Modes Global configuration (config)

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	This command was introduced.

Usage Guidelines This command enables the AAA access control system.

If the **login local** command is configured for a virtual terminal line (VTY), and the **aaa new-model** command is removed, you must reload the switch to get the default configuration or the **login** command. If the switch is not reloaded, the switch defaults to the **login local** command under the VTY.



Note We do not recommend removing the **aaa new-model** command.

The following example shows this restriction:

```
Switch(config)# aaa new-model
Switch(config)# line vty 0 15
Switch(config-line)# login local
Switch(config-line)# exit
Switch(config)# no aaa new-model
Switch(config)# exit
Switch# show running-config | b line vty

line vty 0 4
  login local !<=== Login local instead of "login"
line vty 5 15
  login local
!
```

Examples

The following example initializes AAA:

```
Switch(config)# aaa new-model
Switch(config)#
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication arap	Enables an AAA authentication method for ARAP using TACACS+.
aaa authentication enable default	Enables AAA authentication to determine if a user can access the privileged command level.
aaa authentication login	Sets AAA authentication at login.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

authentication host-mode

To set the authorization manager mode on a port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication host-mode { **multi-auth** | **multi-domain** | **multi-host** | **single-host** }
no authentication host-mode

Syntax Description		
multi-auth	Enables multiple-authorization mode (multi-auth mode) on the port.	
multi-domain	Enables multiple-domain mode on the port.	
multi-host	Enables multiple-host mode on the port.	
single-host	Enables single-host mode on the port.	

Command Default Single host mode is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines Single-host mode should be configured if only one data host is connected. Do not connect a voice device to authenticate on a single-host port. Voice device authorization fails if no voice VLAN is configured on the port.

Multi-domain mode should be configured if data host is connected through an IP phone to the port. Multi-domain mode should be configured if the voice device needs to be authenticated.

Multi-auth mode should be configured to allow devices behind a hub to obtain secured port access through individual authentication. Only one voice device can be authenticated in this mode if a voice VLAN is configured.

Multi-host mode also offers port access for multiple hosts behind a hub, but multi-host mode gives unrestricted port access to the devices after the first user gets authenticated.

This example shows how to enable multi-auth mode on a port:

```
Device(config-if)# authentication host-mode multi-auth
```

This example shows how to enable multi-domain mode on a port:

```
Device(config-if)# authentication host-mode multi-domain
```

This example shows how to enable multi-host mode on a port:

```
Device(config-if)# authentication host-mode multi-host
```

This example shows how to enable single-host mode on a port:

```
Device(config-if)# authentication host-mode single-host
```

You can verify your settings by entering the **show authentication sessions interface** *interface* **details** privileged EXEC command.

authentication mac-move permit

To enable MAC move on a device, use the **authentication mac-move permit** command in global configuration mode. To disable MAC move, use the **no** form of this command.

authentication mac-move permit
no authentication mac-move permit

Syntax Description This command has no arguments or keywords.

Command Default MAC move is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines The command enables authenticated hosts to move between 802.1x-enabled ports on a device. For example, if there is a device between an authenticated host and port, and that host moves to another port, the authentication session is deleted from the first port, and the host is reauthenticated on the new port.

If MAC move is disabled, and an authenticated host moves to another port, it is not reauthenticated, and a violation error occurs.

MAC move is not supported on port-security enabled 802.1x ports. If MAC move is globally configured on the switch and a port security-enabled host moves to an 802.1x-enabled port, a violation error occurs.

This example shows how to enable MAC move on a device:

```
Device(config)# authentication mac-move permit
```

authentication priority

To add an authentication method to the port-priority list, use the **authentication priority** command in interface configuration mode. To return to the default, use the **no** form of this command.

```
authentication priority [dot1x | mab] {webauth}
no authentication priority [dot1x | mab] {webauth}
```

Syntax Description	dot1x	(Optional) Adds 802.1x to the order of authentication methods.
	mab	(Optional) Adds MAC authentication bypass (MAB) to the order of authentication methods.
	webauth	Adds web authentication to the order of authentication methods.

Command Default The default priority is 802.1x authentication, followed by MAC authentication bypass and web authentication.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines Ordering sets the order of methods that the switch attempts when trying to authenticate a new device is connected to a port.

When configuring multiple fallback methods on a port, set web authentication (webauth) last.

Assigning priorities to different authentication methods allows a higher-priority method to interrupt an in-progress authentication method with a lower priority.



Note If a client is already authenticated, it might be reauthenticated if an interruption from a higher-priority method occurs.

The default priority of an authentication method is equivalent to its position in execution-list order: 802.1x authentication, MAC authentication bypass (MAB), and web authentication. Use the **dot1x**, **mab**, and **webauth** keywords to change this default order.

This example shows how to set 802.1x as the first authentication method and web authentication as the second authentication method:

```
Device(config-if)# authentication priority dotx webauth
```

This example shows how to set MAB as the first authentication method and web authentication as the second authentication method:

```
Device(config-if) # authentication priority mab webauth
```

Related Commands	Command	Description
	authentication control-direction	Configures the port mode as unidirectional or bidirectional.
	authentication event fail	Specifies how the Auth Manager handles authentication failures as a result of unrecognized user credentials.
	authentication event no-response action	Specifies how the Auth Manager handles authentication failures as a result of a nonresponsive host.
	authentication event server alive action reinitialize	Reinitializes an authorized Auth Manager session when a previously unreachable authentication, authorization, and accounting server becomes available.
	authentication event server dead action authorize	Authorizes Auth Manager sessions when the authentication, authorization, and accounting server becomes unreachable.
	authentication fallback	Enables a web authentication fallback method.
	authentication host-mode	Allows hosts to gain access to a controlled port.
	authentication open	Enables open access on a port.
	authentication order	Specifies the order in which the Auth Manager attempts to authenticate a client on a port.
	authentication periodic	Enables automatic reauthentication on a port.
	authentication port-control	Configures the authorization state of a controlled port.
	authentication timer inactivity	Configures the time after which an inactive Auth Manager session is terminated.
	authentication timer reauthenticate	Specifies the period of time between which the Auth Manager attempts to reauthenticate authorized ports.
	authentication timer restart	Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port.
	authentication violation	Specifies the action to be taken when a security violation occurs on a port.
	mab	Enables MAC authentication bypass on a port.

Command	Description
show authentication registrations	Displays information about the authentication methods that are registered with the Auth Manager.
show authentication sessions	Displays information about current Auth Manager sessions.
show authentication sessions interface	Displays information about the Auth Manager for a given interface.

authentication violation

To configure the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port, use the **authentication violation** command in interface configuration mode.

```
authentication violation { protect | replace | restrict | shutdown }
no authentication violation { protect | replace | restrict | shutdown }
```

Syntax Description	Mode	Description
	protect	Drops unexpected incoming MAC addresses. No syslog errors are generated.
	replace	Removes the current session and initiates authentication with the new host.
	restrict	Generates a syslog error when a violation error occurs.
	shutdown	Error-disables the port or the virtual port on which an unexpected MAC address occurs.

Command Default Authentication violation shutdown mode is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines Use the **authentication violation** command to specify the action to be taken when a security violation occurs on a port.

This example shows how to configure an IEEE 802.1x-enabled port as error-disabled and to shut down when a new device connects it:

```
Device(config-if) # authentication violation shutdown
```

This example shows how to configure an 802.1x-enabled port to generate a system error message and to change the port to restricted mode when a new device connects to it:

```
Device(config-if) # authentication violation restrict
```

This example shows how to configure an 802.1x-enabled port to ignore a new device when it connects to the port:

```
Device(config-if) # authentication violation protect
```

This example shows how to configure an 802.1x-enabled port to remove the current session and initiate authentication with a new device when it connects to the port:

```
Device(config-if)# authentication violation replace
```

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

auto security

To configure global auto security, use the **auto security** command in global configuration mode. To disable auto security, use the **no** form of this command.

auto security
no auto security

This command has no arguments and keywords.

Command Default Auto security is enabled globally.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS Release 15.2(5)E	This command was introduced in a release prior to Cisco IOS Release 15.2(5)E.

Usage Guidelines When you configure auto security in global configuration mode, auto security is enabled on all interfaces. When you disable auto security, it is disabled on all interfaces.

To enable auto security on specific interfaces, use the **auto security-port** command in interface configuration mode.



Note In Cisco IOS Release 15.2(5)E, auto security is enabled on interfaces, when the **auto security** command is configured in global configuration mode; however, the **auto security-port {host |uplink}** command is not explicitly saved to the interface configuration. When auto security is configured on an interface, and then the **auto security-port {host |uplink}** command is removed from that interface; the **no auto security-port {host |uplink}** command is saved to interface configuration.

This example shows how to enable auto security globally:

```
Switch(config)# auto security
```

Related Commands	Command	Description
	auto security-port	Configures auto security on an interface.
	show auto security	Displays auto security status.

auto security-port

To configure auto security on an interface, use the **auto security-port** command in interface configuration mode. To disable auto security on an interface, use the **no** form of this command.

```
auto security {host | uplink}
no auto security
```

Syntax Description

host	Configures auto security for a host port.
uplink	Configures auto security for an uplink port.

Command Default

Auto security is disabled on all interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS Release 15.2(5)E	This command was introduced in a release prior to Cisco IOS Release 15.2(5)E.

Usage Guidelines

You can enable auto security globally, by using the **auto security** in global configuration mode.



Note

In Cisco IOS Release 15.2(5)E, auto security is enabled on interfaces, when the **auto security** command is configured in global configuration mode; however, the **auto security-port {host | uplink}** command is not explicitly saved to the interface configuration. When auto security is configured on an interface, and then the **auto security-port {host | uplink}** command is removed from that interface; the **no auto security-port {host | uplink}** command is saved to interface configuration.

The following example shows how to configure auto security on an interface:

```
Switch(config)# interface gigabitethernet 1/0/2
Switch(config-if)# auto security-port host
```

Related Commands

Command	Description
auto security	Configures global auto security.
show auto security	Displays auto security status.

cisp enable

To enable Client Information Signaling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch and a supplicant to an authenticator switch, use the **cisp enable** global configuration command.

cisp enable
no cisp enable

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was reintroduced. This command was not supported in and

Usage Guidelines The link between the authenticator and supplicant switch is a trunk. When you enable VTP on both switches, the VTP domain name must be the same, and the VTP mode must be server.

To avoid the MD5 checksum mismatch error when you configure VTP mode, verify that:

- VLANs are not configured on two different switches, which can be caused by two VTP servers in the same domain.
- Both switches have different configuration revision numbers.

This example shows how to enable CISP:

```
Device(config)# cisp enable
```

Related Commands	Command	Description
	dot1x credentials <i>profile</i>	Configures a profile on a supplicant switch.
	dot1x supplicant force-multicast	Forces 802.1X supplicant to send multicast packets.
	dot1x supplicant controlled transient	Configures controlled access by 802.1X supplicant.
	show cisp	Displays CISP information for a specified interface.

clear errdisable interface vlan

To reenable a VLAN that was error-disabled, use the **clear errdisable interface** command in privileged EXEC mode.

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

Syntax Description	<i>interface-id</i>	Specifies an interface.
	<i>vlan list</i>	(Optional) Specifies a list of VLANs to be reenabled. If a VLAN list is not specified, then all VLANs are reenabled.
Command Default	No default behavior or values.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines You can reenable 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.

This example shows how to reenable all VLANs that were error-disabled on Gigabit Ethernet port 4/0/2:

```
Device# clear errdisable interface gigabitethernet4/0/2 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	Displays error-disabled recovery timer information.
	show interfaces status err-disabled	Displays interface status of a list of interfaces in error-disabled state.

clear mac address-table

To delete from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, all dynamic addresses on stack members, or all dynamic addresses on a particular VLAN, use the **clear mac address-table** command in privileged EXEC mode. This command also clears the MAC address notification global counters.

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

Syntax Description		
dynamic		Deletes all dynamic MAC addresses.
address <i>mac-addr</i>		(Optional) Deletes the specified dynamic MAC address.
interface <i>interface-id</i>		(Optional) Deletes all dynamic MAC addresses on the specified physical port or port channel.
vlan <i>vlan-id</i>		(Optional) Deletes all dynamic MAC addresses for the specified VLAN. The range is 1 to 4094.
move update		Clears the MAC address table move-update counters.
notification		Clears the notifications in the history table and reset the counters.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

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

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

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

Related Commands	Command	Description
	mac address-table notification	Enables the MAC address notification feature.
	mac address-table move update { receive transmit }	Configures MAC address-table move update on the switch.

Command	Description
show mac address-table	Displays the MAC address table static and dynamic entries.
show mac address-table move update	Displays the MAC address-table move update information on the switch.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or on the specified interface when the interface keyword is appended.
snmp trap mac-notification change	Enables the SNMP MAC address notification trap on a specific interface.

debug ip rip

To display information on Routing Information Protocol (RIP) routing transactions, use the **debug ip rip** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip rip [{database | events | trigger}]
no debug ip rip [{database | events | trigger}]
```

Syntax Description

database	(Optional) Displays information about RIP database events.
events	(Optional) Displays information about RIP protocol-based events.
trigger	(Optional) Displays information about RIP trigger extensions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS Release 15.2(5)E2	This command was introduced.

Examples

In the following example, the router being debugged has received updates from a router at source address 10.89.80.28. In this scenario, information has been sent to about five destinations in the routing table update. Notice that the fourth destination address in the update, 172.31.0.0, is inaccessible because it is more than 15 hops away from the router from which the update was sent. The router being debugged also sends updates, in both cases to broadcast address 255.255.255.255 as the destination.

```
Device# debug ip rip

RIP: received update from 10.89.80.28 on GigabitEthernet0/0/0
 10.89.95.0 in 1 hops
 10.89.81.0 in 1 hops
 10.89.66.0 in 2 hops
 172.31.0.0 in 16 hops (inaccessible)
 0.0.0.0 in 7 hop
RIP: sending update to 255.255.255.255 via GigabitEthernet0/0/0 (10.89.64.31)
 subnet 10.89.94.0, metric 1
 172.31.0.0 in 16 hops (inaccessible)
RIP: sending update to 255.255.255.255 via Serial1 (10.89.94.31)
 subnet 10.89.64.0, metric 1
 subnet 10.89.66.0, metric 3
 172.31.0.0 in 16 hops (inaccessible)
 default 0.0.0.0, metric 8
```

The second line is an example of a routing table update. It shows the number of hops between a given Internet address and the device.

The entries show that the device is sending updates that are similar, except that the number in parentheses is the source address encapsulated into the IP header.

The following are examples for the **debug ip rip** command of entries that appear at startup, during an interface transition event, or when a user manually clears the routing table:

```
RIP: broadcasting general request on GigabitEthernet0/0/0  
RIP: broadcasting general request on GigabitEthernet1/0/0
```

The following entry is most likely caused by a malformed packet from the sender:

```
RIP: bad version 128 from 160.89.80.43
```

Related Commands

Command	Description
show ip rip database	Displays summary address entries in the RIP routing database entries if relevant are routes being summarized based upon a summary address.

deny (MAC access-list configuration)

To prevent non-IP traffic from being forwarded if the conditions are matched, use the **deny** MAC access-list configuration command on the switch stack or on a standalone switch. To remove a deny condition from the named MAC access list, use the **no** form of this command.

```
deny {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | larc-sca | lsap lsap mask | mop-console
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [cos cos]
no deny {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | larc-sca | lsap lsap mask | mop-console
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [cos cos]
```

Syntax Description

any	Denies any source or destination MAC address.
host <i>src-MAC-addr</i> <i>src-MAC-addr mask</i>	Defines a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
host <i>dst-MAC-addr</i> <i>dst-MAC-addr mask</i>	Defines a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
<i>type mask</i>	(Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. The type is 0 to 65535, specified in hexadecimal. The mask is a mask of don't care bits applied to the EtherType before testing for a match.
aarp	(Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	(Optional) Specifies EtherType DEC-Amber.
appletalk	(Optional) Specifies EtherType AppleTalk/EtherTalk.
dec-spanning	(Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	(Optional) Specifies EtherType DECnet Phase IV protocol.
diagnostic	(Optional) Specifies EtherType DEC-Diagnostic.

dsm	(Optional) Specifies EtherType DEC-DSM.
etype-6000	(Optional) Specifies EtherType 0x6000.
etype-8042	(Optional) Specifies EtherType 0x8042.
lat	(Optional) Specifies EtherType DEC-LAT.
lavr-sca	(Optional) Specifies EtherType DEC-LAVC-SCA.
lsap <i>lsap-number mask</i>	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. <i>mask</i> is a mask of don't care bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Specifies EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Specifies EtherType DEC-MOP Dump.
msdos	(Optional) Specifies EtherType DEC-MSDOS.
mumps	(Optional) Specifies EtherType DEC-MUMPS.
netbios	(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NetBIOS).
vines-echo	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Specifies EtherType VINES IP.
xns-idp	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary EtherType in decimal, hexadecimal, or octal.
cos <i>cos</i>	(Optional) Specifies a class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message reminds the user if the cos option is configured.

Command Default

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

Command Modes

Mac-access list configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

You enter MAC-access list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **host** keyword, you must enter an address mask.

When an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

To filter IPX traffic, you use the *type mask* or **lsap lsap mask** keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in the table.

Table 29: IPX Filtering Criteria

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	Novel Name	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

This example shows how to define the named MAC extended access list to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is denied.

```
Device(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

This example shows how to remove the deny condition from the named MAC extended access list:

```
Device(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

This example denies all packets with EtherType 0x4321:

```
Device(config-ext-macl)# deny any any 0x4321 0
```

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

Related Commands

Command	Description
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
permit	Permits from the MAC access-list configuration. Permits non-IP traffic to be forwarded if conditions are matched.

Command	Description
show access-lists	Displays access control lists configured on a switch.

device-role (IPv6 snooping)

To specify the role of the device attached to the port, use the **device-role** command in IPv6 snooping configuration mode.

```
device-role {node | switch}
```

Syntax Description	<p>node Sets the role of the attached device to node.</p> <p>switch Sets the role of the attached device to switch.</p>						
Command Default	The device role is node.						
Command Modes	IPv6 snooping configuration						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E</td> </tr> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E		This command was introduced.
Release	Modification						
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E						
	This command was introduced.						
Usage Guidelines	<p>The device-role command specifies the role of the device attached to the port. By default, the device role is node.</p> <p>The switch keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.</p> <p>This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the device as the node:</p> <pre>Device(config)# ipv6 snooping policy policy1 Device(config-ipv6-snooping)# device-role node</pre>						

device-role (IPv6 nd inspection)

To specify the role of the device attached to the port, use the **device-role** command in neighbor discovery (ND) inspection policy configuration mode.

device-role {**host** | **monitor** | **router** | **switch**}

Syntax Description	host	Sets the role of the attached device to host.
	monitor	Sets the role of the attached device to monitor.
	router	Sets the role of the attached device to router.
	switch	Sets the role of the attached device to switch.

Command Default The device role is host.

Command Modes ND inspection policy configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines The **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is enabled using the **router** keyword, all messages (router solicitation [RS], router advertisement [RA], or redirect) are allowed on this port.

When the **router** or **monitor** keyword is used, the multicast RS messages are bridged on the port, regardless of whether limited broadcast is enabled. However, the monitor keyword does not allow inbound RA or redirect messages. When the monitor keyword is used, devices that need these messages will receive them.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:

```
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# device-role host
```


device-tracking policy

To configure a Switch Integrated Security Features (SISF)-based IP device tracking policy, use the **device-tracking** command in global configuration mode. To delete a device tracking policy, use the **no** form of this command.

device-tracking policy *policy-name*
no device-tracking policy *policy-name*

Syntax Description	<i>policy-name</i> User-defined name of the device tracking policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).				
Command Default	A device tracking policy is not configured.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification		This command was introduced.
Release	Modification				
	This command was introduced.				

Usage Guidelines Use the SISF-based **device-tracking policy** command to create a device tracking policy. When the **device-tracking policy** command is enabled, the configuration mode changes to device-tracking configuration mode. In this mode, the administrator can configure the following first-hop security commands:

- (Optional) **device-role** {**node** | **switch**}—Specifies the role of the device attached to the port. Default is **node**.
- (Optional) **limit address-count** *value*—Limits the number of addresses allowed per target.
- (Optional) **no**—Negates a command or sets it to defaults.
- (Optional) **destination-glean** {**recovery** | **log-only**} [**dhcp**]}—Enables binding table recovery by data traffic source address gleaning.
- (Optional) **data-glean** {**recovery** | **log-only**} [**dhcp** | **ndp**]}—Enables binding table recovery using source or data address gleaning.
- (Optional) **security-level** {**glean** | **guard** | **inspect**}—Specifies the level of security enforced by the feature. Default is **guard**.
 - glean**—Gleans addresses from messages and populates the binding table without any verification.
 - guard**—Gleans addresses and inspects messages. In addition, it rejects RA and DHCP server messages. This is the default option.
 - inspect**—Gleans addresses, validates messages for consistency and conformance, and enforces address ownership.
- (Optional) **tracking** {**disable** | **enable**}—Specifies a tracking option.
- (Optional) **trusted-port**—Sets up a trusted port. It disables the guard on applicable targets. Bindings learned through a trusted port have preference over bindings learned through any other port. A trusted port is given preference in case of a collision while making an entry in the table.

This example shows how to configure an a device-tracking policy:

```
Device(config)# device-tracking policy policy1  
Device(config-device-tracking)# trusted-port
```

dot1x critical (global configuration)

To configure the IEEE 802.1X critical authentication parameters, use the **dot1x critical** command in global configuration mode.

dot1x critical eapol

Syntax Description	eapol Specifies that the switch send an EAPOL-Success message when the switch successfully authenticates the critical port.				
Command Default	eapol is disabled				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.				

This example shows how to specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port:

```
Device(config)# dot1x critical eapol
```

dot1x pae

To set the Port Access Entity (PAE) type, use the **dot1x pae** command in interface configuration mode. To disable the PAE type that was set, use the **no** form of this command.

```
dot1x pae {supplicant | authenticator}
no dot1x pae {supplicant | authenticator}
```

Syntax Description	supplicant The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.										
	authenticator The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.										
Command Default	PAE type is not set.										
Command Modes	Interface configuration										
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E</td> </tr> <tr> <td></td> <td>This command was introduced.</td> </tr> <tr> <td></td> <td>This command was reintroduced.</td> </tr> <tr> <td></td> <td>This command was not supported in and</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E		This command was introduced.		This command was reintroduced.		This command was not supported in and
Release	Modification										
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E										
	This command was introduced.										
	This command was reintroduced.										
	This command was not supported in and										
Usage Guidelines	<p>Use the no dot1x pae interface configuration command to disable IEEE 802.1x authentication on the port.</p> <p>When you configure IEEE 802.1x authentication on a port, such as by entering the dot1x port-control interface configuration command, the switch automatically configures the port as an IEEE 802.1x authenticator. After the no dot1x pae interface configuration command is entered, the Authenticator PAE operation is disabled.</p> <p>The following example shows that the interface has been set to act as a supplicant:</p> <pre>Device(config)# interface g1/0/3 Device(config-if)# dot1x pae supplicant</pre>										

dot1x supplicant force-multicast

To force a supplicant switch to send only multicast Extensible Authentication Protocol over LAN (EAPOL) packets whenever it receives multicast or unicast EAPOL packets, use the **dot1x supplicant force-multicast** command in global configuration mode. To return to the default setting, use the **no** form of this command.

dot1x supplicant force-multicast
no dot1x supplicant force-multicast

Syntax Description

This command has no arguments or keywords.

Command Default

The supplicant switch sends unicast EAPOL packets when it receives unicast EAPOL packets. Similarly, it sends multicast EAPOL packets when it receives multicast EAPOL packets.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	This command was introduced.
Cisco IOS Release 15.2(5)E	This command was reintroduced. This command was not supported in and

Usage Guidelines

Enable this command on the supplicant switch for Network Edge Access Topology (NEAT) to work in all host modes.

This example shows how force a supplicant switch to send multicast EAPOL packets to the authenticator switch:

```
Device(config)# dot1x supplicant force-multicast
```

Related Commands

Command	Description
cisp enable	Enable Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch.
dot1x credentials	Configure the 802.1x supplicant credentials on the port.
dot1x pae supplicant	Configure an interface to act only as a supplicant.

dot1x test eapol-capable

To monitor IEEE 802.1x activity on all the switch ports and to display information about the devices that are connected to the ports that support IEEE 802.1x, use the **dot1x test eapol-capable** command in privileged EXEC mode on the switch stack or on a standalone switch.

dot1x test eapol-capable [**interface** *interface-id*]

Syntax Description	interface <i>interface-id</i>	(Optional) Port to be queried.
Command Default	There is no default setting.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines Use this command to test the IEEE 802.1x capability of the devices connected to all ports or to specific ports on a switch.

There is not a no form of this command.

This example shows how to enable the IEEE 802.1x readiness check on a switch to query a port. It also shows the response received from the queried port verifying that the device connected to it is IEEE 802.1x-capable:

```
Device# dot1x test eapol-capable interface gigabitethernet1/0/13
```

```
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable
```

Related Commands	Command	Description
	dot1x test timeout <i>timeout</i>	Configures the timeout used to wait for EAPOL response to an IEEE 802.1x readiness query.

dot1x test timeout

To configure the timeout used to wait for EAPOL response from a port being queried for IEEE 802.1x readiness, use the **dot1x test timeout** command in global configuration mode on the switch stack or on a standalone switch.

dot1x test timeout *timeout*

Syntax Description	<i>timeout</i>	Time in seconds to wait for an EAPOL response. The range is from 1 to 65535 seconds.
---------------------------	----------------	--

Command Default The default setting is 10 seconds.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines Use this command to configure the timeout used to wait for EAPOL response.

There is not a no form of this command.

This example shows how to configure the switch to wait 27 seconds for an EAPOL response:

```
Device# dot1x test timeout 27
```

You can verify the timeout configuration status by entering the **show run** privileged EXEC command.

Related Commands	Command	Description
	dot1x test eapol-capable [<i>interface interface-id</i>]	Checks for IEEE 802.1x readiness on devices connected to all or to specified IEEE 802.1x-capable ports.

dot1x timeout

To configure the value for retry timeouts, use the **dot1x timeout** command in global configuration or interface configuration mode. To return to the default value for retry timeouts, use the **no** form of this command.

dot1x timeout {**auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds*}

Syntax Description		
auth-period <i>seconds</i>		Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). The range is from 1 to 65535. The default is 30.
held-period <i>seconds</i>		Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). The range is from 1 to 65535. The default is 60
quiet-period <i>seconds</i>		Configures the time, in seconds, that the authenticator (server) remains quiet (in the HELD state) following a failed authentication exchange before trying to reauthenticate the client. The range is from 1 to 65535. The default is 60
ratelimit-period <i>seconds</i>		Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of switch processing power). <ul style="list-style-type: none"> • The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration. • The range is from 1 to 65535. By default, rate limiting is disabled.
server-timeout <i>seconds</i>		Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. <ul style="list-style-type: none"> • The range is from 1 to 65535. The default is 30. <p>If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.</p>
start-period <i>seconds</i>		Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. The range is from 1 to 65535. The default is 30. In Cisco IOS Release 15.2(5)E, this command is only available in the supplicant mode. If the command is applied in any other mode, the command misses from the configuration.

supp-timeout <i>seconds</i>	Sets the authenticator-to-supplicant retransmission time for all EAP messages other than EAP Request ID. The range is from 1 to 65535. The default is 30.
tx-period <i>seconds</i>	Configures the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client. <ul style="list-style-type: none"> The range is from 1 to 65535. The default is 30. If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.

Command Default Periodic reauthentication and periodic rate-limiting are done.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The **dot1x timeout reauth-period** interface configuration command affects the behavior of the switch only if you have enabled periodic re-authentication by using the **dot1x reauthentication** interface configuration command.

During the quiet period, the switch does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a number smaller than the default.

When the **ratelimit-period** is set to 0 (the default), the switch does not ignore EAPOL packets from clients that have been successfully authenticated and forwards them to the RADIUS server.

The following example shows that various 802.1X retransmission and timeout periods have been set:

```
Device(config)# configure terminal
Device(config)# interface g1/0/3
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x timeout auth-period 2000
Device(config-if)# dot1x timeout held-period 2400
Device(config-if)# dot1x timeout quiet-period 600
Device(config-if)# dot1x timeout start-period 90
Device(config-if)# dot1x timeout supp-timeout 300
Device(config-if)# dot1x timeout tx-period 60
Device(config-if)# dot1x timeout server-timeout 60
```

epm access-control open

To configure an open directive for ports that do not have an access control list (ACL) configured, use the **epm access-control open** command in global configuration mode. To disable the open directive, use the **no** form of this command.

epm access-control open
no epm access-control open

Syntax Description This command has no arguments or keywords.

Command Default The default directive applies.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	This command was introduced.
	Cisco IOS Release 15.2(5)E	

Usage Guidelines Use this command to configure an open directive that allows hosts without an authorization policy to access ports configured with a static ACL. If you do not configure this command, the port applies the policies of the configured ACL to the traffic. If no static ACL is configured on a port, both the default and open directives allow access to the port.

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

This example shows how to configure an open directive.

```
Device(config)# epm access-control open
```

Related Commands	Command	Description
	show running-config	Displays the contents of the current running configuration file.

ip admission

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

ip admission *rule*
no ip admission *rule*

Syntax Description *rule* IP admission rule name.

Command Default Web authentication is disabled.

Command Modes Interface configuration
 Fallback-profile configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

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

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

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip admission rule1
```

This example shows how to apply a web authentication rule to a fallback profile for use on an IEEE 802.1x enabled switch port.

```
Device# configure terminal
Device(config)# fallback profile profile1
Device(config-fallback-profile)# ip admission rule1
```

ip admission name

To enable web authentication, use the **ip admission name** command in global configuration mode. To disable web authentication, use the **no** form of this command.

ip admission name *name* { **consent** | **proxy http** } [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** { *acl* | *acl-name* } | **service-policy type tag** *service-policy-name*]
no ip admission name *name* { **consent** | **proxy http** } [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** { *acl* | *acl-name* } | **service-policy type tag** *service-policy-name*]

Syntax Description

<i>name</i>	Name of network admission control rule.
consent	Associates an authentication proxy consent web page with the IP admission rule specified using the <i>admission-name</i> argument.
proxy http	Configures web authentication custom page.
absolute-timer <i>minutes</i>	(Optional) Elapsed time, in minutes, before the external server times out.
inactivity-time <i>minutes</i>	(Optional) Elapsed time, in minutes, before the external file server is deemed unreachable.
list	(Optional) Associates the named rule with an access control list (ACL).
<i>acl</i>	Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199, or from 1300 through 2699 for expanded range.
<i>acl-name</i>	Applies a named access list to a named admission control rule.
service-policy type tag	(Optional) A control plane service policy is to be configured.
<i>service-policy-name</i>	Control plane tag service policy that is configured using the policy-map type control tag <i>polycyname</i> command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received.

Command Default

Web authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

The **ip admission name** 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 switch port:

```
Device# configure terminal
Device(config) ip admission name http-rule proxy http
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 101 in
Device(config-if)# ip admission rule
Device(config-if)# end
```

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback mechanism on a switch port:

```
Device# configure terminal
Device(config)# ip admission name rule2 proxy http
Device(config)# fallback profile profile1
Device(config)# ip access group 101 in
Device(config)# ip admission name rule2
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x fallback profile1
Device(config-if)# end
```

Related Commands

Command	Description
dot1x fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
fallback profile	Creates a web authentication fallback profile.
ip admission	Enables web authentication on a port.
show authentication sessions interface <i>interface</i> detail	Displays information about the web authentication session status.
show ip admission	Displays information about NAC cached entries or the NAC configuration.

ip device tracking maximum

To configure IP device tracking parameters on a Layer 2 access port, use the **ip device tracking maximum** command in interface configuration mode. To remove the maximum value, use the **no** form of the command.

ip device tracking maximum *number*
no ip device tracking maximum

Syntax Description	<i>number</i> Number of bindings created in the IP device tracking table for a port. The range is 0 (disabled) to 65535.						
Command Default	None						
Command Modes	Interface configuration mode						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E</td> </tr> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E		This command was introduced.
Release	Modification						
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E						
	This command was introduced.						

Usage Guidelines

To remove the maximum value, use the **no ip device tracking maximum** command.

To disable IP device tracking, use the **ip device tracking maximum 0** command.



Note This command enables IPDT wherever its configured

Examples

This example shows how to configure IP device tracking parameters on a Layer 2 access port:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip device tracking
Device(config)# interface gigabitethernet1/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 1
Device(config-if)# ip device tracking maximum 5
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
Device(config-if)# end
```

ip device tracking probe

To configure the IP device tracking table for Address Resolution Protocol (ARP) probes, use the **ip device tracking probe** command in global configuration mode. To disable ARP probes, use the **no** form of this command.

```
ip device tracking probe {count number | delay seconds | interval seconds | use-svi address}
no ip device tracking probe {count number | delay seconds | interval seconds | use-svi address}
```

Syntax Description	
count <i>number</i>	Sets the number of times that the device sends the ARP probe. The range is from 1 to 255.
delay <i>seconds</i>	Sets the number of seconds that the device waits before sending the ARP probe. The range is from 1 to 120.
interval <i>seconds</i>	Sets the number of seconds that the device waits for a response before resending the ARP probe. The range is from 30 to 1814400 seconds.
use-svi	Uses the switch virtual interface (SVI) IP address as source of ARP probes.

Command Default	
	The count number is 3.
	There is no delay.
	The interval is 30 seconds.
	The ARP probe default source IP address is the Layer 3 interface and 0.0.0.0 for switchports.

Command Modes	
	Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines	
	Use the use-svi keyword to configure the IP device tracking table to use the SVI IP address for ARP probes in cases when the default source IP address 0.0.0.0 for switch ports is used and the ARP probes drop.

Examples	
	This example shows how to set SVI as the source for ARP probes:

```
Device(config)# ip device tracking probe use-svi
```

ip dhcp snooping database

To configure the Dynamic Host Configuration Protocol (DHCP)-snooping database, use the **ip dhcp snooping database** command in global configuration mode. To disable the DHCP-snooping database, use the **no** form of this command.

```
ip dhcp snooping database {flash:url | flash1:url | ftp:url | http:url | https:url | rcp:url |
scp:url | tftp:url | timeout seconds | write-delay seconds}
no ip dhcp snooping database [ timeout | write-delay ]
```

Syntax Description		
	flash1:url	Specifies the database URL for storing entries using flash.
	flash:url	Specifies the database URL for storing entries using flash.
	ftp:url	Specifies the database URL for storing entries using FTP.
	http:url	Specifies the database URL for storing entries using HTTP.
	https:url	Specifies the database URL for storing entries using secure HTTP (https).
	rcp:url	Specifies the database URL for storing entries using remote copy (rcp).
	scp:url	Specifies the database URL for storing entries using Secure Copy (SCP).
	tftp:url	Specifies the database URL for storing entries using TFTP.
	timeout <i>seconds</i>	Specifies the timeout interval; valid values are from 0 to 86400 seconds.
	write-delay <i>seconds</i>	Specifies the amount of time before writing the DHCP-snooping entries to an external server after a change is seen in the local DHCP-snooping database; valid values are from 15 to 86400 seconds.

Command Default The DHCP-snooping database is not configured.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

You must enable DHCP snooping on the interface before entering this command. Use the **ip dhcp snooping** command to enable DHCP snooping.

This example shows how to specify the database URL using TFTP:

```
Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```


This example shows how to specify the amount of time before writing DHCP snooping entries to an external server:

```
Device(config)# ip dhcp snooping database write-delay 15
```

ip dhcp snooping information option format remote-id

To configure the option-82 remote-ID suboption, use the **ip dhcp snooping information option format remote-id** command in global configuration mode on the switch to configure the option-82 remote-ID suboption. To configure the default remote-ID suboption, use the **no** form of this command.

```
ip dhcp snooping information option format remote-id {hostname | string string}
no ip dhcp snooping information option format remote-id {hostname | string string}
```

Syntax Description	hostname Specify the switch hostname as the remote ID.				
	string <i>string</i> Specify a remote ID, using from 1 to 63 ASCII characters (no spaces).				
Command Default	The switch MAC address is the remote ID.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.				
Usage Guidelines	<p>You must globally enable DHCP snooping by using the ip dhcp snooping global configuration command for any DHCP snooping configuration to take effect.</p> <p>When the option-82 feature is enabled, the default remote-ID suboption is the switch MAC address. This command allows you to configure either the switch hostname or a string of up to 63 ASCII characters (but no spaces) to be the remote ID.</p>				
 Note	If the hostname exceeds 63 characters, it will be truncated to 63 characters in the remote-ID configuration.				

This example shows how to configure the option- 82 remote-ID suboption:

```
Device(config)# ip dhcp snooping information option format remote-id hostname
```

ip dhcp snooping verify no-relay-agent-address

To disable the DHCP snooping feature from verifying that the relay agent address (giaddr) in a DHCP client message matches the client hardware address on an untrusted port, use the **ip dhcp snooping verify no-relay-agent-address** command in global configuration mode. To enable verification, use the **no** form of this command.

ip dhcp snooping verify no-relay-agent-address
no ip dhcp snooping verify no-relay-agent-address

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

By default, the DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0; the message is dropped if the giaddr field is not 0. Use the **ip dhcp snooping verify no-relay-agent-address** command to disable the verification. Use the **no ip dhcp snooping verify no-relay-agent-address** to reenables verification.

This example shows how to enable verification of the giaddr in a DHCP client message:

```
Device(config)# no ip dhcp snooping verify no-relay-agent-address
```

ip source binding

To add a static IP source binding entry, use the **ip source binding** command. Use the **no** form of this command to delete a static IP source binding entry.

ip source binding *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*
no ip source binding *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*

Syntax Description		
	<i>mac-address</i>	Binding MAC address.
	vlan <i>vlan-id</i>	Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
	<i>ip-address</i>	Binding IP address.
	interface <i>interface-id</i>	ID of the physical interface.
Command Default	No IP source bindings are configured.	
Command Modes	Global configuration.	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

You can use this command to add a static IP source binding entry only.

The **no** format deletes the corresponding IP source binding entry. It requires the exact match of all required parameter in order for the deletion to be successful. Note that each static IP binding entry is keyed by a MAC address and a VLAN number. If the command contains the existing MAC address and VLAN number, the existing binding entry is updated with the new parameters instead of creating a separate binding entry.

This example shows how to add a static IP source binding entry:

```
Device# configure terminal
Device(config) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1
```

ip verify source

To enable IP source guard on an interface, use the **ip verify source** command in interface configuration mode. To disable IP source guard, use the **no** form of this command.

ip verify source [**port-security**]
no ip verify source

port-security	(Optional) Enables IP source guard with IP and MAC address filtering. If you do not enter the port-security keyword, IP source guard with IP address filtering is enabled.
----------------------	--

Command Default IP source guard is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines To enable IP source guard with source IP address filtering, use the **ip verify source** interface configuration command.

To enable IP source guard with source IP and MAC address filtering, use the **ip verify source port-security** interface configuration command.

Examples

This example shows how to enable IP source guard with source IP address filtering on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
```

This example shows how to enable IP source guard with source IP and MAC address filtering:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source port-security

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip dhcp snooping
Device(config)# ip dhcp snooping vlan 10 20
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport trunk encapsulation dot1q
Device(config-if)# switchport mode trunk
Device(config-if)# switchport trunk native vlan 10
Device(config-if)# switchport trunk allowed vlan 11-20
Device(config-if)# no ip dhcp snooping trust
Device(config-if)# ip verify source vlan dhcp-snooping
Device(config)# end
Device# show ip verify source interface fastethernet0/1
```

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
-----	-----	-----	-----	-----	-----
Gil/0/1	ip-mac	active	10.0.0.1		10
Gil/0/1	ip-mac	active	deny-all		11-20

Device#

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip device tracking
Device(config)# interface gigabitethernet1/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 1
Device(config-if)# ip device tracking maximum 5
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
Device(config-if)# ip verify source tracking port-security
Device(config-if)# end
```

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

ipv6 snooping policy



Note All existing IPv6 Snooping commands (prior to) now have corresponding SISP-based device-tracking commands that allow you to apply your configuration to both IPv4 and IPv6 address families. For more information, see [device-tracking policy](#)

To configure an IPv6 snooping policy and enter IPv6 snooping configuration mode, use the **ipv6 snooping policy** command in global configuration mode. To delete an IPv6 snooping policy, use the **no** form of this command.

ipv6 snooping policy *snooping-policy*
no ipv6 snooping policy *snooping-policy*

Syntax Description	<i>snooping-policy</i> User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).
---------------------------	--

Command Default	An IPv6 snooping policy is not configured.
------------------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines Use the **ipv6 snooping policy** command to create an IPv6 snooping policy. When the **ipv6 snooping policy** command is enabled, the configuration mode changes to IPv6 snooping configuration mode. In this mode, the administrator can configure the following IPv6 first-hop security commands:

- The **device-role** command specifies the role of the device attached to the port.
- The **limit address-count** *maximum* command limits the number of IPv6 addresses allowed to be used on the port.
- The **protocol** command specifies that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP).
- The **security-level** command specifies the level of security enforced.
- The **tracking** command overrides the default tracking policy on a port.
- The **trusted-port** command configures a port to become a trusted port; that is, limited or no verification is performed when messages are received.

This example shows how to configure an IPv6 snooping policy:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)#
```

limit address-count

To limit the number of IPv6 addresses allowed to be used on the port, use the **limit address-count** command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode or IPv6 snooping configuration mode. To return to the default, use the **no** form of this command.

limit address-count *maximum*
no limit address-count

Syntax Description	<i>maximum</i> The number of addresses allowed on the port. The range is from 1 to 10000.
---------------------------	---

Command Default	The default is no limit.
------------------------	--------------------------

Command Modes	ND inspection policy configuration IPv6 snooping configuration
----------------------	---

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines	The limit address-count command limits the number of IPv6 addresses allowed to be used on the port on which the policy is applied. Limiting the number of IPv6 addresses on a port helps limit the binding table size. The range is from 1 to 10000.
-------------------------	---

This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and limit the number of IPv6 addresses allowed on the port to 25:

```
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# limit address-count 25
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and limit the number of IPv6 addresses allowed on the port to 25:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# limit address-count 25
```


mab request format attribute 32

To enable VLAN ID-based MAC authentication on a switch, use the **mab request format attribute 32 vlan access-vlan** command in global configuration mode. To return to the default setting, use the **no** form of this command.

mab request format attribute 32 vlan access-vlan
no mab request format attribute 32 vlan access-vlan

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN-ID based MAC authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	This command was introduced.

Usage Guidelines

Use this command to allow a RADIUS server to authenticate a new user based on the host MAC address and VLAN.

Use this feature on networks with the Microsoft IAS RADIUS server. The Cisco ACS ignores this command.

This example shows how to enable VLAN-ID based MAC authentication on a switch:

```
Device(config)# mab request format attribute 32 vlan access-vlan
```

Related Commands

Command	Description
authentication event	Sets the action for specific authentication events.
authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.
authentication order	Sets the order of authentication methods used on a port.
authentication periodic	Enables or disables reauthentication on a port.
authentication port-control	Enables manual control of the port authorization state.
authentication priority	Adds an authentication method to the port-priority list.

Command	Description
authentication timer	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
authentication violation	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port with the maximum number of devices already connected to that port.
mab	Enables MAC-based authentication on a port.
mab eap	Configures a port to use the Extensible Authentication Protocol (EAP).
show authentication	Displays information about authentication manager events on the switch.

match (access-map configuration)

To set the VLAN map to match packets against one or more access lists, use the **match** command in access-map configuration mode on the switch stack or on a standalone switch. To remove the match parameters, use the **no** form of this command.

```
match {ip address {namenumber} [{namenumber}] [{namenumber}]... | ipv6 address {namenumber}
[namenumber] [{namenumber}]... | mac address {name} [{name}] [{name}]...}
no match {ip address {namenumber} [{namenumber}] [{namenumber}]... | ipv6 address
{namenumber} [{namenumber}] [{namenumber}]... | mac address {name} [{name}] [{name}]...}
```

Syntax Description	
ip address	Sets the access map to match packets against an IP address access list.
ipv6 address	Sets the access map to match packets against an IPv6 address access list.
mac address	Sets the access map to match packets against a MAC address access list.
<i>name</i>	Name of the access list to match packets against.
<i>number</i>	Number of the access list to match packets against. This option is not valid for MAC access lists.

Command Default The default action is to have no match parameters applied to a VLAN map.

Command Modes Access-map configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines You enter access-map configuration mode by using the **vlan access-map** global configuration command. You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, IPv6 packets are matched against IPv6 access lists, and all other packets are matched against MAC access lists.

IP, IPv6, and MAC addresses can be specified for the same map entry.

This example shows how to define and apply a VLAN access map vmap4 to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list al2:

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address al2
Device(config-access-map)# action drop
```

```
Device(config-access-map) # exit  
Device(config) # vlan filter vmap4 vlan-list 5-6
```

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

Related Topics

[vlan access-map](#), on page 535

mls qos copp protocol

To protect the switch's control plane, use the **mls qos protocol** command in global configuration mode. To return to the default settings, use the **no** form of this command.

```
mls qos copp protocol {protocol-name} police {pps | bps} police rate  
no mls qos copp protocol {protocol-name} police
```

Syntax Description

Names of protocols for policing.

protocol-name

The following are the protocol names:

autorp-announce

autorp-discovery

bgp

cdp

cgmp

dai

dhcp-snoop-client-to-server

dhcp-snoop-server-to-client

dhcpv6-client-to-server

dhcpv6-server-to-client

eigrp

eigrp-v6

energy-wise

igmp-gs-query

igmp-leave

igmp-query

igmp-report

igrp

ipv6-pimv2

lldp

mld-gs-query

mld-leave

mld-query

mld-report

ndp-redirect

ndp-router-advertisement

ndp-router-solicitation

ospf

ospf-v6

pimv1

pxe

rep-hfl

reserve-multicast-group

rip

rip-v6

rsvp-snoop

stp

police *pps* | *bps* Indicates the type of policing required for a specific protocol. It can be packets per second (pps) or bit per second (bps).

police *rate* Specifies the rate limit for pps or bps for policing. The range for bps is 8000 to 2000000000 and pps is 100 to 100000.

Command Default Policer is disabled.

Command Modes Global configuration.

Command History

Release	Modification
Cisco IOS 15.2.4E	This command was introduced.

Usage Guidelines

Use this command to enable control-plane policer (CoPP) for a specific protocol. The police rate should be specified either as packets per second (PPS) or Bit per second (BPS).

This example shows how to enable control-plane policer (CoPP) for a specific protocol:

```
Device(config)# mls qos copp protocol cdp police bps 10000
```

Related Commands

Command	Description
show mls qos copp protocols	Displays the CoPP parameters and counters for all the configured protocol.

authentication logging verbose

To filter detailed information from authentication system messages, use the **authentication logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

authentication logging verbose
no authentication logging verbose

Syntax Description This command has no arguments or keywords.

Command Default Detailed logging of system messages is not enabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines This command filters details, such as anticipated success, from authentication system messages. Failure messages are not filtered.

To filter verbose authentication system messages:

```
Device(config)# authentication logging verbose
```

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

Related Commands	Command	Description
	authentication logging verbose	Filters details from authentication system messages.
	dot1x logging verbose	Filters details from 802.1x system messages.
	mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

dot1x logging verbose

To filter detailed information from 802.1x system messages, use the **dot1x logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

dot1x logging verbose
no dot1x logging verbose

Syntax Description This command has no arguments or keywords.

Command Default Detailed logging of system messages is not enabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines This command filters details, such as anticipated success, from 802.1x system messages. Failure messages are not filtered.

To filter verbose 802.1x system messages:

```
Device(config)# dot1x logging verbose
```

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

Related Commands	Command	Description
	authentication logging verbose	Filters details from authentication system messages.
	dot1x logging verbose	Filters details from 802.1x system messages.
	mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

mab logging verbose

To filter detailed information from MAC authentication bypass (MAB) system messages, use the **mab logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

mab logging verbose
no mab logging verbose

Syntax Description This command has no arguments or keywords.

Command Default Detailed logging of system messages is not enabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines This command filters details, such as anticipated success, from MAC authentication bypass (MAB) system messages. Failure messages are not filtered.

To filter verbose MAB system messages:

```
Device(config)# mab logging verbose
```

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

Related Commands	Command	Description
	authentication logging verbose	Filters details from authentication system messages.
	dot1x logging verbose	Filters details from 802.1x system messages.
	mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

permit (MAC access-list configuration)

To allow non-IP traffic to be forwarded if the conditions are matched, use the **permit** MAC access-list configuration command on the switch stack or on a standalone switch. To remove a permit condition from the extended MAC access list, use the **no** form of this command.

```
{permit {any | hostsrc-MAC-addr | src-MAC-addr mask} {any | hostdst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | larc-sca | lsaplsap mask | mop-console
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [coscos]
nopermit {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | larc-sca | lsap lsap mask | mop-console
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [coscos]
```

Syntax Description

any	Denies any source or destination MAC address.
host <i>src-MAC-addr</i> <i>src-MAC-addr mask</i>	Specifies a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
host <i>dst-MAC-addr</i> <i>dst-MAC-addr mask</i>	Specifies a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
<i>type mask</i>	(Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. <ul style="list-style-type: none"> <i>type</i> is 0 to 65535, specified in hexadecimal. <i>mask</i> is a mask of don't care bits applied to the EtherType before testing for a match.
aarp	(Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	(Optional) Specifies EtherType DEC-Amber.
appletalk	(Optional) Specifies EtherType AppleTalk/EtherTalk.
dec-spanning	(Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	(Optional) Specifies EtherType DECnet Phase IV protocol.
diagnostic	(Optional) Specifies EtherType DEC-Diagnostic.

dsm	(Optional) Specifies EtherType DEC-DSM.
etype-6000	(Optional) Specifies EtherType 0x6000.
etype-8042	(Optional) Specifies EtherType 0x8042.
lat	(Optional) Specifies EtherType DEC-LAT.
lavc-sca	(Optional) Specifies EtherType DEC-LAVC-SCA.
lsap <i>lsap-number mask</i>	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. The <i>mask</i> is a mask of don't care bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Specifies EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Specifies EtherType DEC-MOP Dump.
msdos	(Optional) Specifies EtherType DEC-MSDOS.
mumps	(Optional) Specifies EtherType DEC-MUMPS.
netbios	(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NetBIOS).
vines-echo	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Specifies EtherType VINES IP.
xns-idp	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite.
cos <i>cos</i>	(Optional) Specifies an arbitrary class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message appears if the cos option is configured.

Command Default

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

Command Modes

Mac-access list configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

You enter MAC access-list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **any** or **host** keywords, you must enter an address mask.

After an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

To filter IPX traffic, you use the *type mask* or **lsap lsap mask** keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in the following table.

Table 30: IPX Filtering Criteria

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	Novell Name	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

This example shows how to define the MAC-named extended access list to allow NetBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is allowed.

```
Device(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

This example shows how to remove the permit condition from the MAC-named extended access list:

```
Device(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

This example permits all packets with EtherType 0x4321:

```
Device(config-ext-macl)# permit any any 0x4321 0
```

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

Related Commands

Command	Description
deny	Denies from the MAC access-list configuration. Denies non-IP traffic to be forwarded if conditions are matched.
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.

Command	Description
show access-lists	Displays access control lists configured on a switch.

protocol (IPv6 snooping)

To specify that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP), or to associate the protocol with an IPv6 prefix list, use the **protocol** command. To disable address gleaning with DHCP or NDP, use the **no** form of the command.

```
protocol { dhcp | ndp }
no protocol { dhcp | ndp }
```

Syntax Description	dhcp Specifies that addresses should be gleaned in Dynamic Host Configuration Protocol (DHCP) packets.						
	ndp Specifies that addresses should be gleaned in Neighbor Discovery Protocol (NDP) packets.						
Command Default	Snooping and recovery are attempted using both DHCP and NDP.						
Command Modes	IPv6 snooping configuration mode						
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Release</th> <th style="text-align: left;">Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E</td> </tr> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E		This command was introduced.
Release	Modification						
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E						
	This command was introduced.						

Usage Guidelines

If an address does not match the prefix list associated with DHCP or NDP, then control packets will be dropped and recovery of the binding table entry will not be attempted with that protocol.

- Using the **no protocol** { **dhcp** | **ndp** } command indicates that a protocol will not be used for snooping or gleaning.
- If the **no protocol dhcp** command is used, DHCP can still be used for binding table recovery.
- Data glean can recover with DHCP and NDP, though destination guard will only recovery through DHCP.

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to use DHCP to glean addresses:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# protocol dhcp
```


radius server



Note Starting from Cisco IOS 15.2(5)E release, the **radius server** command replaces the **radius-server host** command, being used in releases prior to Cisco IOS Release 15.2(5)E. The old command has been deprecated.

Use the **radius server** configuration sub-mode command on the switch stack or on a standalone switch 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 name
address {ipv4 | ipv6} ip{address / hostname} auth-port udp-port acct-port udp-port
key string
automate tester name | retransmit value | timeout seconds
no radius server name
```

Syntax Description

address { ipv4 ipv6 } <i>ip{address / hostname}</i>	Specify the IP address of the RADIUS server.
auth-port <i>udp-port</i>	(Optional) Specify the UDP port for the RADIUS authentication server. The range is from 0 to 65536.
acct-port <i>udp-port</i>	(Optional) Specify the UDP port for the RADIUS accounting server. The range is from 0 to 65536.
key <i>string</i>	(Optional) Specify the authentication and encryption key for all RADIUS communication between the switch and the RADIUS daemon. Note 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.
automate tester <i>name</i>	(Optional) Enable automatic server testing of the RADIUS server status, and specify the username to be used.
retransmit <i>value</i>	(Optional) Specifies the number of times a RADIUS request is resent when the server is not responding or responding slowly. The range is 1 to 100. This setting overrides the radius-server retransmit global configuration command setting.
timeout <i>seconds</i>	(Optional) Specifies the time interval that the Switch waits for the RADIUS server to reply before sending a request again. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting.
no radius server <i>name</i>	Returns to the default settings

Command Default

- 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 timeout 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

Radius server sub-mode configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced to replace the radius-server host command.

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 non-default values.
- You can configure the authentication and encryption key by using the **key string** sub-mode configuration command. Always configure the key as the last item in this command.
- Use the **automate-tester name** keywords to enable automatic server testing of the RADIUS server status and to specify the username to be used.

This example shows how to configure 1645 as the UDP port for the authentication server and 1646 as the UDP port for the accounting server, and configure a key string:

```
Device(config)# radius server ISE
Device(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646
Device(config-radius-server)# key cisco123
```

router rip

To configure the Routing Information Protocol (RIP) routing process, use the **router rip** command in global configuration mode. To turn off the RIP routing process, use the **no** form of this command.

router rip
no router rip

Syntax Description This command has no arguments or keywords.

Command Default No RIP routing process is defined.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS Release 15.2(5)E2	This command was introduced.

Examples The following example shows how to begin the RIP routing process:

```
Device(config)# router rip
```

Related Commands	Command	Description
	network (RIP)	Specifies a list of networks for the RIP process.

security level (IPv6 snooping)

To specify the level of security enforced, use the **security-level** command in IPv6 snooping policy configuration mode.

security level { **glean** | **guard** | **inspect** }

Syntax Description	glean	Extracts addresses from the messages and installs them into the binding table without performing any verification.
	guard	Performs both glean and inspect. Additionally, RA and DHCP server messages are rejected unless they are received on a trusted port or another policy authorizes them.
	inspect	Validates messages for consistency and conformance; in particular, address ownership is enforced. Invalid messages are dropped.
Command Default	The default security level is guard.	
Command Modes	IPv6 snooping configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the security level as inspect:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# security-level inspect
```

show aaa acct-stop-cache

To show accounting session IDs of poisoned sessions, use the **show aaa acct-stop-cache** command.

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines Accounting Stop records for poisoned sessions are cached only on the standby switch.

This is an example of output from the **show aaa acct-stop-cache** command:

```
Device# show aaa acct-stop-cache
```

show aaa clients

To show AAA client statistics, use the **show aaa clients** command.

show aaa clients [**detailed**]

Syntax Description

detailed (Optional) Shows detailed AAA client statistics.

Command Modes

User EXEC

Command History

Release

Modification

Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E

This command was introduced.

This is an example of output from the **show aaa clients** command:

```
Device# show aaa clients
```

```
Dropped request packets: 0
```

show aaa command handler

To show AAA command handler statistics, use the **show aaa command handler** command.

show aaa command handler

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

This is an example of output from the **show aaa command handler** command:

```
Device# show aaa command handler

AAA Command Handler Statistics:
  account-logon: 0, account-logoff: 0
  account-query: 0, pod: 0
  service-logon: 0, service-logoff: 0
  user-profile-push: 0, session-state-log: 0
  reauthenticate: 0, bounce-host-port: 0
  disable-host-port: 0, update-rbacl: 0
  update-sgt: 0, update-cts-policies: 0
  invalid commands: 0
  async message not sent: 0
```

show aaa local

To show AAA local method options, use the **show aaa local** command.

show aaa localuser lockout

Syntax Description	
user	Specifies the AAA local locked-out user.
lockout	

Command Modes	
	User EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

This is an example of output from the **show aaa local user lockout** command:

```
Device# show aaa local user lockout
      Local-user          Lock time
```


show aaa servers

To shows all AAA servers as seen by the AAA server MIB, use the **show aaa servers** command.

show aaa servers [**private** | **public** | [**detailed**]]

Syntax Description		
	detailed	(Optional) Displays private AAA servers as seen by the AAA Server MIB.
	public	(Optional) Displays public AAA servers as seen by the AAA Server MIB.
	detailed	(Optional) Displays detailed AAA server statistics.
Command Modes	User EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

This is an example of output from the **show aaa servers** command:

```
Device# show aaa servers
RADIUS: id 1, priority 1, host 172.20.128.2, auth-port 1645, acct-port 1646
State: current UP, duration 9s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
Request: start 0, interim 0, stop 0
Response: start 0, interim 0, stop 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 0m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

show aaa sessions

To show AAA sessions as seen by the AAA Session MIB, use the **show aaa sessions** command.

show aaa sessions

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

This is an example of output from the **show aaa sessions** command:

```
Device# show aaa sessions
Total sessions since last reload: 7
Session Id: 4007
  Unique Id: 4025
  User Name: *not available*
  IP Address: 0.0.0.0
  Idle Time: 0
  CT Call Handle: 0
```

show authentication sessions

To display information about current Auth Manager sessions, use the **show authentication sessions** command.

show authentication sessions [**handle** *handle-id*] [**interface** *type number*] [**mac** *mac-address*] [**interface** *type number*] [**method** *method-name*] [**interface** *type number*] [**session-id** *session-id*]

Syntax Description

handle <i>handle-id</i>	(Optional) Specifies the particular handle for which Auth Manager information is to be displayed.
interface <i>type number</i>	(Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed.
mac <i>mac-address</i>	(Optional) Specifies the particular MAC address for which you want to display information.
method <i>method-name</i>	(Optional) Specifies the particular authentication method for which Auth Manager information is to be displayed. If you specify a method (dot1x , mab , or webauth), you may also specify an interface.
session-id <i>session-id</i>	(Optional) Specifies the particular session for which Auth Manager information is to be displayed.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	This command was introduced.

Usage Guidelines

Use the **show authentication sessions** command to display information about all current Auth Manager sessions. To display information about specific Auth Manager sessions, use one or more of the keywords.

This table shows the possible operating states for the reported authentication sessions.

Table 31: Authentication Method States

State	Description
Not run	The method has not run for this session.
Running	The method is running for this session.
Failed over	The method has failed and the next method is expected to provide a result.
Success	The method has provided a successful authentication result for the session.
Authc Failed	The method has provided a failed authentication result for the session.

This table shows the possible authentication methods.

Table 32: Authentication Method States

State	Description
dot1x	802.1X
mab	MAC authentication bypass
webauth	web authentication

The following example shows how to display all authentication sessions on the switch:

```
Device# show authentication sessions
Interface  MAC Address      Method  Domain  Status      Session ID
Gi1/0/48   0015.63b0.f676  dot1x   DATA   Authz Success 0A3462B1000000102983C05C
Gi1/0/5    000f.23c4.a401  mab     DATA   Authz Success 0A3462B10000000D24F80B58
Gi1/0/5    0014.bf5d.d26d  dot1x   DATA   Authz Success 0A3462B10000000E29811B94
```

The following example shows how to display all authentication sessions on an interface:

```
Device# show authentication sessions interface gigabitethernet2/0/47
      Interface: GigabitEthernet2/0/47
      MAC Address: Unknown
      IP Address: Unknown
      Status: Authz Success
      Domain: DATA
      Oper host mode: multi-host
      Oper control dir: both
      Authorized By: Guest Vlan
      Vlan Policy: 20
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: 0A3462C8000000000002763C
      Acct Session ID: 0x00000002
      Handle: 0x25000000

Runnable methods list:
  Method  State
  mab     Failed over
  dot1x   Failed over
-----
      Interface: GigabitEthernet2/0/47
      MAC Address: 0005.5e7c.da05
      IP Address: Unknown
      User-Name: 00055e7cda05
      Status: Authz Success
      Domain: VOICE
      Oper host mode: multi-domain
      Oper control dir: both
      Authorized By: Authentication Server
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: 0A3462C8000000010002A238
      Acct Session ID: 0x00000003
      Handle: 0x91000001

Runnable methods list:
  Method  State
  mab     Authc Success
```

```
dot1x    Not run
```

show auto security

To display auto security status, use the **show auto security** command in privileged EXEC mode.

show auto-security

This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS Release 15.2(5)E	This command was introduced in a release prior to Cisco IOS Release 15.2(5)E.

Usage Guidelines Configuring the **auto security** command in global configuration mode, configures auto security globally; including all interfaces. When you disable auto security, it is disabled on all interfaces.

Use the **auto security-port** command to enable auto security on specific interfaces.

The following is sample output from the **show auto security** command, when auto security is enabled globally:

```
Switch# show auto security

Auto Security is Enabled globally

AutoSecurity is Enabled on below interface(s):
-----
GigabitEthernet1/0/2
GigabitEthernet1/0/3
GigabitEthernet1/0/4
GigabitEthernet1/0/5
GigabitEthernet1/0/7
GigabitEthernet1/0/8
GigabitEthernet1/0/10
GigabitEthernet1/0/12
GigabitEthernet1/0/23
```

The following is sample output from the **show auto security** command, when auto security is enabled on a specific interface:

```
Switch# show auto security

Auto Security is Disabled globally

AutoSecurity is Enabled on below interface(s):
-----
GigabitEthernet1/0/2
```

Related Commands

Command	Description
auto security	Configures global auto security.
auto security-port	Configures auto security on an interface.

show cisp

To display CISP information for a specified interface, use the **show cisp** command in privileged EXEC mode.

show cisp {[**clients** | **interface** *interface-id*] | **registrations** | **summary**}

Syntax Description		
clients		(Optional) Display CISP client details.
interface <i>interface-id</i>		(Optional) Display CISP information about the specified interface. Valid interfaces include physical ports and port channels.
registrations		Displays CISP registrations.
summary		(Optional) Displays CISP summary.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.
		This command was reintroduced. This command was not supported in and

This example shows output from the **show cisp interface** command:

```
Device# show cisp interface fast 0
CISP not enabled on specified interface
```

This example shows output from the **show cisp registration** command:

```
Device# show cisp registrations
Interface(s) with CISP registered user(s):
-----
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
Auth Mgr (Authenticator)
Gi2/0/13
```



```
Auth Mgr (Authenticator)
Gi3/0/3
Gi3/0/5
Gi3/0/23
```

Related Commands

Command	Description
cisp enable	Enable Client Information Signalling Protocol (CISP)
dot1x credentials <i>profile</i>	Configure a profile on a supplicant switch

show dot1x

To display IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port, use the **show dot1x** command in user EXEC mode.

show dot1x [**all** [**count** | **details** | **statistics** | **summary**]] [**interface type number** [**details** | **statistics**]] [**statistics**]

Syntax Description		
all	(Optional) Displays the IEEE 802.1x information for all interfaces.	
count	(Optional) Displays total number of authorized and unauthorized clients.	
details	(Optional) Displays the IEEE 802.1x interface details.	
statistics	(Optional) Displays the IEEE 802.1x statistics for all interfaces.	
summary	(Optional) Displays the IEEE 802.1x summary for all interfaces.	
interface type number	(Optional) Displays the IEEE 802.1x status for the specified port.	

Command Modes User EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

This is an example of output from the **show dot1x all** command:

```
Device# show dot1x all
Sysauthcontrol          Enabled
Dot1x Protocol Version      3
```

This is an example of output from the **show dot1x all count** command:

```
Device# show dot1x all count
Number of Dot1x sessions
-----
Authorized Clients      = 0
UnAuthorized Clients    = 0
Total No of Client      = 0
```

This is an example of output from the **show dot1x all statistics** command:

```
Device# show dot1x statistics
Dot1x Global Statistics for
-----
RxStart = 0      RxLogoff = 0      RxResp = 0      RxRespID = 0
RxReq = 0        RxInvalid = 0    RxLenErr = 0
RxTotal = 0
```

```
TxStart = 0      TxLogoff = 0      TxResp = 0
TxReq = 0        ReTxReq = 0        ReTxReqFail = 0
TxReqID = 0      ReTxReqID = 0      ReTxReqIDFail = 0
TxTotal = 0
```

show eap pac peer

To display stored Protected Access Credentials (PAC) for Extensible Authentication Protocol (EAP) Flexible Authentication via Secure Tunneling (FAST) peers, use the **show eap pac peer** command in privileged EXEC mode.

show eap pac peer

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	
Cisco IOS Release 15.2(5)E	This command was introduced.

This is an example of output from the **show eap pac peers** privileged EXEC command:

```
Device> show eap pac peers
No PACs stored
```

Related Commands

Command	Description
clear eap sessions	Clears EAP session information for the switch or for the specified port.

show ip dhcp snooping statistics

To display DHCP snooping statistics in summary or detail form, use the **show ip dhcp snooping statistics** command in user EXEC mode.

show ip dhcp snooping statistics [**detail**]

Syntax Description

detail (Optional) Displays detailed statistics information.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	This command was introduced.

Usage Guidelines

In a switch stack, all statistics are generated on the stack primary. If a new active switch is elected, the statistics counters reset.

This is an example of output from the **show ip dhcp snooping statistics** command:

```
Device> show ip dhcp snooping statistics

Packets Forwarded                = 0
Packets Dropped                  = 0
Packets Dropped From untrusted ports = 0
```

This is an example of output from the **show ip dhcp snooping statistics detail** command:

```
Device> show ip dhcp snooping statistics detail

Packets Processed by DHCP Snooping = 0
Packets Dropped Because
  IDB not known                    = 0
  Queue full                        = 0
  Interface is in errdisabled      = 0
  Rate limit exceeded              = 0
  Received on untrusted ports      = 0
  Nonzero giaddr                   = 0
  Source mac not equal to chaddr   = 0
  Binding mismatch                  = 0
  Insertion of opt82 fail          = 0
  Interface Down                    = 0
  Unknown output interface         = 0
  Reply output port equal to input port = 0
  Packet denied by platform        = 0
```

This table shows the DHCP snooping statistics and their descriptions:

Table 33: DHCP Snooping Statistics

DHCP Snooping Statistic	Description
Packets Processed by DHCP Snooping	Total number of packets handled by DHCP snooping, including forwarded and dropped packets.
Packets Dropped Because IDB not known	Number of errors when the input interface of the packet cannot be determined.
Queue full	Number of errors when an internal queue used to process the packets is full. This might happen if DHCP packets are received at an excessively high rate and rate limiting is not enabled on the ingress ports.
Interface is in errdisabled	Number of times a packet was received on a port that has been marked as error disabled. This might happen if packets are in the processing queue when a port is put into the error-disabled state and those packets are subsequently processed.
Rate limit exceeded	Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state.
Received on untrusted ports	Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped.
Nonzero giaddr	Number of times the relay agent address field (giaddr) in the DHCP packet received on an untrusted port was not zero, or the no ip dhcp snooping information option allow-untrusted global configuration command is not configured and a packet received on an untrusted port contained option-82 data.
Source mac not equal to chaddr	Number of times the client MAC address field of the DHCP packet (chaddr) does not match the packet source MAC address and the ip dhcp snooping verify mac-address global configuration command is configured.
Binding mismatch	Number of times a RELEASE or DECLINE packet was received on a port that is different than the port in the binding for that MAC address-VLAN pair. This indicates someone might be trying to spoof the real client, or it could mean that the client has moved to another port on the switch and issued a RELEASE or DECLINE. The MAC address is taken from the chaddr field of the DHCP packet, not the source MAC address in the Ethernet header.
Insertion of opt82 fail	Number of times the option-82 insertion into a packet failed. The insertion might fail if the packet with the option-82 data exceeds the size of a single physical packet on the internet.

DHCP Snooping Statistic	Description
Interface Down	Number of times the packet is a reply to the DHCP relay agent, but the SVI interface for the relay agent is down. This is an unlikely error that occurs if the SVI goes down between sending the client request to the DHCP server and receiving the response.
Unknown output interface	Number of times the output interface for a DHCP reply packet cannot be determined by either option-82 data or a lookup in the MAC address table. The packet is dropped. This can happen if option 82 is not used and the client MAC address has aged out. If IPSG is enabled with the port-security option and option 82 is not enabled, the MAC address of the client is not learned, and the reply packets will be dropped.
Reply output port equal to input port	Number of times the output port for a DHCP reply packet is the same as the input port, causing a possible loop. Indicates a possible network misconfiguration or misuse of trust settings on ports.
Packet denied by platform	Number of times the packet has been denied by a platform-specific registry.

show ip rip database

To display summary address entries in the Routing Information Protocol (RIP) routing database entries if relevant are routes being summarized based upon a summary address, use the **show ip rip database** command in privileged EXEC mode.

show ip rip database [*ip-address mask*]

Syntax Description

<i>ip-address</i>	(Optional) Address about which routing information should be displayed.
<i>mask</i>	(Optional) Argument for the subnet mask. The subnet mask must also be specified if the IP address argument is entered.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS Release 15.2(5)E2	This command was introduced.

Usage Guidelines

Summary address entries will appear in the database only if relevant child routes are being summarized. When the last child route for a summary address becomes invalid, the summary address is also removed from the routing table.

The RIP private database is populated only if triggered extensions to RIP are enabled with the **ip rip triggered** command.

Examples

The following output shows a summary address entry for route 10.11.0.0/16, with three child routes active:

```
Device# show ip rip database
10.0.0.0/8    auto-summary
10.0.0.0/8
    [1] via 172.16.0.10, 00:00:17, GigabitEthernet7/0/10
192.168.0.0/8    auto-summary
192.168.0.0/8
    [2] via 172.16.0.10, 00:00:17, GigabitEthernet7/0/10
172.16.0.0/8    auto-summary
172.16.0.0/24    directly connected, GigabitEthernet7/0/10
```

The table below describes the fields in the display.

Table 34: show ip rip database Field Descriptions

Field	Description
10.0.0.0/8 auto-summary	Summary address entry.

Field	Description
172.16.0.0/24 directly connected, GigabitEthernet7/0/10	Directly connected entry for GigabitEthernet 7/0/10.

Related Commands

Commands	Description
debug ip rip	Displays information on RIP routing transactions.

show mls qos copp protocols

To display the Copp parameters and counters for all the configured protocol, use the **show mls qos copp protocols** command in EXEC mode.

show mls qos copp protocols

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Exec mode.

Command History	Release	Modification
	Cisco IOS 15.2.4E	This command was introduced.

Usage Guidelines Use this command to display CoPP parameters and counters for all the configured protocol.

The following example shows the CoPP parameters and counters for all the configured protocol:

```
Device # show running-config | inc copp
mls qos copp protocol rep-hfl police pps 5600
mls qos copp protocol lldp police bps 908900
mls qos copp protocol cdp police pps 3434
/* Copp detailed output */
Device# show mls qos copp protocols
```

Protocol	InProfilePackets	OutProfilePackets	Mode	PolicerRate	PolicerBurst
				InProfileBytes	OutProfileBytes
rep-hfl			pps	5600	5600
0	0			0	0
lldp			bps	908900	908900
0	0			0	0
cdp			pps	3434	3434
45172	0			2891008	0

Related Commands

Command	Description
mls qos copp protocol	Protects the switch's control plane.

show radius server-group

To display properties for the RADIUS server group, use the **show radius server-group** command.

```
show radius server-group {name | all}
```

Syntax Description

name Name of the server group. The character string used to name the group of servers must be defined using the **aaa group server radius** command.

all Displays properties for all of the server groups.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	This command was introduced.

Usage Guidelines

Use the **show radius server-group** command to display the server groups that you defined by using the **aaa group server radius** command.

This is an example of output from the **show radius server-group all** command:

```
Device# show radius server-group all
Server group radius
  Sharecount = 1  sg_unconfigured = FALSE
  Type = standard Memlocks = 1
```

This table describes the significant fields shown in the display.

Table 35: show radius server-group command Field Descriptions

Field	Description
Server group	Name of the server group.
Sharecount	Number of method lists that are sharing this server group. For example, if one method list uses a particular server group, the sharecount would be 1. If two method lists use the same server group, the sharecount would be 2.
sg_unconfigured	Server group has been unconfigured.
Type	The type can be either standard or nonstandard. The type indicates whether the servers in the group accept nonstandard attributes. If all servers within the group are configured with the nonstandard option, the type will be shown as "nonstandard".

Field	Description
Memlocks	An internal reference count for the server-group structure that is in memory. The number represents how many internal data structure packets or transactions are holding references to this server group. Memlocks is used internally for memory management purposes.

show vlan group

To display the VLANs that are mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

```
show vlan group [{group-name vlan-group-name [user_count]}]
```

Syntax Description	group-name <i>vlan-group-name</i> (Optional) Displays the VLANs mapped to the specified VLAN group.	
	user_count (Optional) Displays the number of users in each VLAN mapped to a specified VLAN group.	
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.
Usage Guidelines	The show vlan group command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you enter the group-name keyword, only the members of the specified VLAN group are displayed.	

This example shows how to display the members of a specified VLAN group:

Related Topics

[vlan group](#), on page 538

switchport port-security aging

To set the aging time and type for secure address entries or to change the aging behavior for secure addresses on a particular port, use the **switchport port-security aging** command in interface configuration mode. To disable port security aging or to set the parameters to their default states, use the **no** form of this command.

```
switchport port-security aging {static | time time | type {absolute | inactivity}}
no switchport port-security aging {static | time | type}
```

Syntax Description	
static	Enables aging for statically configured secure addresses on this port.
time <i>time</i>	Specifies the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
type	Sets the aging type.
absolute	Sets absolute aging type. All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.
inactivity	Sets the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Command Default	
	The port security aging feature is disabled. The default time is 0 minutes.
	The default aging type is absolute.
	The default static aging behavior is disabled.

Command Modes	
	Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines	
	To enable secure address aging for a particular port, set the aging time to a value other than 0 for that port.
	To allow limited time access to particular secure addresses, set the aging type as absolute . When the aging time lapses, the secure addresses are deleted.
	To allow continuous access to a limited number of secure addresses, set the aging type as inactivity . This removes the secure address when it become inactive, and other addresses can become secure.
	To allow unlimited access to a secure address, configure it as a secure address, and disable aging for the statically configured secure address by using the no switchport port-security aging static interface configuration command.

This example sets the aging time as 2 hours for absolute aging for all the secure addresses on the port:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport port-security aging time 120
```

This example sets the aging time as 2 minutes for inactivity aging type with aging enabled for configured secure addresses on the port:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport port-security aging time 2
Device(config-if)# switchport port-security aging type inactivity
Device(config-if)# switchport port-security aging static
```

This example shows how to disable aging for configured secure addresses:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport port-security aging static
```

switchport port-security mac-address

To configure secure MAC addresses or sticky MAC address learning, use the **switchport port-security mac-address** interface configuration command. To return to the default setting, use the **no** form of this command.

```
switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}]} | sticky
[{mac-address | vlan {vlan-id {access | voice}}]}]
no switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}]} | sticky
[{mac-address | vlan {vlan-id {access | voice}}]}]
```

Syntax Description

mac-address A secure MAC address for the interface by entering a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value configured.

vlan vlan-id (Optional) On a trunk port only, specifies the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used.

vlan access (Optional) On an access port only, specifies the VLAN as an access VLAN.

vlan voice (Optional) On an access port only, specifies the VLAN as a voice VLAN.

Note The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

sticky Enables the interface for sticky learning. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses.

mac-address (Optional) A MAC address to specify a sticky secure MAC address.

Command Default

No secure MAC addresses are configured.
Sticky learning is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

A secure port has the following limitations:

- A secure port can be an access port or a trunk port; it cannot be a dynamic access port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group.

- You cannot configure static secure or sticky secure MAC addresses in the voice VLAN.
- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.
- Voice VLAN is supported only on access ports and not on trunk ports.

Sticky secure MAC addresses have these characteristics:

- When you enable sticky learning on an interface by using the **switchport port-security mac-address sticky** interface configuration command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses and adds all sticky secure MAC addresses to the running configuration.
- If you disable sticky learning by using the **no switchport port-security mac-address sticky** interface configuration command or the running configuration is removed, the sticky secure MAC addresses remain part of the running configuration but are removed from the address table. The addresses that were removed can be dynamically reconfigured and added to the address table as dynamic addresses.
- When you configure sticky secure MAC addresses by using the **switchport port-security mac-address sticky mac-address** interface configuration command, these addresses are added to the address table and the running configuration. If port security is disabled, the sticky secure MAC addresses remain in the running configuration.
- If you save the sticky secure MAC addresses in the configuration file, when the switch restarts or the interface shuts down, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost. If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.
- If you disable sticky learning and enter the **switchport port-security mac-address sticky mac-address** interface configuration command, an error message appears, and the sticky secure MAC address is not added to the running configuration.

You can verify your settings by using the **show port-security** privileged EXEC command.

This example shows how to configure a secure MAC address and a VLAN ID on a port:

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

This example shows how to enable sticky learning and to enter two sticky secure MAC addresses on a port:

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Device(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

switchport port-security maximum

To configure the maximum number of secure MAC addresses, use the **switchport port-security maximum** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
switchport port-security maximum value [vlan [{vlan-list | [{access | voice}]]]
no switchport port-security maximum value [vlan [{vlan-list | [{access | voice}]]]
```

Syntax Description

value	Sets the maximum number of secure MAC addresses for the interface. The default setting is 1.
vlan	(Optional) For trunk ports, sets the maximum number of secure MAC addresses on a VLAN or range of VLANs. If the vlan keyword is not entered, the default value is used.
vlan-list	(Optional) Range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used.
access	(Optional) On an access port only, specifies the VLAN as an access VLAN.
voice	(Optional) On an access port only, specifies the VLAN as a voice VLAN.
Note	The voice keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

Command Default

When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

The maximum number of secure MAC addresses that you can configure on a switch or switch stack is set by the maximum number of available MAC addresses allowed in the system. This number is determined by the active Switch Database Management (SDM) template. See the **sdm prefer** command. This number represents the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.

A secure port has the following limitations:

- A secure port can be an access port or a trunk port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group.

- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.

Voice VLAN is supported only on access ports and not on trunk ports.

- When you enter a maximum secure address value for an interface, if the new value is greater than the previous value, the new value overrides the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

Setting a maximum number of addresses to one and configuring the MAC address of an attached device ensures that the device has the full bandwidth of the port.

When you enter a maximum secure address value for an interface, this occurs:

- If the new value is greater than the previous value, the new value overrides the previously configured value.
- If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

You can verify your settings by using the **show port-security** privileged EXEC command.

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 5. The violation mode is the default, and no secure MAC addresses are configured.

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
```

switchport port-security violation

To configure secure MAC address violation mode or the action to be taken if port security is violated, use the **switchport port-security violation** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
switchport port-security violation {protect | restrict | shutdown | shutdown vlan}
no switchport port-security violation {protect | restrict | shutdown | shutdown vlan}
```

Syntax Description

protect	Sets the security violation protect mode.
restrict	Sets the security violation restrict mode.
shutdown	Sets the security violation shutdown mode.
shutdown vlan	Sets the security violation mode to per-VLAN shutdown.

Command Default

The default violation mode is **shutdown**.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

In the security violation protect mode, when the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.



Note

We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

In the security violation restrict mode, when the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

In the security violation shutdown mode, the interface is error-disabled when a violation occurs and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shutdown** interface configuration commands.

When the security violation mode is set to per-VLAN shutdown, only the VLAN on which the violation occurred is error-disabled.

A secure port has the following limitations:

- A secure port can be an access port or a trunk port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group.

A security violation occurs when the maximum number of secure MAC addresses are in the address table and a station whose MAC address is not in the address table attempts to access the interface or when a station whose MAC address is configured as a secure MAC address on another secure port attempts to access the interface.

When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command. You can manually re-enable the port by entering the **shutdown** and **no shutdown** interface configuration commands or by using the **clear errdisable interface** privileged EXEC command.

You can verify your settings by using the **show port-security** privileged EXEC command.

This example show how to configure a port to shut down only the VLAN if a MAC security violation occurs:

```
Device(config)# interface gigabitethernet2/0/2
Device(config)# switchport port-security violation shutdown vlan
```

tracking (IPv6 snooping)

To override the default tracking policy on a port, use the **tracking** command in IPv6 snooping policy configuration mode.

tracking {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}

Syntax Description		
enable		Enables tracking.
reachable-lifetime		(Optional) Specifies the maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability. <ul style="list-style-type: none"> The reachable-lifetime keyword can be used only with the enable keyword. Use of the reachable-lifetime keyword overrides the global reachable lifetime configured by the ipv6 neighbor binding reachable-lifetime command.
<i>value</i>		Lifetime value, in seconds. The range is from 1 to 86400, and the default is 300.
infinite		Keeps an entry in a reachable or stale state for an infinite amount of time.
disable		Disables tracking.
stale-lifetime		(Optional) Keeps the time entry in a stale state, which overwrites the global stale-lifetime configuration. <ul style="list-style-type: none"> The stale lifetime is 86,400 seconds. The stale-lifetime keyword can be used only with the disable keyword. Use of the stale-lifetime keyword overrides the global stale lifetime configured by the ipv6 neighbor binding stale-lifetime command.

Command Default The time entry is kept in a reachable state.

Command Modes IPv6 snooping configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines The **tracking** command overrides the default tracking policy set by the **ipv6 neighbor tracking** command on the port on which this policy applies. This function is useful on trusted ports where, for example, you may not want to track entries but want an entry to stay in the binding table to prevent it from being stolen.

The **reachable-lifetime** keyword is the maximum time an entry will be considered reachable without proof of reachability, either directly through tracking or indirectly through IPv6 snooping. After the **reachable-lifetime** value is reached, the entry is moved to stale. Use of the **reachable-lifetime** keyword with the tracking command overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.

The **stale-lifetime** keyword is the maximum time an entry is kept in the table before it is deleted or the entry is proven to be reachable, either directly or indirectly. Use of the **reachable-lifetime** keyword with the **tracking** command overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# tracking disable stale-lifetime infinite
```

trusted-port

To configure a port to become a trusted port, use the **trusted-port** command in IPv6 snooping policy mode or ND inspection policy configuration mode. To disable this function, use the **no** form of this command.

trusted-port
no trusted-port

Syntax Description This command has no arguments or keywords.

Command Default No ports are trusted.

Command Modes ND inspection policy configuration
 IPv6 snooping configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E
		This command was introduced.

Usage Guidelines When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and configure the port to be trusted:

```
Device(config)# ipv6 nd inspection policy1
Device(config-nd-inspection)# trusted-port
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to be trusted:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# trusted-port
```


vlan access-map

To create or modify a VLAN map entry for VLAN packet filtering, and change the mode to the VLAN access-map configuration, use the **vlan access-map** command in global configuration mode on the switch stack or on a standalone switch. To delete a VLAN map entry, use the **no** form of this command.

```
vlan access-map name [number]
no vlan access-map name [number]
```



Note This command is not supported on switches running the LAN Base feature set.

Syntax Description

name Name of the VLAN map.

number (Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry.

Command Default

There are no VLAN map entries and no VLAN maps applied to a VLAN.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
	This command was introduced.

Usage Guidelines

In global configuration mode, use this command to create or modify a VLAN map. This entry changes the mode to VLAN access-map configuration, where you can use the **match** access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the **action** command to set whether a match causes the packet to be forwarded or dropped.

In VLAN access-map configuration mode, these commands are available:

- **action**—Sets the action to be taken (forward or drop).
- **default**—Sets a command to its defaults.
- **exit**—Exits from VLAN access-map configuration mode.
- **match**—Sets the values to match (IP address or MAC address).
- **no**—Negates a command or set its defaults.

When you do not specify an entry number (sequence number), it is added to the end of the map.

There can be only one VLAN map per VLAN and it is applied as packets are received by a VLAN.

You can use the **no vlan access-map name [number]** command with a sequence number to delete a single entry.

Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs. For more information about VLAN map entries, see the software configuration guide for this release.

This example shows how to create a VLAN map named vac1 and apply matching conditions and actions to it. If no other entries already exist in the map, this will be entry 10.

```
Device(config)# vlan access-map vac1  
Device(config-access-map)# match ip address acl1  
Device(config-access-map)# action forward
```

This example shows how to delete VLAN map vac1:

```
Device(config)# no vlan access-map vac1
```

Related Topics

[match \(access-map configuration\)](#), on page 481

[vlan filter](#), on page 537

vlan filter

To apply a VLAN map to one or more VLANs, use the **vlan filter** command in global configuration mode on the switch stack or on a standalone switch. To remove the map, use the **no** form of this command.

```
vlan filter mapname vlan-list {list | all}
no vlan filter mapname vlan-list {list | all}
```



Note This command is not supported on switches running the LAN Base feature set.

Syntax Description

<i>mapname</i>	Name of the VLAN map entry.
vlan-list	Specifies which VLANs to apply the map to.
<i>list</i>	The list of one or more VLANs in the form tt, uu-vv, xx, yy-zz, where spaces around commas and dashes are optional. The range is 1 to 4094.
all	Adds the map to all VLANs.

Command Default

There are no VLAN filters.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN.

For more information about VLAN map entries, see the software configuration guide for this release.

This example applies VLAN map entry map1 to VLANs 20 and 30:

```
Device(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry mac1 from VLAN 20:

```
Device(config)# no vlan filter map1 vlan-list 20
```

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

Related Topics

[vlan access-map](#), on page 535

vlan group

To create or modify a VLAN group, use the **vlan group** command in global configuration mode. To remove a VLAN list from the VLAN group, use the **no** form of this command.

vlan group *group-name* **vlan-list** *vlan-list*
no vlan group *group-name* **vlan-list** *vlan-list*

Syntax Description	<i>group-name</i>	Name of the VLAN group. The group name may contain up to 32 characters and must begin with a letter.
	vlan-list <i>vlan-list</i>	Specifies one or more VLANs to be added to the VLAN group. The <i>vlan-list</i> argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID range. Multiple entries are separated by a hyphen (-) or a comma (,).
Command Default	None	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E

Usage Guidelines

If the named VLAN group does not exist, the **vlan group** command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is mapped to the group.

The **no** form of the **vlan group** command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, the VLAN group is deleted.

A maximum of 100 VLAN groups can be configured, and a maximum of 4094 VLANs can be mapped to a VLAN group.

This example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Device(config)# vlan group group1 vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Device(config)# no vlan group group1 vlan-list 7
```

Related Topics

[show vlan group](#), on page 523



PART **VIII**

Stack Manager

- [Stack Manager Commands, on page 541](#)



Stack Manager Commands

- [debug platform remote-commands, on page 542](#)
- [debug platform stack-manager, on page 543](#)
- [reload, on page 544](#)
- [remote command, on page 546](#)
- [session, on page 547](#)
- [show platform stack compatibility configuration, on page 548](#)
- [show platform stack compatibility feature, on page 549](#)
- [show platform stack compatibility table, on page 551](#)
- [show platform stack manager, on page 553](#)
- [show switch, on page 555](#)
- [stack-mac persistent timer, on page 558](#)
- [switch stack port, on page 561](#)
- [switch priority, on page 563](#)
- [switch provision, on page 564](#)
- [switch renumber, on page 566](#)
- [switch stack port-speed 10, on page 567](#)

debug platform remote-commands

To enable debugging of remote commands, use the **debug platform remote-commands** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug platform remote-commands
no debug platform remote-commands

Syntax Description This command has no arguments or keywords.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines The **undebug platform remote-commands** command is the same as the **no debug platform remote-commands** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the stack's active switch by using the **session** *switch-number* privileged EXEC command. Enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number* *LINE* privileged EXEC command on the active switch to enable debugging on a member switch without first starting a session.

Related Topics

[remote command](#), on page 546

[session](#), on page 547

debug platform stack-manager

To enable debugging of the stack manager software, use the **debug platform stack-manager** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug platform stack-manager {all | rpc | sdp | sim | ssm | tdm | trace}
no debug platform stack-manager {all | rpc | sdp | sim | ssm | tdm | trace}
```

Syntax Description

all	Displays all stack manager debug messages.
rpc	Displays stack manager remote procedure call (RPC) usage debug messages.
sdp	Displays the Stack Discovery Protocol (SDP) debug messages.
sim	Displays the stack information module debug messages.
ssm	Displays the stack state-machine debug messages.
tdm	Displays the stack manager topology discovery use debug messages.
trace	Traces the stack manager entry and exit debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

This command is supported only on stacking-capable switches.

The **undebug platform stack-manager** command is the same as the **no debug platform stack-manager** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session switch-number** EXEC command. Enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command stack-member-number LINE** EXEC command on the active switch to enable debugging on a member switch without first starting a session.

Related Topics

[remote command](#), on page 546

[session](#), on page 547

reload

To reload the stack member and to apply a configuration change, use the **reload** command in privileged EXEC mode.

reload [{/noverify | /verify}] [{LINE | at | cancel | in | slot *stack-member-number* | standby-cpu}]

Syntax Description	
/noverify	(Optional) Specifies to not verify the file signature before the reload.
/verify	(Optional) Verifies the file signature before the reload.
<i>LINE</i>	(Optional) Reason for the reload.
at	(Optional) Specifies the time in hh:mm for the reload to occur.
cancel	(Optional) Cancels the pending reload.
in	(Optional) Specifies a time interval for reloads to occur.
slot	(Optional) Saves the changes on the specified stack member and then restarts it.
<i>stack-member-number</i>	(Optional) Stack member number on which to save the changes. The range is 1 to 8.
standby-cpu	(Optional) Reloads the standby route processor (RP).

Command Default Immediately reloads the stack member and puts a configuration change into effect.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines If there is more than one switch in the switch stack, and you enter the **reload slot *stack-member-number*** command, you are not prompted to save the configuration.

Examples

This example shows how to reload the switch stack:

```
Device# reload
System configuration has been modified. Save? [yes/no]: y
Proceed to reload the whole Stack? [confirm] y
```

This example shows how to reload a specific stack member:

```
Device# reload slot 6
Proceed with reload? [confirm] y
```

This example shows how to reload a single-switch switch stack (there is only one member switch):

```
Device# reload slot 3
System configuration has been modified. Save? [yes/no]: y
Proceed to reload the whole Stack? [confirm] y
```

Related Topics

[show switch](#), on page 555

[switch stack port](#), on page 561

[switch renumber](#), on page 566

remote command

To monitor all or specified stack members, use the **remote command** privileged EXEC command.

remote command {*allstack-member-number*} *LINE*

Syntax Description		
all		Applies to all stack members.
<i>stack-member-number</i>		The stack member. The range is 1 to 8.
<i>LINE</i>		The command to execute.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines The commands that you use in the *LINE* command-to-execute string (such as **debug**, **show**, or **clear**) apply to a specific stack member or to the switch stack.

Examples

This example shows how to execute the **undebug** command on the switch stack:

```
Switch(config)# remote command all undebug all
Switch :1 :
-----
All possible debugging has been turned off
Switch :5 :
-----
All possible debugging has been turned off
Switch :7 :
-----
All possible debugging has been turned off
```

This example shows how to execute the **debug uddld event** command on stack member 5:

```
Switch(config)# remote command 5 undebug all
Switch :5 :
-----
UDLD events debugging is on
```

Related Topics

- [reload](#), on page 544
- [show switch](#), on page 555
- [switch stack port](#), on page 561
- [switch renumber](#), on page 566

session

To access a specific stack member, use the **session** command in privileged EXEC mode on the active stack.

session *stack-member-number*

Syntax Description	<i>stack-member-number</i>	Stack member number to access from the active switch. The range is 1 to 8.
---------------------------	----------------------------	--

Command Default	None
------------------------	------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

When you access the member, its member number is appended to the system prompt.

Use the **session** command from the active switch to access a member.

Use the **session** command with **processor 1** from the active or a standalone switch to access the internal controller. A standalone device is always member 1.

Examples

This example shows how to access stack member 3:

```
Device# session 3
Device-3#
```

Related Topics

- [reload](#), on page 544
- [show switch](#), on page 555
- [switch stack port](#), on page 561
- [switch renumber](#), on page 566

show platform stack compatibility configuration

To display switch stack compatibility information, use the **show platform stack compatibility configuration** command in privileged EXEC mode.

show platform stack compatibility configuration {**current** | **failure-log** | **mismatch** [**switch** *switch-number*]}

Syntax Description	current	Displays currently configured system level features.
	failure-log	Displays non-baseline feature configuration failure log.
	mismatch	Displays configured non-baseline features that are causing a mismatch.
	switch <i>switch-number</i>	(Optional) Displays configured non-baseline features that are causing a mismatch for the specified switch. The range is 1 to 8.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines 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.

This example shows how to display switch stack compatibility information:

```
Device# show platform stack compatibility configuration current
```

show platform stack compatibility feature

To display switch stack state machine and message trace feature compatibility information, use the **show platform stack compatibility feature** command in privileged EXEC mode.

```
show platform stack compatibility feature {all|independent [feature-id feature-id]|interdependent
[feature-id feature-id]|port [feature-id feature-id]}
```

Syntax Description	all	Displays all non-baseline features.
	independent	Displays switch-level independent features.
	feature-id <i>feature-id</i>	(Optional) Displays switch-level independent, system-level interdependent or port-level independent features with the specified feature ID.
	interdependent	Displays system-level interdependent features.
	port	Displays port-level independent features.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines The **show platform stack compatibility** commands display feature incompatibility information between stack members in a mixed stack. Compatibility checks ensure that features that are supported across members of a stack using a forwarding ASIC with different capabilities will function effortlessly and error free.

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.

This example shows how to display all non-baseline features:

```
Device# show platform stack compatibility feature all
      System Level Interdependent Features
=====
1: FHRR hardware vlan entry sharing feature
2: Jumbo MTU Routing Support
3: VRF on PVLAN interface
4: Global VRF config with greater than MAX policies
5: Routing keyword in IPv6 ACL
6: Ahp keyword in IPv6 ACL
7: Unsupported prefixes in IPv6 ACL
8: Unicast Reverse Path Forwarding
9: Multiple FHRP support
10: Gateway Load Balancing ProtocolVLAN-based FSPAN
11: CTS tagging and role-based enforcement
12: SPAN support 4 source session
13: Unknown
```

Switch Level Independent Features

=====

Port Level Independent Features

=====

- 1: Routing keyword in IPv6 ACL
- 2: Ahp keyword in IPv6 ACL
- 3: Unsupported prefixes in IPv6 ACL
- 4: Port-based FSPAN
- 5: IPv6 QoS match protocol support
- 6: IPv6 QoS ipv6 named ACL support

show platform stack compatibility table

To display feature compatibility tables for the switch stack, use the **show platform stack compatibility table** command in privileged EXEC mode.

show platform stack compatibility table {all | independent | interdependent | port}

Syntax Description	all	Displays all feature compatibility tables.
	independent	Displays a switch-level independent feature compatibility table.
	interdependent	Displays a system-level interdependent feature compatibility table.
	port	Displays a port-level independent feature compatibility table.
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

The **show platform stack compatibility** commands display feature incompatibility information between stack members in a mixed stack. Compatibility checks ensure that features that are supported across members of a stack using a forwarding ASIC with different capabilities will function effortlessly and error free.

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.

This example shows how to display all feature compatibility tables:

```
Device# show platform stack compatibility feature all
      System Level Interdependent Feature Matrix
=====
1: FHRR hardware vlan entry sharing feature
   Supported by switch versions: 1 3 4
2: Jumbo MTU Routing Support
   Supported by switch versions: 1 3 4
3: VRF on PVLAN interface
   Supported by switch versions: 1 3 4
4: Global VRF config with greater than MAX policies
   Supported by switch versions: 1 3 4
5: Routing keyword in IPv6 ACL
   Supported by switch versions: 1 3 4
6: Ahp keyword in IPv6 ACL
   Supported by switch versions: 1 3 4
7: Unsupported prefixes in IPv6 ACL
   Supported by switch versions: 1 3 4
8: Unicast Reverse Path Forwarding
   Supported by switch versions: 1 3 4
9: Multiple FHRP support
   Supported by switch versions: 1 3 4
```

```

10: Gateway Load Balancing ProtocolVLAN-based FSPAN
    Supported by switch versions: 1 2 3 4
11: CTS tagging and role-based enforcement
    Supported by switch versions: 1 3 4
12: SPAN support 4 source session
    Supported by switch versions: 3
13: Unknown
    Supported by switch versions: 4

```

Switch Level Independent Feature Matrix

```
=====
```

Port Level Independent Feature Matrix

```
=====
```

```

1: Routing keyword in IPv6 ACL
    Supported by ASIC versions: 1 2 3
2: Ahp keyword in IPv6 ACL
    Supported by ASIC versions: 1 2 3
3: Unsupported prefixes in IPv6 ACL
    Supported by ASIC versions: 1 2 3
4: Port-based FSPAN
    Supported by ASIC versions: 1 2 3
5: IPv6 QoS match protocol support
    Supported by ASIC versions: 1 2 3
6: IPv6 QoS ipv6 named ACL support
    Supported by ASIC versions: 1 2 3

```

show platform stack manager

To display platform-dependent switch-stack information, use the **show platform stack manager** command in privileged EXEC mode.

```
show platform stack manager {all | counters | trace [{cs [cs] | sdp [reverse] | state [reverse] | tdm}]}
```

Syntax Description

all	Displays all information for the entire switch stack.
counters	Displays the stack manager counters.
trace	Displays trace information.
cs	(Optional) Displays information about changes in stack-related trace messages.
sdp	(Optional) Displays Stack Discovery Protocol (SDP) information.
reverse	(Optional) Displays trace information in reverse chronological order (from recent to older chronological sequence).
state	(Optional) Displays stack state machine information.
tdm	(Optional) Displays information about topology discovery including a summary of the stacking over Ethernet state machine events and messages.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

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.



Note This command is supported only on stacking-capable switches.

The summary information about the switch stack shows these states:

- **Waiting**—A switch is booting up and waiting for communication from other switches in the stack. The switch has not determined whether or not it is active switch.

Stack members not participating in election remain in the waiting state until the active switch is elected and ready.

- **Initializing**—A switch has determined whether it is the active switch. If not, the switch receives its system- and interface-level configuration from the active switch and loads it.
- **Ready**—The member has completed loading the system- and interface-level configurations and can forward traffic.
- **Ver Mismatch**—A switch in version mismatch mode. Version-mismatch mode is when a switch that joins the stack has a different stack protocol minor version number than the active switch.

A typical state transition for a stack member (including the active) booting up is Waiting > Initializing > Ready.

A typical state transition for a stack member to active switch after an election is Ready > Re-Init > Ready.

A typical state transition for a stack member in version mismatch (VM) mode is Waiting > Ver Mismatch.

show switch

To display information that is related to the stack member or the switch stack, use the **show switch** command in EXEC mode.

show switch [{*stack-member-number* | **detail** | **neighbors** | **stack-ports** | **stack-ring speed**}]



Note This command is supported only on Catalyst 2960-X switches running the LAN Base image.

Syntax Description

stack-member-number (Optional) Number of the stack member. The range is 1 to 8.

detail (Optional) Displays detailed information about the stack ring.

neighbors (Optional) Displays the neighbors of the entire switch stack.

stack-ports (Optional) Displays port information for the entire switch stack.

stack-ring (Optional) Displays information about the stack ring.

speed Displays the stack ring speed.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

This command output displays these states:

- **Waiting**—A switch is booting up and waiting for communication from other switches in the stack. The switch has not determined whether or not it is an active stack.
Stack members not participating in a active stack election remain in the waiting state until the active stack is elected and ready.
- **Initializing**—A switch has determined whether it has the active stack status. If it is not the active stack, it receives and loads the system- and interface-level configuration from the active stack.
- **Ready**—The member has completed loading the system- and interface-level configurations and can forward traffic.
- **Ver Mismatch**—A switch in version mismatch mode. Version-mismatch mode is when a switch joining the stack has a different stack protocol minor version number than the active stack.
- **SDM Mismatch**—A switch in Switch Database Management (SDM) mismatch mode. SDM mismatch is when a member does not support the SDM template running on the active stack.

- **Provisioned**—The state of a preconfigured switch before it becomes an active member of a switch stack, or the state of a stack member after it has left the switch stack. The MAC address and the priority number in the display are always 0 for the provisioned switch.

A typical state transition for a stack member (including the active) booting up is Waiting > Initializing > Ready.

A typical state transition for a stack member becoming the active stack after the election is Ready > Re-Init > Ready.

A typical state transition for a stack member in version mismatch (VM) mode is Waiting > Ver Mismatch.

You can use the **show switch** command to identify whether the provisioned switch exists in the switch stack. The **show running-config** and the **show startup-config** privileged EXEC commands do not provide this information.

The display also includes stack MAC-persistence wait-time if persistent MAC address is enabled.

Examples

This example shows how to display summary stack information:

```
Device# show switch
Switch/Stack Mac Address : d4a0.2a37.4800
```

Switch#	Role	Mac Address	Priority	H/W Version	Current State
1	Member	0cd9.9624.f980	7	4	Ready
*2	Master	d4a0.2a37.4800	1	4	Ready
6	Member	0003.e31a.1e00	2	4	Ready

This example shows how to display detailed stack information:

```
Device# show switch detail
Switch/Stack Mac Address : d4a0.2a37.4800
```

Switch#	Role	Mac Address	Priority	H/W Version	Current State
1	Member	0cd9.9624.f980	7	4	Ready
*2	Master	d4a0.2a37.4800	8	4	Ready
6	Member	0003.e31a.1e00	2	0	Ready

Switch#	Stack Port Status		Neighbors	
	Port 1	Port 2	Port 1	Port 2
1	Ok	Down	2	None
2	Down	Ok	None	1
6	Down	Ok	None	1

This example shows how to display the member 6 summary information:

```
Device# show switch 6
```

Switch#	Role	Mac Address	Priority	State
6	Member	0003.e31a.1e00	1	Ready

This example shows how to display the neighbor information for a stack:

```
Device# show switch neighbors
Switch #      Port A      Port B
```

```
-----
      6      None      8
      8      6        None
```

This example shows how to display stack-port information:

```
Device# show switch stack-ports
Switch #   Port A   Port B
-----
      6     Down     Ok
      8     Ok      Down
```

Related Topics

- [reload](#), on page 544
- [remote command](#), on page 546
- [session](#), on page 547
- [switch stack port](#), on page 561
- [switch provision](#), on page 564
- [switch renumber](#), on page 566

stack-mac persistent timer

To enable the persistent MAC address feature, use the **stack-mac persistent timer** command in global configuration mode on the switch stack or on a standalone switch. To disable the persistent MAC address feature, use the **no** form of this command.

stack-mac persistent timer [*{0time-value}*]

no stack-mac persistent timer

Syntax Description	0 (Optional) Continues using the MAC address of the current active switch after a new active switch takes over.
	<i>time-value</i> (Optional) Time period in minutes before the stack MAC address changes to that of the new active switch. The range is 1 to 60 minutes. When no value is entered, the default is 4 minutes. We recommend that you configure an explicit value for this command.

Command Default	Persistent MAC address is disabled. The MAC address of the stack is always that of the first active switch. When the command is entered with no value, the default time before the MAC address changes is four minutes. We recommend that you configure an explicit value for this command.
------------------------	---

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines	The MAC address of the switch stack is determined by the MAC address of the active switch. In the default state (persistent MAC address disabled), if a new switch becomes active switch, the stack MAC address changes to the MAC address of the new active switch.
-------------------------	--

When persistent MAC address is enabled, the stack MAC address does not change for a time period. During that time, if the previous active switch rejoins the stack as a stack member, the stack retains its MAC address for as long as that switch is in the stack. If the previous active switch does not rejoin the stack during the specified time period, the switch stack takes the MAC address of the new active switch as the stack MAC address.

You can set the time period to be from 0 to 60 minutes.

- If you enter the command with no value, the default delay is 4 minutes.
- If you enter **0**, the stack continues to use the current stack MAC address until you enter the **no stack-mac persistent timer** command.
- If you enter a time delay of 1 to 60 minutes, the stack MAC address of the previous active switch is used until the configured time period expires or until you enter the **no stack-mac persistent timer** command.



Note When you enter the **stack-mac persistent timer** command with or without keywords, a message appears warning that traffic might be lost if the old active switch MAC address appears elsewhere in the network domain. You should use this feature cautiously.

If you enter the **no stack-mac persistent timer** command after a switchover, before the time expires, the switch stack moves to the current stack's active switch MAC address.

If the whole stack reloads, when it comes back up, the MAC address of the active switch is the stack MAC address.

Examples

This example shows how to configure the persistent MAC address feature, with the warning messages for each configuration. It also shows how to verify the configuration:

```
Device(config)# stack-mac persistent timer

WARNING: Use of an explicit timer value with the command is recommended.
WARNING: Default value of 4 minutes is being used.
WARNING: The stack continues to use the base MAC of the old Master
WARNING: as the stack-mac after a master switchover until the MAC
WARNING: persistency timer expires. During this time the Network
WARNING: Administrators must make sure that the old stack-mac does
WARNING: not appear elsewhere in this network domain. If it does,
WARNING: user traffic may be blackholed.

Device(config)# stack-mac persistent timer 0

WARNING: Stack MAC persistency timer value of 0 means that, after a
WARNING: master switchover, the current stack-mac will continue
WARNING: to be used indefinitely.
WARNING: The Network Administrators must make sure that the old
WARNING: stack-mac does not appear elsewhere in this network
WARNING: domain. If it does, user traffic may be blackholed.

Device(config)# stack-mac persistent timer 7

WARNING: The stack continues to use the base MAC of the old Master
WARNING: as the stack-mac after a master switchover until the MAC
WARNING: persistency timer expires. During this time the Network
WARNING: Administrators must make sure that the old stack-mac does
WARNING: not appear elsewhere in this network domain. If it does,
WARNING: user traffic may be blackholed.

Device(config)# end
Device(config)# show switch

Switch/Stack Mac Address : 0cd9.9624.dd80
Mac persistency wait time: 7 mins

          H/W   Current
Switch#  Role   Mac Address      Priority Version  State
-----
*1       Master 0cd9.9624.dd80    1         4         Ready
```

You can verify your settings by entering either of two privileged EXEC commands:

- **show running-config**—If enabled, **stack-mac persistent timer** and the time in minutes appears in the output.

- **show switch**—If enabled, **Mac persistency wait time** and the number of minutes appears in the output.

Related Topics

[show switch](#), on page 555

switch stack port

To disable or enable the specified stack port on the member, use the **switch** command in privileged EXEC mode on a stack member.

```
switch stack-member-number stack port port-number {disable | enable}
```



Note This command is supported only on Catalyst 2960-X switches running the LAN Base image.

Syntax Description

stack-member-number Current stack member number. The range is 1 to 8.

stack port *port-number* Specifies the stack port on the member. The range is 1 to 2.

disable Disables the specified port.

enable Enables the specified port.

Command Default

The stack port is enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

A stack is in the full-ring state when all members are connected through the stack ports and are in the ready state.

The stack is in the partial-ring state when the following occurs:

- All members are connected through their stack ports but some are not in the ready state.
- Some members are not connected through the stack ports.



Note Be careful when using the **switch** *stack-member-number* **stack port** *port-number* **disable** command. When you disable the stack port, the stack operates at half bandwidth.

If you enter the **switch** *stack-member-number* **stack port** *port-number* **disable** privileged EXEC command and the stack is in the full-ring state, you can disable only one stack port. This message appears:

```
Enabling/disabling a stack port may cause undesired stack changes. Continue?[confirm]
```

If you enter the **switch** *stack-member-number* **stack port** *port-number* **disable** privileged EXEC command and the stack is in the partial-ring state, you cannot disable the port. This message appears:

```
Disabling stack port not allowed with current stack configuration.
```

Examples

This example shows how to disable stack port 2 on member 4:

```
Device# switch 4 stack port 2 disable
```

Related Topics

[show switch](#), on page 555

switch priority

To change the stack member priority value, use the **switch priority** command in global configuration mode on the active switch.

switch *stack-member-number* **priority** *new-priority-value*

Syntax Description

stack-member-number Current stack member number. The range is 1 to 8.

new-priority-value New stack member priority value. The range is 1 to 15.

Command Default

The default priority value is 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

The new priority value is a factor when a new active switch is elected. When you change the priority value, the active switch is not changed immediately.

Examples

This example shows how to change the priority value of stack member 6 to 8:

```
Device(config)# switch 6 priority 8
Changing the Switch Priority of Switch Number 6 to 8
Do you want to continue?[confirm]
```

Related Topics

- [reload](#), on page 544
- [session](#), on page 547
- [show switch](#), on page 555
- [switch renumber](#), on page 566

switch provision

To supply a configuration to a new switch before it joins the switch stack, use the **switch provision** command in global configuration mode on the active switch. To delete all configuration information that is associated with the removed switch (a stack member that has left the stack), use the **no** form of this command.

switch *stack-member-number* **provision** *type*
no switch *stack-member-number* **provision**

Syntax Description	
	<i>stack-member-number</i> Stack member number. The range is 1 to 8.
	<i>type</i> Switch type of the new switch before it joins the stack.

Command Default The switch is not provisioned.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

For *type*, enter the model number of a supported switch that is listed in the command-line help strings.

To avoid receiving an error message, you must remove the specified switch from the switch stack before using the **no** form of this command to delete a provisioned configuration.

To change the switch type, you must also remove the specified switch from the switch stack. You can change the stack member number of a provisioned switch that is physically present in the switch stack if you do not also change the switch type.

If the switch type of the provisioned switch does not match the switch type in the provisioned configuration on the stack, the switch stack applies the default configuration to the provisioned switch and adds it to the stack. The switch stack displays a message when it applies the default configuration.

Provisioned information appears in the running configuration of the switch stack. When you enter the **copy running-config startup-config** privileged EXEC command, the provisioned configuration is saved in the startup configuration file of the switch stack.



Caution When you use the **switch provision** command, memory is allocated for the provisioned configuration. When a new switch type is configured, the previously allocated memory is not fully released. Therefore, do not use this command more than approximately 200 times, or the switch will run out of memory and unexpected behavior will result.

Examples

This example shows how to provision a switch with a stack member number of 2 for the switch stack. The **show running-config** command output shows the interfaces associated with the provisioned switch.

```
Device(config)# switch 2 provision WS-xxxx
Device(config)# end
```

```
Device# show running-config | include switch 2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
<output truncated>
```

You also can enter the **show switch** user EXEC command to display the provisioning status of the switch stack.

This example shows how to delete all configuration information about stack member 5 when the switch is removed from the stack:

```
Device(config)# no switch 5 provision
```

You can verify that the provisioned switch is added to or removed from the running configuration by entering the **show running-config** privileged EXEC command.

Related Topics

[show switch](#), on page 555

switch renumber

To change the stack member number, use the **switch renumber** command in global configuration mode on the active switch.

switch *current-stack-member-number* **renumber** *new-stack-member-number*

Syntax Description

current-stack-member-number Current stack member number. The range is 1 to 8.

new-stack-member-number New stack member number for the stack member. The range is 1 to 8.

Command Default

The default stack member number is 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

If another stack member is already using the member number that you just specified, the active switch assigns the lowest available number when you reload the stack member.



Note

If you change the number of a stack member, and no configuration is associated with the new stack member number, that stack member loses its current configuration and resets to its default configuration.

Do not use the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* command on a provisioned switch. If you do, the command is rejected.

Use the **reload slot** *current stack member number* privileged EXEC command to reload the stack member and to apply this configuration change.

Examples

This example shows how to change the member number of stack member 6 to 7:

```
Device(config)# switch 6 renumber 7
```

```
WARNING:Changing the switch number may result in a configuration change for that switch.
The interface configuration associated with the old switch number will remain as a provisioned
configuration.
```

```
Do you want to continue?[confirm]
```

Related Topics

- [reload](#), on page 544
- [session](#), on page 547
- [show switch](#), on page 555
- [switch stack port](#), on page 561

switch stack port-speed 10

To set the switch stack port speed to 10 Gbps and enable mixed stacking with one or more Catalyst 2960-S switches, use the **switch stack port-speed 10** command in global configuration mode. To return to the default setting, use the **no** form of this command.

```
switch stack port-speed 10
no switch stack port-speed
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	The default port speed is 20 Gbps.
------------------------	------------------------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines	By default, Catalyst 2960-X switches operate at a port speed of 20 Gbps while 2960-S switches have a maximum port speed of 10 Gbps. In a mixed stack of Catalyst 2960-X and Catalyst 2960-S switches, the stack must operate at the port speed of the Catalyst 2960-S switch; otherwise, the switches will not stack.
-------------------------	---

To set the port speed of the stack to 10 Gbps, use the **switch stack port-speed 10** global configuration command on a Catalyst 2960-X stack member before you add a Catalyst 2960-S switch to the stack, and then reload the stack.

This example shows how to set the switch stack port speed to 10 Gbps and then reload the stack:

```
Device(config)# switch stack port-speed 10
WARNING: Changing the stack speed may result in a stack speed mismatch.
Do you want to continue?[confirm]
New stack speed will be effective after next reload

Device(config)# exit
Device# reload
System configuration has been modified. Save? [yes/no]:
```

You can verify your settings by entering the **show switch stack-ring speed** privileged EXEC command.

switch stack port-speed 10



PART IX

System Management

- [System Management Commands, on page 571](#)



System Management Commands

- [archive download-sw](#), on page 574
- [archive tar](#), on page 578
- [archive upload-sw](#), on page 582
- [avc dns-as client](#), on page 584
- [show logging smartlog](#), on page 586
- [boot](#), on page 588
- [boot buffersize](#), on page 589
- [boot enable-break](#), on page 590
- [boot host dhcp](#), on page 591
- [boot host retry timeout](#), on page 592
- [boot manual](#), on page 593
- [boot system](#), on page 594
- [cat](#), on page 595
- [clear logging onboard](#), on page 596
- [clear mac address-table](#), on page 597
- [clear mac address-table move update](#), on page 598
- [clear nmsp statistics](#), on page 599
- [cluster commander-address](#), on page 600
- [cluster discovery hop-count](#), on page 602
- [cluster enable](#), on page 603
- [cluster holdtime](#), on page 604
- [cluster member](#), on page 605
- [cluster outside-interface](#), on page 607
- [cluster run](#), on page 608
- [cluster timer](#), on page 609
- [copy](#), on page 610
- [debug cluster](#), on page 611
- [debug matm move update](#), on page 612
- [delete](#), on page 613
- [dir](#), on page 614
- [help](#), on page 616
- [hw-module](#), on page 617
- [ip name-server](#), on page 619

- license boot level, on page 621
- logging, on page 622
- logging buffered, on page 623
- logging console, on page 624
- logging file flash, on page 625
- logging history, on page 626
- logging history size, on page 627
- logging monitor, on page 628
- logging trap, on page 629
- mac address-table aging-time, on page 630
- mac address-table learning vlan, on page 631
- logging smartlog, on page 633
- mac address-table notification, on page 634
- mac address-table static, on page 635
- mkdir, on page 636
- more, on page 637
- nmsp notification interval, on page 638
- rcommand, on page 640
- rename, on page 642
- reset, on page 643
- rmdir, on page 644
- service sequence-numbers, on page 645
- set, on page 646
- show avc dns-as client, on page 649
- show boot, on page 652
- show cable-diagnostics prbs, on page 654
- show cable-diagnostics tdr, on page 656
- show cluster, on page 658
- show cluster candidates, on page 660
- show cluster members, on page 662
- show ip name-server, on page 664
- show license right-to-use, on page 665
- show logging onboard, on page 668
- show mac address-table, on page 673
- show mac address-table address, on page 674
- show mac address-table aging-time, on page 675
- show mac address-table count, on page 676
- show mac address-table dynamic, on page 677
- show mac address-table interface, on page 678
- show mac address-table learning, on page 679
- show mac address-table move update, on page 680
- show mac address-table multicast, on page 681
- show mac address-table notification, on page 682
- show mac address-table secure, on page 684
- show mac address-table static, on page 685
- show mac address-table vlan, on page 686

- [show nmsp](#), on page 687
- [show onboard switch](#), on page 688
- [shutdown](#), on page 690
- [test cable-diagnostics prbs](#), on page 691
- [test cable-diagnostics tdr](#), on page 692
- [traceroute mac](#), on page 693
- [traceroute mac ip](#), on page 696
- [type](#), on page 698
- [unset](#), on page 699
- [version](#), on page 701

archive download-sw

To download a new image from a TFTP server to the switch or switch stack and to overwrite or keep the existing image, use the **archive download-sw** command in privileged EXEC mode.

```
archive download-sw {/directory | /force-reload | /imageonly | /leave-old-sw | /no-set-boot
| /no-version-check | /overwrite | /reload | /safe} source-url
```

Syntax Description

/directory	Specifies a directory for the images.
/force-reload	Unconditionally forces a system reload after successfully downloading the software image.
/imageonly	Downloads only the software image but not the HTML files associated with 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	Keeps the old software version after a successful download.
/no-set-boot	Stops the setting of the BOOT environment variable from being altered to point to the new software image after it is successfully downloaded.
/no-version-check	Downloads the software image without verifying its version compatibility with the image that is running on the switch. On a switch stack, downloads the software image without checking the compatibility of the stack protocol version on the image and on the stack. This feature is supported only on the LAN Base image.
/overwrite	Overwrites the software image in flash memory with the downloaded image.
/reload	Reloads the system after successfully downloading the image, unless the configuration has been changed and has not saved.
/safe	Keeps the current software image. Does 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.

<i>source-url</i>	<p>Specifies the source URL alias for a local or network file system. These options are supported:</p> <ul style="list-style-type: none"> The secondary boot loader (BS1): bsl: The local flash: file system on the standalone switch or the active switch: flash: The local flash: file system on a member: flash member number: FTP: ftp: <code>[[/username [:password] @location] /directory] /image-name.tar</code> An HTTP server: http: <code>[[/username:password] @] { hostname host-ip } [/directory] /image-name.tar</code> A secure HTTP server: https: <code>[[/username:password] @] { hostname host-ip } [/directory] /image-name.tar</code> Remote Copy Protocol (RCP): rcp: <code>[[/username@location] /directory] /image-name.tar</code> TFTP: tftp: <code>[[/location] /directory] /image-name.tar</code>
-------------------	--

image-name.tar is the software image to download and install on the switch.

Command Default

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 files are case-sensitive; the image file is provided in TAR format.

Compatibility of the stack protocol version of the image to be downloaded is checked with the version on the stack.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

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 you leave the software in place, the new image does not have enough flash memory due to space constraints, and an error message is displayed.

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 [delete, on page 613](#).

If you want to download an image that has a different stack protocol version than the one existing on the stack, use the **/no-version-check** option.



Note This feature is supported only on the LAN Base image.



Note Use the **/no-version-check** option carefully. All members, including the active switch, must have the same stack protocol version to be in the same stack.

This option allows an image to be downloaded without first confirming the compatibility of its stack protocol version with the version of the stack.

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 determines whether or not the new image is the same as the one on the switch flash device or is running on any stack members.

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.

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:

```
Device# 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:

```
Device# 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:

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

```
Device# archive download-sw /imageonly /destination-system 6 /destination-system 8  
tftp://172.20.129.10/test-image.tar
```

archive tar

To create a TAR file, list files in a TAR file, or extract the files from a TAR file, use the **archive tar** command in privileged EXEC mode.

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

Syntax Description

/create <i>destination-url</i> flash: / <i>file-url</i>	Creates a new TAR file on the local or network file system. <i>destination-url</i> —Specifies the destination URL alias for the local or network file system and the name of the tar file to create. These options are supported:
---	--

- The local flash file system:
flash:
- FTP:
ftp: [[//*username* [:*password*] @*location*] /*directory*] /*tar-filename.tar*
- An HTTP server:
http: //[[*username:password*] @] { *hostname* | *host-ip* } [/*directory*] /*image-name.tar*
- A secure HTTP server:
https: //[[*username:password*] @] { *hostname* | *host-ip* } [/*directory*] /*image-name.tar*
- Remote Copy Protocol (RCP):
rcp: [[//*username*@*location*] /*directory*] /*tar-filename.tar*
- TFTP:
tftp: [[//*location*] /*directory*] /*image-name.tar*

tar-filename.tar is the TAR file to be created.

flash:/*file-url*—Specifies the location on the local flash: file system from which the new tar file is created.

Optionally, you can specify the list of files list of files or directories within the source directory that you want to be written 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* Displays the contents of an existing TAR file to the screen.

source-url—Specifies the source URL alias for the local or network file system. These options are supported:

- The local flash: file system:

flash:

- FTP:

ftp: [[/*username* [: *password*] @ *location*] / *directory*] / *itar-filename.tar*

- An HTTP server:

http: //[[*username:password*] @] { *hostname* | *host-ip* } [/ *directory*] / *image-name.tar*

- A secure HTTP server:

https: //[[*username:password*] @] { *hostname* | *host-ip* } [/ *directory*] / *image-name.tar*

- Remote Copy Protocol (RCP):

rcp: [[/*username@location*] / *directory*] / *tar-filename.tar*

- TFTP:

tftp: [[/*location*] / *directory*] / *image-name.tar*

tar-filename.tar is the TAR file to be displayed.

/xtract	Extracts files from a TAR file to the local file system.
<i>source-url</i>	
flash: <i>/file-url</i> [<i>dir/file . . .</i>]	<i>source-url</i> —Specifies the source URL alias for the local file system. These options are supported:
	<ul style="list-style-type: none"> The local flash: file system: flash: FTP: ftp: [[<i>/username</i> [<i>:password</i>] @<i>location</i>]/<i>directory</i>]/<i>tar-filename.tar</i> An HTTP server: http: //[[<i>username:password</i>] @] {<i>hostname</i> <i>host-ip</i>} [<i>/directory</i>]/<i>image-name.tar</i> A secure HTTP server: https: //[[<i>username:password</i>] @] {<i>hostname</i> <i>host-ip</i>} [<i>/directory</i>]/<i>image-name.tar</i> Remote Copy Protocol (RCP): rcp: [[<i>/username@location</i>]/<i>directory</i>]/<i>tar-filename.tar</i> TFTP: tftp: [[<i>/location</i>]/<i>directory</i>]/<i>image-name.tar</i>

tar-filename.tar is the TAR file from which to extract.

flash:*/file-url* [*dir/file . . .*]—Specifies the location on the local flash: file system from which the new 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.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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: file device to a file named *saved.tar* on the TFTP server at 172.20.10.30:

```
Device# archive tar /create tftp:172.20.10.30/saved.tar flash:/new_configs
```

This example shows how to display the contents of the file that is in flash memory. The contents of the TAR file appear on the screen:

```
Device# archive tar /table flash:c2960-lanbase-tar.12-25.FX.tar
info (219 bytes)
(directory)
(610856 bytes)
  info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the /html directory and its contents:

```
flash:2960-lanbase-mz.12-25.FX.tar 2960-lanbase-mz.12-25.FX/html
(directory)
(556 bytes)
(9373 bytes)
(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 not extracted.

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

archive upload-sw

To upload an existing image to the server, use the **archive upload-sw** privileged EXEC command.

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

Syntax Description	<p>/version (Optional) Specifies the specific version string of the image to be uploaded. <i>version_string</i></p> <hr/> <p>destination-url The destination URL alias for a local or network file system. These options are supported:</p> <ul style="list-style-type: none"> • The local flash: file system on the standalone switch or the active switch: flash: • The local flash: file system on a member: flash member number: • FTP: ftp: [[/username [:password] @location] /directory] /image-name.tar • An HTTP server: http: [[/username:password] @] { hostname host-ip } [/directory] /image-name.tar • A secure HTTP server: https: [[/username:password] @] { hostname host-ip } [/directory] /image-name.tar • Secure Copy Protocol (SCP): scp: [[/username@location] /directory] /image-name.tar • Remote Copy Protocol (RCP): rcp: [[/username@location] /directory] /image-name.tar • TFTP: tftp: [[/location] /directory] /image-name.tar <p><i>image-name.tar</i> is the name of the software image to be stored on the server.</p>
---------------------------	--

Command Default	Uploads the currently running image from the flash: file system.
------------------------	--

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Use the upload feature only if the HTML files associated with 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 on member switch 3 to a TFTP server at 172.20.140.2:

```
Switch# archive upload-sw /source-system-num 3tftp://172.20.140.2/test-image.tar
```

avc dns-as client

To enable Application Visibility Control (AVC) with Domain Name System as an Authoritative Source (DNS-AS) feature (AVC with DNS-AS) on the switch (DNS-AS client) and maintain a list of trusted domains, enter the **avc dns-as client** in global configuration mode

avc dns-as client [**enable** | **trusted-domains** [**domain** *domain-name*]]

no avc dns-as client [**enable** | **trusted-domains** [**domain** *domain-name*]]]

Syntax Description		
enable		Enables AVC with DNS-AS on the DNS-AS client.
trusted-domains [domain <i>domain-name</i>]		Enter the domain name you would like to add to the list of trusted domains for the DNS-AS client. All remaining domains are ignored and will follow default forwarding behavior. You can enter up to 50 domains. You can use regular expressions to match the domain name.

Command Default AVC with DNS-AS is disabled.

Command Modes Global configuration mode
Trusted domain configuration mode

Command History	Release	Modification
	Cisco IOS Release 15.2(5)E1	This command was introduced.

Usage Guidelines When you use regular expressions to match a domain name, for example, to represent all the domains for an organization, if you enter:

```
Device(config-trusted-domains)# domain *.example.*
```

The DNS-AS client matches `www.example.com`, `ftp.example.org` and any other domain that pertains to the organization “example”. Use such an entry in the trusted domain list carefully, because it increases the size of the binding table considerably. Entries in the trusted domain list affect the binding table, because the table serves as a database of parsed DNS server responses, which (among other things) contains the domain name and IP address information.

Example

The following example shows how to enable AVC with DNS-AS:

```
Device# configure terminal
Device(config)# avc dns-as client enable
```

The following example shows how to make entries in the trusted domain list:

```
Device# configure terminal
Device(config)# trusted-domains
```

```
Device(config-trusted-domains)# domain www.example.com
Device(config-trusted-domains)# domain example.com
Device(config-trusted-domains)# domain www.example.net
Device(config-trusted-domains)# domain example.net
Device(config-trusted-domains)# domain www.example.org
Device(config-trusted-domains)# domain example.org
```

Related Commands

Command	Description
show avc dns-as client, on page 649	Displays the various AVC with DNS-AS settings you have configured.

show logging smartlog

To display smart logging information, use the **show logging smartlog** command in privileged EXEC mode.

show logging smartlog [**event-ids** | **events** | **statistics** {**interface** *interface-id* | **summary**}]

Syntax Description	event-ids	(Optional) Displays the IDs and names of smart log events. The NetFlow collector uses the event IDs to identify each event.
	events	(Optional) Displays descriptions of smart log events. The display shows the last 10 smart logging events.
	statistics	(Optional) Displays smart log statistics.
	interface <i>interface-id</i>	(Optional) Displays smart log statistics for the specified interface.
	summary	(Optional) Displays a summary of the smart log event statistics.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines You can configure smart logging of packets dropped because of DHCP snooping violations, Dynamic ARP inspection violations, IP source guard denied traffic, or ACL permitted or denied traffic. The packet contents are sent to the identified Cisco IOS NetFlow collector.

The statistics counters reflect the number of packets that have been sent to the collector by smart logging.

Examples

This example shows output from the **show logging smartlog event-ids** command:

```
Switch# show logging smartlog event-ids
EventID: 1 Description: DHCPSP
Extended Events:
-----
ID | Description
-----
1 | DHCPSP_DENY_INVALID_MSGTYPE
2 | DHCPSP_DENY_INVALID_PKTLEN
3 | DHCPSP_DENY_INVALID_BIND
4 | DHCPSP_DENY_INVALID_OPT
5 | DHCPSP_DENY_OPT82_DISALLOW
6 | DHCPSP_DENY_SRCMAC_MSMTCH

EventID: 2 Description: DAI
Extended Events:
-----
```

```

ID | Description
-----
1  | DAI_DENY_INVALID_BIND
2  | DAI_DENY_INVALID_SRCMAC
3  | DAI_DENY_INVALID_IP
4  | DAI_DENY_ACL
5  | DAI_DENY_INVALID_PKT
6  | DAI_DENY_INVALID_DSTMAC

```

EventID: 3 Description: IPSG

Extended Events:

```

ID | Description
-----
1  | IPSG_DENY

```

EventID: 4 Description: ACL

Extended Events:

```

ID | Description
-----
1  | PACL_PERMIT
2  | PACL_DENY

```

This example shows output from the **show logging smartlog statistics interface** command:

```
Switch# show logging smartlog statistics interface gigabitethernet1/0
```

Total number of DHCP Snooping logged packets: 0

DHCPSNP_DENY_INVALID_MSGTYPE: 0

DHCPSNP_DENY_INVALID_PKTLEN: 0

DHCPSNP_DENY_INVALID_BIND: 0

DHCPSNP_DENY_INVALID_OPT: 0

DHCPSNP_DENY_OPT82_DISALLOW: 0

DHCPSNP_DENY_SRCMAC_MSMTCH: 0

Total number of Dynamic ARP Inspection logged packets: 0

DAI_DENY_INVALID_BIND: 0

DAI_DENY_INVALID_SRCMAC: 0

DAI_DENY_INVALID_IP: 0

DAI_DENY_ACL: 0

DAI_DENY_INVALID_PKT: 0

DAI_DENY_INVALID_DSTMAC: 0

Total number of IP Source Guard logged packets: 793

IPSG_DENY: 793

Total number of ACL logged packets: 10135

PACL_PERMIT: 10135

PACL_DENY: 0

boot

To load and boot an executable image and display the command-line interface (CLI), use the **boot** command in boot loader mode.

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 launching.	
-p	(Optional) Pause for the JTAG Debugger right after loading the image.	
<i>filesystem:</i>	Alias for a file system. Use flash: for the system board flash device; use usbflash0: for USB memory sticks.	
<i>/file-url</i>	Path (directory) and name of a bootable image. Separate image names with a semicolon.	

Command Default No default behavior or values.

Command Modes Boot loader

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

When you enter the **boot** command without any arguments, the device 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 specify 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.

Example

This example shows how to boot the device using the *new-image.bin* image:

```
Device: set BOOT flash:/new-images/new-image.bin
Device: boot
```

After entering this command, you are prompted to start the setup program.

boot buffersize

To configure the NVRAM buffer size, use the **boot buffersize** global configuration command.

boot buffersize *size*

Syntax Description

size The NVRAM buffer size in KB. The valid range is from 4096 to 1048576.

Command Default

The default NVRAM buffer size is 512 KB.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

After you configure the NVRAM buffer size, reload the switch or switch stack.

When you add a switch to a stack and the NVRAM size differs, the new switch synchronizes with the stack and reloads automatically.

Example

The following example sets the buffer size to 524288 KB:

```
Switch(config)# boot buffersize 524288
```

boot enable-break

To enable the interruption of the automatic boot process on a standalone switch, use the **boot enable-break** global configuration command. 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.

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

This command works properly only from a standalone switch. 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 setting 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.

boot host dhcp

To configure the switch to download files from a DHCP server, use the **boot host dhcp** global configuration command.

boot host dhcp

Syntax Description	This command has no arguments or keywords.	
Command Default	None	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Example

This example uses the **boot host dhcp** command to enable auto-configuration with a saved configuration.

```
Switch(config)# boot host dhcp
```

boot host retry timeout

To set the amount of time for which the system tries to download a configuration file, use the **boot host retry timeout** global configuration command.

boot host retry timeout *timeout-value*

Syntax Description	<i>timeout-value</i> The length of time before the system times out, after trying to download a configuration file.				
Command Default	There is no default. If you do not set a timeout, the system indefinitely tries to obtain an IP address from the DHCP server.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.				

Example

This example sets the timeout to 300 seconds:

```
Switch(config)# boot host retry timeout 300
```

boot manual

To enable the ability to manually boot a standalone switch during the next boot cycle, use the **boot manual** global configuration command. 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.

Command Default Manual booting is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines This command works properly only from a standalone switch.

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.

boot system

To specify the name of the configuration file that is used as a boot image, use the **boot system** global configuration command.

boot system *filename* [**switch** {*switch number* | **all**}]

Syntax Description	
<i>filename</i>	The name of the boot image configuration file.
switch	(Optional) Sets the system image for switches in the stack.
<i>switch number</i>	The switch number.
all	Sets the system image for all switches in the stack.

Command Default None

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Example

The following example specifies the name of the boot image configuration file as *config-boot.text*:

```
Switch(config)# boot system config-boot.text
```

cat

To display the contents of one or more files, use the **cat** command in boot loader mode.

cat *filesystem:/file-url...*

Syntax Description

filesystem: Specifies a file system.

/file-url Specifies the path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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 an image file:

```
Device: cat flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

clear logging onboard

To clear all of the on-board failure logging (OBFL) data, use the **clear logging onboard** privileged EXEC command on the switch stack or on a standalone switch. The command clears all of the OBFL data except for the uptime and CLI-command information stored in the flash memory.

clear logging onboard [**module** {*switch-number* | **all**}]



Note This command is supported only on the LAN Base image.

Syntax Description	module	(Optional) Clears OBFL data on specified switches in the stack.
	<i>switch-number</i>	The identity of the specified switch. The range is from 1 to 4.
	all	(Optional) Clears OBFL data on all switches in the stack.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

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

Example

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 is deleted by entering the **show logging onboard** privileged EXEC command.

clear mac address-table

To delete a specific dynamic address, all dynamic addresses on a particular interface, all dynamic addresses on stack members,

or all dynamic addresses on a particular VLAN from the MAC address table, use the **clear mac address-table** privileged EXEC command.

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** }



Note This command is supported only on the LAN Base image.

Syntax Description

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

Command Default

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

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 is deleted by entering the **show mac address-table** privileged EXEC command.

clear mac address-table move update

To clear the mac address-table-move update-related counters, use the **clear mac address-table move update** privileged EXEC command.

clear mac address-table move update

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Example

This example shows how to clear the **mac address-table move** update-related counters.

```
Switch# clear mac address-table move update
```

You can verify that the information is cleared by entering the **show mac address-table move update** privileged EXEC command.

clear nmsp statistics

To clear the Network Mobility Services Protocol (NMSP) statistics, use the **clear nmsp statistics** command in EXEC mode.

clear nmsp statistics

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes User Exec
Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E
		This command was introduced.

The following is sample output from the **clear nmsp statistics** command and shows how to clear all statistics about NMSP information exchanged between the controller and the connected Cisco Mobility Services Engine (MSE):

```
Device> clear nmsp statistics
```

cluster commander-address

To specify the cluster command MAC address on a cluster member switch when the member has lost communication with the cluster command switch, use the

cluster commander-address global configuration command. Use the **no** form of this global configuration command from the

cluster member switch console 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		
	<i>mac-address</i>	The MAC address of the cluster command switch.
	member <i>number</i>	(Optional) Specifies the number of a configured cluster member switch. The range is 0 to 15.
	name <i>name</i>	(Optional) Specifies the name of the configured cluster up to 31 characters.

Command Default The switch is not a member of any cluster.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines This command is available only on the cluster command 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.

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 usually use this command from

the cluster member switch console port only when the member has lost communication with the cluster command switch. With a typical 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.

Example

The following example shows partial 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.

cluster discovery hop-count

To set the hop-count limit for extended discovery of candidate switches, use the **cluster discovery hop-count** global configuration command on the cluster command switch. 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	<i>number</i> The number of hops from the cluster edge that the cluster command switch limits the discovery of candidates. The range is 1 to 7.
---------------------------	---

Command Default	The default hop count is 3.
------------------------	-----------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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, extended discovery is disabled. 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.

Example

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.

cluster enable

To enable a command-capable switch as the cluster command switch, assign a cluster name, and optionally assign a member number to it, use the

cluster enable global configuration command. 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	<i>name</i>	The name of the cluster up to 31 characters. Valid characters include only alphanumerics, dashes, and underscores.
	<i>command-switch-member-number</i>	(Optional) A member number that is assigned to the cluster command switch of the cluster. The range is 0 to 15.

Command Default	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
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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.

Example

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.

cluster holdtime

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 **cluster holdtime** global configuration command on the cluster command switch. 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	<i>holdtime-in-secs</i> 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.
---------------------------	--

Command Default	The default holdtime is 80 seconds.
------------------------	-------------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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.

Example

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.

cluster member

To add candidates to a cluster, use the **cluster member** global configuration command on the cluster command switch.

Use the **no** form of the command to remove members from the cluster.

```
cluster member [n] mac-address H.H.H [password enable-password] [vlan vlan-id]  
no cluster member n
```

Syntax Description		
<i>n</i>	(Optional) The number that identifies a cluster member. The range is 0 to 15.	
mac-address <i>H.H.H</i>	Specifies the MAC address of the cluster member switch in hexadecimal format.	
password <i>enable-password</i>	(Optional) Enables the password of the candidate switch. The password is not required if there is no password on the candidate switch.	
vlan <i>vlan-id</i>	(Optional) Specifies the ID of the VLAN through which the candidate is added to the cluster by the cluster command switch. The range is 1 to 4094.	

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

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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 enabled 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.

Example

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.

cluster outside-interface

To configure the outside interface for cluster Network Address Translation (NAT), use the **cluster outside-interface** global configuration

command on the cluster command switch, 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 6. The VLAN range is 1 to 4094.

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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.

Example

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.

cluster run

To enable clustering on a switch, use the **cluster run** global configuration command. 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.

Command Default Clustering is enabled on all switches.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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.

Example

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

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

cluster timer

To set the number of seconds between heartbeat messages, use the **cluster timer** global configuration command on the cluster command switch. To set the interval to the default value, use the **no** form of the command

```
cluster timer interval-in-secs
no cluster timer
```

Syntax Description	<i>interval-in-secs</i> Interval in seconds between heartbeat messages. The range is 1 to 300 seconds.
---------------------------	--

Command Default	The default interval is 8 seconds.
------------------------	------------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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, the number of heartbeat messages that are missed in a row before a switch is declared down is calculated by dividing the number of seconds of holdtime by the

number of seconds in the interval.

Example

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.

copy

To copy a file from a source to a destination, use the **copy** command in boot loader mode.

copy *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description

<i>filesystem:</i>	Alias for a file system. Use usbflash0: for USB memory sticks.
<i>/source-file-url</i>	Path (directory) and filename (source) to be copied.
<i>/destination-file-url</i>	Path (directory) and filename of the destination.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 127 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 shows how to copy a file at the root:

```
Device: copy usbflash0:test1.text usbflash0:test4.text
File "usbflash0:test1.text" successfully copied to "usbflash0:test4.text"
```

You can verify that the file was copied by entering the **dir** *filesystem:* boot loader command.

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 | hrsp | http | ip [packet] | members |
nat | neighbors | platform | snmp | vqpxy}
no debug cluster {discovery | events | extended | hrsp | http | ip [packet] | members
| nat | neighbors | platform | snmp | vqpxy}
```

Syntax Description

discovery	Displays cluster discovery debug messages.
events	Displays cluster event debug messages.
extended	Displays extended discovery debug messages.
hrsp	Displays the Hot Standby Router Protocol (HSRP) debug messages.
http	Displays Hypertext Transfer Protocol (HTTP) debug messages.
ip [packet]	Displays IP or transport packet debug messages.
members	Displays cluster member debug messages.
nat	Displays Network Address Translation (NAT) debug messages.
neighbors	Displays cluster neighbor debug messages.
platform	Displays platform-specific cluster debug messages.
snmp	Displays Simple Network Management Protocol (SNMP) debug messages.
vqpxy	Displays VLAN Query Protocol (VQP) proxy debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

This command is available only on the cluster command switch stack or cluster command switch.

The **undebug cluster** command works the same as the **no debug cluster** command.

When you enable debugging, it is enabled only on the active switch. To enable debugging on a member switch, you can start a session from the active switch by using the **session switch-number** privileged EXEC command.

Then enter the **debug** command at the command-line prompt of the member switch.

You also can use the **remote command stack-member-number** LINE privileged EXEC command on the active switch to enable debugging on a member switch without first starting a session.

debug matm move update

To enable debugging of MAC address-table move update message processing, use the **debug matm move update** privileged EXEC command. Use the **no** form of this command to return to the default setting.

debug matm move update
no debug matm move update

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines The **undebug matm move update** command works the same as the **no debug matm move update** command.



Note This command is supported only on the LAN Base image.

When you enable debugging, it is enabled only on the active switch. To enable debugging on a member switch, you can start a session from the active switch by using the **session switch-number** privileged EXEC command.

Then enter the **debug** command at the command-line prompt of the member switch.

You can also use the **remote command stack-member-number LINE** privileged EXEC command on the active switch to enable debugging on a member switch without first starting a session.

delete

To delete one or more files from the specified file system, use the **delete** command in boot loader mode.

delete *filesystem:/file-url...*

Syntax Description

filesystem: Alias for a file system. Use **usbflash0:** for USB memory sticks.

/file-url... Path (directory) and filename to delete. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

The device prompts you for confirmation before deleting each file.

Examples

This example shows how to delete two files:

```
Device: delete usbflash0:test2.text usbflash0:test5.text
Are you sure you want to delete "usbflash0:test2.text" (y/n)?y
File "usbflash0:test2.text" deleted
Are you sure you want to delete "usbflash0:test5.text" (y/n)?y
File "usbflash0:test2.text" deleted
```

You can verify that the files were deleted by entering the **dir usbflash0:** boot loader command.

dir

To display the list of files and directories on the specified file system, use the **dir** command in boot loader mode.

dir *filesystem:/file-url*

Syntax Description	<i>filesystem:</i> Alias for a file system. Use flash: for the system board flash device; use usbflash0: for USB memory sticks.
	<i>/file-url</i> (Optional) Path (directory) and directory name that contain the contents you want to display. Separate each directory name with a space.

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Boot Loader Privileged EXEC
----------------------	--------------------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines	Directory names are case sensitive.
-------------------------	-------------------------------------

Examples	This example shows how to display the files in flash memory:
-----------------	--

```
Device: dir flash:
Directory of flash:/
  2  -rwx      561   Mar 01 2013 00:48:15  express_setup.debug
  3  -rwx  2160256   Mar 01 2013 04:18:48  c2960x-dmon-mz-150-2r.EX
  4  -rwx      1048   Mar 01 2013 00:01:39  multiple-fs
  6  drwx       512   Mar 01 2013 23:11:42  c2960x-universalk9-mz.150-2.EX
645 drwx       512   Mar 01 2013 00:01:11  dc_profile_dir
647 -rwx      4316   Mar 01 2013 01:14:05  config.text
648 -rwx         5   Mar 01 2013 00:01:39  private-config.text

96453632 bytes available (25732096 bytes used)
```

Table 36: dir Field Descriptions

Field	Description
2	Index number of the file.
-rwx	File permission, which can be any or all of the following: <ul style="list-style-type: none"> • d—directory • r—readable • w—writable • x—executable

Field	Description
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

help

To display the available commands, use the **help** command in boot loader mode.

help

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Boot loader

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Example

This example shows how to display a list of available boot loader commands:

```
Device:help
? -- Present list of available commands
arp -- Show arp table or arp-resolve an address
boot -- Load and boot an executable image
cat -- Concatenate (type) file(s)
copy -- Copy a file
delete -- Delete file(s)
dir -- List files in directories
emergency-install -- Initiate Disaster Recovery
...
...
...
unset -- Unset one or more environment variables
version -- Display boot loader version
```

hw-module

To enable on-board failure logging (OBFL), use the **hw-module** global configuration command on the switch stack or on a standalone switch. 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 level**]



Note This command is supported only on the LAN Base image.

Syntax Description	module	Specifies the module number.
	<i>switch-number</i>	(Optional) The switch number, which is the member switch number. If the switch is a standalone switch, the switch number is 1. If the switch is in a stack, the range is 1 to 4, depending on the switch member numbers in the stack.
	logging-onboard	Specifies on-board failure logging.
	message level level	(Optional) Specifies the severity of the hardware-related messages that are stored in the flash memory. The range is from 1 to 7.

Command Default OBFL is enabled, and all messages appear.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E 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.

On a standalone switch, entering the **hw-module module** [*switch-number*] **logging onboard** [**message level level**] command is the same as entering the **hw-module module logging onboard** [**message level level**] command.

Entering the **hw-module module logging onboard** [**message level level**] command on an active switch enables OBFL on all the member switches that support OBFL.

Example

This example shows how to enable OBFL on a switch stack and to specify that all the hardware-related messages on member switch 4 are stored in the flash memory when this command is entered on the active switch:

```
Switch(config)# hw-module module 4 logging onboard
```

This example shows how to enable OBFL on a standalone 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 **show logging onboard** privileged EXEC command.

ip name-server

To configure the IP address of the domain name server (DNS), use the **ip name-server** command. To delete the name server use the **no** form of this command.

ip name-server [*ip-server-address* | *ipv6-server-address* | *vrf*]

no ip name-server [*ip-server-address* | *ipv6-server-address* | *vrf*]

Syntax Description		
	<i>ip-server-address</i>	IPv4 addresses of a name server to use for name and address resolution.
	<i>ipv6-server-address</i>	IPv4 addresses of a name server to use for name and address resolution.
	<i>vrf</i>	VRF name

Command Default No name server addresses are specified.

Command Modes Global configuration mode

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines You can configure up to six name servers (including IPv4 and IPv6 name servers). Separate each server address with a space.

The first server specified is the primary server. The switch sends DNS queries to the primary server first. If that query fails, the backup servers are queried.

Enter the **show ip name-server** command to display all the name server IP addresses that have been maintained.

Specifics for Application Visibility Control (AVC) with Domain Name System as an Authoritative Source (DNS-AS):

Only IPv4 server addresses are supported. Ensure that at least the first two IP addresses in the sequence are IPv4 addresses, because the AVC with DNS-AS feature will use only these. In the example below, the first two addresses are IPv4 (192.0.2.1 and 192.0.2.2), the third one (2001:DB8::1) is an IPv6 address. AVC with DNS-AS uses the first two:

```
Device(config)# ip name-server 192.0.2.1 192.0.2.2 2001:DB8::1
```

Example

The following example shows how to specify IPv4 hosts 192.0.2.1 and 192.0.2.2 as the name servers:

```
Device# configure terminal
Device(config)# ip name-server 192.0.2.1 192.0.2.2 2001:DB8::1
```

The following example shows how to specify IPv6 hosts 3FFE:C00::250:8BFF:FEE8:F800 and 2001:0DB8::3 as the name servers

```
Device# configure terminal
Device(config)# ip name-server 3FFE:C00::250:8BFF:FEE8:F800 2001:0DB8::3
```

Related Commands

Command	Description
show ip name-server	Displays all the name server IP addresses that have been maintained

license boot level

To boot a new software license on the device, use the `license boot level` command in global configuration mode. To return to the previously configured license level, use the `no` form of this command.

```
license {accept end user agreement force | boot level addon addon-license-level {dna-essentials
| dna-advantage} }
no license {accept end user agreement force | boot level addon addon-license-level {dna-essentials
| dna-advantage} }
```

Syntax Description	accept end user agreement force	Enables acceptance of the end-user license agreement (EULA).
	boot level addon addon-license-level	Enter the add-on license level you want to enable on the switch. <ul style="list-style-type: none"> • dna-essentials • dna-advantage

Command Default The switch boots the configured image.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS Release 15.2(6)E1	This command was introduced.

Usage Guidelines You do not have to reboot the switch for the configure (add-on license) to take effect.

Example

The following example shows how to activate the `dna-essentials` license on the switch:

```
Device(config)# license boot level addon dna-essentials
```

logging

To log messages to a UNIX syslog server host, use the **logging** global configuration command.

logging *host*

Syntax Description

host The name or IP address of the host to be used as the syslog server.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

To build a list of syslog servers that receive logging messages, enter this command more than once.

Example

The following example specifies the logging host IP as 125.1.1.100:

```
Switch(config)# logging 125.1.1.100
```


logging buffered

To log messages to an internal buffer, use the **logging buffered** global configuration command. Use it on the switch or on a standalone switch or, in the case of a switch stack, on the active switch.

logging buffered [*size*]

Syntax Description	<i>size</i> (Optional) The size of the buffer created, in bytes. The range is 4096 to 2147483647 bytes. The default buffer size is 4096 bytes.
---------------------------	--

Command Default	The default buffer size is 4096 bytes.
------------------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines	If a standalone switch or the active switch fails, the log file is lost unless you previously saved it to flash memory using the logging file flash global configuration command.
-------------------------	--

Do not make the buffer size too large because the switch could run out of memory for other tasks.

Use the **show memory** privileged EXEC command to view the free processor memory on the switch.

However, this value is the maximum number of bytes available, and the buffer size should not be set to this amount.

Example

The following example sets the logging buffer to 8192 bytes:

```
Switch(config)# logging buffered 8192
```

logging console

To limit messages logged to the console according to severity, use the **logging console** command. Use the **no** form of this command to disable message logging.

logging console *level*
no logging console

Syntax Description

level The severity level of messages logged to the console. The severity levels are:

- 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 conditions (severity=5)
- Informational—Informational messages (severity=6)
- Debugging—Debugging messages (severity=7)
- Discriminator—Establish MD-Console association
- Filtered—Enable filtered logging
- Guaranteed—Guarantee console messages
- XML—Enable logging in XML

Command Default

By default, the console receives debugging messages and numerically lower levels.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Example

The following example sets the level of console messages received to severity 3 (errors) and above:

```
Switch(config)# logging console 3
```

logging file flash

To store log messages in a file in flash memory, use the **logging file flash** command. Use it on a standalone switch or, in the case of a switch stack, on the active switch.

logging file flash:*filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]

Syntax Description	<i>:filename</i>	The log message filename.
	<i>max-file-size</i>	(Optional) The maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes.
	<i>min-file-size</i>	(Optional) The minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes.
	<i>max-file-size</i> <i>type</i>	(Optional) Either the logging severity level or the logging type. The severity range is 0 to 7.
Command Default	The default maximum file size is 4096 bytes and the default minimum file size is 1024 bytes.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Example

The following example sets the logging flash: filename to log_msg.txt, the maximum file size to 40960, the minimum file size to 4096, and the message severity level to 3:

```
Switch(config)# logging file flash:log_msg.txt 40960 4096 3
```

logging history

To change the default level of syslog messages stored in the history file and sent to the SNMP server, use the **logging history** command.

logging history *level*

Syntax Description	<i>level</i> Level of syslog messages stored in the history file and sent to the SNMP server.				
Command Default	By default, warning, error, critical, alert, and emergency messages are sent.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.				

Example

The following example sets the level of syslog messages stored in the history file and sent to the SNMP server to 3:

```
Switch(config)# logging history 3
```

logging history size

To specify the number of syslog messages that can be stored in the history table, use the **logging history size** global configuration command.



Note When the history table contains the maximum number of message entries specified, the oldest message entry is deleted from the table to allow the new message entry to be stored.

logging history size *number*

Syntax Description *number* The number of syslog messages that can be stored in the history table.

Command Default The default is to store one message. The range is 0 to 500 messages.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Example

The following example sets the number of syslog messages that can be stored in the history table to 200:

```
Switch(config)# logging history size 200
```

logging monitor

To limit messages logged to the terminal lines according to severity, use the **logging monitor** command.

logging monitor *level*

Syntax Description

level The severity level of messages logged to the terminal lines. The severity levels are:

- 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 conditions (severity=5)
 - Informational—Informational messages (severity=6)
 - Debugging—Debugging messages (severity=7)
-

Command Default

By default, the terminal receives debugging messages and numerically lower levels.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Example

The following example sets the level of terminal messages received to severity 3 (errors) and above:

```
Switch(config)# logging monitor 3
```

logging trap

To limit messages logged to the syslog servers according to severity, use the **logging trap** command.

logging trap *level*

Syntax Description	<p><i>level</i> The severity level of messages logged to the syslog servers. The severity levels are:</p> <ul style="list-style-type: none"> • 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 conditions (severity=5) • Informational—Informational messages (severity=6) • Debugging—Debugging messages (severity=7) 				
Command Default	By default, the syslog servers receive debugging messages and numerically lower levels.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th style="text-align: left;">Release</th> <th style="text-align: left;">Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)E</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.				

Example

The following example sets the level of syslog server messages received to severity 3 (errors) and above:

```
Switch(config)# logging trap 3
```

mac address-table aging-time

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 **mac address-table aging-time** global configuration command. Use the **no** form of this command to return to the default setting.

```
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.
	<i>10-1000000</i>	Aging time in seconds. The range is 10 to 1000000 seconds.
	vlan <i>vlan-id</i>	(Optional) Specifies the VLAN ID to which to apply the aging time. The range is 1 to 4094.
Command Default	The default is 300 seconds.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.
Usage Guidelines	The aging time applies to all VLANs or a specified VLAN. If you do not specify a specific VLAN, this command sets the aging time for all VLANs. Enter 0 seconds to disable aging.	

Example

This example shows how to set the aging time to 200 seconds for all VLANs:

```
Device(config)# mac address-table aging-time 200
```

You can verify your setting by entering the **show mac address-table aging-time** privileged EXEC command.

mac address-table learning vlan

To enable MAC address learning on a VLAN, use the **mac address-table learning** global configuration command. Use the **no** form of this command to disable MAC address learning on a VLAN to control which VLANs can learn MAC addresses.

mac address-table learning vlan *vlan-id*

no mac address-table learning vlan *vlan-id*



Note This command is supported only on the LAN Base image.

Syntax Description	<i>vlan-id</i>	The VLAN ID or a range of VLAN IDs separated by a hyphen or comma. Valid VLAN IDs are 1 to 4094.
Command Default	By default, MAC address learning is enabled on all VLANs.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines When you control MAC address learning on a VLAN, you can manage the available MAC address table space by controlling which VLANs, and therefore which ports, can learn MAC addresses.

You can disable MAC address learning on a single VLAN ID (for example, **no mac address-table learning vlan 223**) or on a range of VLAN IDs (for example, **no mac address-table learning vlan 1-20, 15**).

Before you disable MAC address learning, be sure that you are familiar with the network topology and the switch system configuration.

Disabling MAC address learning on a VLAN could cause flooding in the network.

For example, if you disable MAC address learning on a VLAN with a configured switch virtual interface (SVI), the switch floods all IP packets in the Layer 2 domain.

If you disable MAC address learning on a VLAN that includes more than two ports, every packet entering the switch is flooded in that VLAN domain.

We recommend that you disable MAC address learning only in VLANs that contain two ports and that you use caution before disabling MAC address learning on a VLAN with an SVI.

You cannot disable MAC address learning on a VLAN that the switch uses internally. If the VLAN ID that you enter in the **no mac address-table learning vlan** *vlan-id* command is an internal VLAN, the switch generates an error message and rejects the command.

To view a list of which internal VLANs are being used, enter the **show vlan internal usage** privileged EXEC command.

If you disable MAC address learning on a VLAN configured as a private VLAN primary or a secondary VLAN, the MAC addresses are still learned on the other VLAN (primary or secondary) that belongs to the private VLAN.

You cannot disable MAC address learning on an RSPAN VLAN. The configuration is not allowed.

If you disable MAC address learning on a VLAN that includes a secure port, MAC address learning is not disabled on the secure port. If you later disable port security on the interface, the disabled MAC address learning state is enabled.

To display the MAC address learning status of all VLANs or a specified VLAN, enter the **show mac-address-table learning [vlan *vlan-id*]** command.

Example

This example shows how to disable MAC address learning on VLAN 2003:

```
Switch(config)# no mac address-table learning vlan 2003
```

To display the MAC address learning status of all VLANs or a specified VLAN, enter the **mac address-table learning vlan [vlan-id]** command.

logging smartlog

To enable smart logging, use the **logging smartlog** command in global configuration mode on the device.

Smart logging sends the contents of specified dropped packets to a Cisco IOS Flexible NetFlow collector.

To disable smart logging or return to the default setting, use the **no** form of this command.

logging smartlog [*exporter name* | **packet capture size** *bytes*]

no logging smartlog [*exporter name* | **packet capture size** *bytes*]

Syntax Description		
exporter name	(Optional) Identifies the Cisco IOS NetFlow exporter (collector) to which contents of dropped packets are sent. You must have already configured the exporter using the Flexible NetFlow CLI. If the exporter name does not exist, you receive an error message. By default, the device sends data to the collector every 60 seconds.	
packet capture size bytes	(Optional) Specifies the size of the smart log packet sent to the collector in the number of bytes. The range is from 64 to 1024 bytes in 4-byte increments. The default size is 64 bytes. Increasing the packet capture size reduces the number of flow records per packet.	

Command Default By default, smart logging is not enabled.

Command Modes Global configuration.

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	This command was introduced.
	Cisco IOS Release 15.2(5)E	

Usage Guidelines You must configure a NetFlow collector before you enable smart logging. For information on configuring Cisco Flexible NetFlow, see the *Cisco IOS Flexible NetFlow Configuration Guide*.

You can configure smart logging of packets dropped due to DHCP snooping violations, Dynamic ARP inspection violations, IP source guard denied traffic, or ACL permitted or denied traffic.

You can verify the configuration by entering the **show logging smartlog** privileged EXEC command.

Examples

This example shows a typical smart logging configuration. It assumes that you have already used the Flexible NetFlow CLI to configure the NetFlow exporter *cisco*, and configures smart logging to capture the first 128 bytes of the packets:

```
Device(config)# logging smartlog
Device(config)# logging smartlog cisco
Device(config)# logging smartlog packet capture size 128
```

mac address-table notification

To enable the MAC address notification feature on the switch stack, use the **mac address-table notification** global configuration command. Use the **no** form of this command to return to the default setting.

mac address-table notification [**mac-move** | **threshold** [[**limit** *percentage*] **interval** *time*]]
no mac address-table notification [**mac-move** | **threshold** [[**limit** *percentage*] **interval** *time*]]

Syntax Description

mac-move	(Optional) Enables MAC move notification.
threshold	(Optional) Enables MAC threshold notification.
limit <i>percentage</i>	(Optional) Sets the MAC utilization threshold percentage. The range is 1 to 100 percent. The default is 50 percent.
interval <i>time</i>	(Optional) Sets the time between MAC threshold notifications. The range is 120 to 1000000 seconds. The default is 120 seconds.

Command Default

By default, the MAC address notification, MAC move, and MAC threshold monitoring are disabled. The default MAC utilization threshold is 50 percent. The default time between MAC threshold notifications is 120 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

You can enable traps whenever a MAC address is moved from one port to another in the same VLAN by entering the **mac address-table notification mac-move** command and the **snmp-server enable traps mac-notification move global configuration** command.

To generate traps whenever the MAC address table threshold limit is reached or exceeded, enter the **mac address-table notification threshold [limit percentage] [interval time]** command and the **snmp-server enable traps mac-notification threshold** global configuration command.

Example

This example shows how to set the threshold limit to 10 and set the interval time to 120 seconds:

```
Device(config)# mac address-table notification threshold limit 10 interval 120
```

You can verify your settings by entering the **show mac address-table notification** privileged EXEC command.

mac address-table static

To add static addresses to the MAC address table, use the **mac address-table static** global configuration command. 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		
<i>mac-addr</i>		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 <i>vlan-id</i>		Specifies the VLAN for which the packet with the specified MAC address is received. The range is 1 to 4094.
interface <i>interface-id</i>		Specifies the interface to which the received packet is forwarded. Valid interfaces include physical ports and port channels.

Command Default No static addresses are configured.

Command Modes Global configuration

Command History

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

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:

```
Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet6/0/1
```

You can verify your setting by entering the **show mac address-table** privileged EXEC command.

mkdir

To create one or more directories on the specified file system, use the **mkdir** command in boot loader mode.

mkdir *filesystem:/directory-url...*

Syntax Description	<i>filesystem:</i> Alias for a file system. Use usbflash0: for USB memory sticks.
	<i>/directory-url...</i> Name of the directories to create. Separate each directory name with a space.

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Boot loader
----------------------	-------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines	<p>Directory names are case sensitive.</p> <p>Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.</p>
-------------------------	---

Example

This example shows how to make a directory called Saved_Configs:

```
Device: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```

more

To display the contents of one or more files, use the **more** command in boot loader mode.

more *filesystem:/file-url...*

Syntax Description

filesystem: Alias for a 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 Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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:

```
Device: more flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

nmsp notification interval

To modify the Network Mobility Services Protocol (NMSP) notification interval value on the controller to address latency in the network, use the **nmsp notification interval** command in global configuration mode.

```
nmsp notification interval { attachment | location | rssi { clients | rfid | rogues { ap | client } } }
```

Syntax Description

attachment	Specifies the time used to aggregate attachment information.
location	Specifies the time used to aggregate location information.
rssi	Specifies the time used to aggregate RSSI information.
clients	Specifies the time interval for clients.
rfid	Specifies the time interval for rfid tags.
rogues	Specifies the time interval for rogue APs and rogue clients .
ap	Specifies the time used to aggregate rogue APs .
client	Specifies the time used to aggregate rogue clients.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

This example shows how to set the NMSP notification interval for the active RFID tags to 25 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval rfid 25
Device(config)# end
```

This example shows how to modify NMSP notification intervals for device attachment (connecting to the network or disconnecting from the network) every 10 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval attachment 10
Device(config)# end
```

This example shows how to configure NMSP notification intervals for location parameters (location change) every 20 seconds:


```
Device# configure terminal  
Device(config)# nmsp notification-interval location 20  
Device(config)# end
```

rcommand

To start a Telnet session and to execute commands, use the **rcommand** user EXEC command. Use it on the switch stack, on the cluster command switch, or on a cluster member switch. To end the session, enter the **exit** command.

rcommand { *n* | **commander** | **mac-address** *hw-addr* }

Syntax Description		
<i>n</i>		The number that identifies a cluster member. The range is 0 to 15.
commander		Provides access to the cluster command switch from a cluster member switch.
mac-address <i>hw-addr</i>		Specifies the MAC address of the cluster member switch.

Command Modes User EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

This command is available only on the cluster command switch stack or 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 2900 XL, 3500 XL, 2950, 2960, 2970, 3550, 3560, and 3750 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 the privilege level, the command accesses the remote device at the privilege level.

If you use an intermediate enable-level lower than the privilege, access to the cluster member switch is at the 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.

Example

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>
```

rename

To rename a file, use the **rename** command in boot loader mode.

rename *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description

<i>filesystem:</i>	Alias for a file system. Use usbflash0: for USB memory sticks.
<i>/source-file-url</i>	Original path (directory) and filename.
<i>/destination-file-url</i>	New path (directory) and filename.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 127 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*:

```
Device: rename usbflash0:config.text usbflash0:config1.text
```

You can verify that the file was renamed by entering the **dir filesystem:** boot loader command.

reset

To perform a hard reset on the system, use the **reset** command in boot loader mode. A hard reset is similar to power-cycling the device; it clears the processor, registers, and memory.

reset

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Boot loader
----------------------	-------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Examples

This example shows how to reset the system:

```
Device: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
```

rmdir

To remove one or more empty directories from the specified file system, use the **rmdir** command in boot loader mode.

rmdir *filesystem:/directory-url...*

Syntax Description

filesystem: Alias for a file system. Use **usbflash0:** for USB memory sticks.

/directory-url... Path (directory) and name of the empty directories to remove. Separate each directory name with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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 of the files in the directory.

The device prompts you for confirmation before deleting each directory.

Example

This example shows how to remove a directory:

```
Device: rmdir usbflash0:Test
```

You can verify that the directory was deleted by entering the **dir filesystem:** boot loader command.

service sequence-numbers

To display messages with sequence numbers when there is more than one log message with the same time stamp, use the **service sequence-numbers** global configuration command.

service sequence-numbers

Syntax Description	This command has no arguments or keywords.	
Command Default	By default, sequence numbers in log messages are not displayed.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Example

This example shows how to display messages with sequence numbers when there is more than one log message with the same time stamp:

```
Switch(config)# service sequence-numbers
```

set

To set or display environment variables, use the **set** command in boot loader mode. Environment variables can be used to control the boot loader or any other software running on the device.

set *variable value*

Syntax Description

<i>variable</i> <i>value</i>	<p>Use one of the following keywords for <i>variable</i> and the appropriate value for <i>value</i>:</p> <p>MANUAL_BOOT—Decides whether the device automatically or manually boots.</p> <p>Valid values are 1/Yes and 0/No. If it is set to 0 or No, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the device from the boot loader mode.</p> <hr/> <p>BOOT <i>filesystem:/file-url</i>—Identifies a semicolon-separated list of executable files to try to load and execute when automatically booting.</p> <p>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.</p> <hr/> <p>ENABLE_BREAK—Allows the automatic boot process to be interrupted when the user presses the Break key on the console.</p> <p>Valid values are 1, Yes, On, 0, No, and Off. If 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.</p> <hr/> <p>HELPER <i>filesystem:/file-url</i>—Identifies 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.</p> <hr/> <p>PS1 <i>prompt</i>—Specifies a string that is used as the command-line prompt in boot loader mode.</p> <hr/> <p>CONFIG_FILE flash: <i>/file-url</i>—Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.</p> <hr/> <p>BAUD <i>rate</i>—Specifies the number of bits per second (b/s) that is used for the baud rate 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 128000 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.</p> <p>The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.</p> <hr/> <p>SWITCH_NUMBER <i>stack-member-number</i>—Changes the member number of a stack member.</p> <hr/> <p>SWITCH_PRIORITY <i>priority-number</i>—Changes the priority value of a stack member.</p>
---------------------------------	--

Command Default

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 device:

CONFIG_FILE: config.text

BAUD: 9600 b/s

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1



Note Environment variables that have values are stored in the flash: file system in various files. Each line in the files 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 these files; it has a value if it is listed 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
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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 typical 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 SWITCH_NUMBER environment variable can also be set by using the **switch current-stack-member-number renumber new-stack-member-number** global configuration command.

The SWITCH_PRIORITY environment variable can also be set by using the device *stack-member-number* **priority** *priority-number* global configuration command.

The boot loader prompt string (PS1) can be up to 120 printable characters not including the equal sign (=).

Example

This example shows how to set the SWITCH_PRIORITY environment variable:

```
Device: set SWITCH_PRIORITY 2
```

You can verify your setting by using the **set** boot loader command.

show avc dns-as client

To display the various AVC with DNS-AS settings you have configured, enter the **show avc dns-as client** command in Privileged EXEC mode

```
show avc dns-as client[{binding-table [ | detail] | | name-server brief | | rate-limiter-table | |
statistics | status | trusted domains}]
```

Syntax Description	
binding-table [detail]	Displays AVC with DNS-AS metadata for the list of trusted domains and resolved entries. You can filter the output by application name, domain name, and so on. The optional detail keyword displays the same information, in a different format.
name-server brief	Displays information about the DNS server to which the metadata request was sent.
rate-limiter-table	—
statistics	Displays packet logging information—the number of DNS queries sent and the number of responses received.
status	Displays current status of the DNS-AS client. Use this command to know whether AVC with DNS-AS is enabled or not.
trusted-domains	Displays list of trusted domains maintained in the binding table.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.2(5)E1	This command was introduced.

show avc dns-as client binding-table detailed

```
Device# show avc dns-as client binding-table
Switch# show avc dns-as client binding-table detailed
DNS-AS generated protocols:
Max number of protocols :50
Customization interval [min] :N/A

Age : The amount of time that the entry is active
TTL : Time to live which was learned from DNS-AS server
Time To Expire : Entry expiration time in case device does not see DNS traffic for the entry
host

Protocol-Name : example
VRF : <default>
Host : www.example.com
Age[min] : 2
TTL[min] : 60
Time To Expire[min] : 58
TXT Record : app-name:example|app-class:VO|business:YES
```

```
Traffic Class : voip-telephony
Business Relevance : business relevant
IP : 192.0.2.121
   : 192.0.2.254
   : 198.51.100.1
   : 198.51.100.254
   : 192.51.100.12
   : 203.0.113.125
<output truncated>
```

show avc dns-as client name-server brief

```
Device# show avc dns-as client name-server brief
```

```
Server-IP | Vrf-name
-----
192.0.2.1 | <default>
192.0.2.2 | <default>
```

show avc dns-as client statistics



Note Two DNS servers are configured in this example.

```
Device# show avc dns-as client statistics
Server details: vrf-id = 0 vrf-name = <default> ip = 192.0.2.1
AAAA Query Error packets 0
AAAA Query TX packets 0
AAAA Response RX packets 0
TXT Query Error packets 0
TXT Query TX packets 8
TXT Response RX packets 0
A Query Error packets 0
A Query TX packets 6
A Response RX packets 0
Server details: vrf-id = 0 vrf-name = <default> ip = 192.0.2.2
AAAA Query Error packets 0
AAAA Query TX packets 0
AAAA Response RX packets 0
TXT Query Error packets 0
TXT Query TX packets 2
TXT Response RX packets 2
A Query Error packets 0
A Query TX packets 4
A Response RX packets 2
Total Drop packets 0

avc_dns_as_pkts_logged = 2
avc_dns_as_q_pkts_processed = 2
```

show avc dns-as client status

```
Device# show avc dns-as client status
DNS-AS client is enabled
```

show avc dns-as client trusted-domains

```
Device# show avc dns-as client trusted-domains
```

```
Id | Trusted domain
```

```
-----  
1| example.com  
2| www.example.com  
3| example.net  
4| www.example.net  
5| example.org  
6| www.example.org
```

Related Commands

Command	Description
avc dns-as client, on page 584	Enables AVC with DNS-AS on the switch (DNS-AS client) and maintains a list of trusted domains

show boot

To display the settings of the boot environment variables, use the **show boot** privileged EXEC command.

show boot

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Example

This example shows the output from the **show boot** command. The table below describes each field in the display:

```
Switch# show boot
BOOT path-list      :flash:/image
Config file        :flash:/config.text
Private Config file :flash:/private-config.text
Enable Break       :no
Manual Boot        :yes
HELPER path-list   :
Auto upgrade       :yes
-----
```

For switch stacks, information is shown for each switch in the stack.

This feature is supported only on the LAN Base image.

Table 37: show boot Field Descriptions

Field	Description
BOOT path-list	<p>Displays a semicolon-separated list of executable files to try to load and execute when automatically booting up.</p> <p>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.</p> <p>If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot up with the first bootable file that it can find in the flash: file system.</p>

Field	Description
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 private nonvolatile copy of the system configuration.
Enable break	Displays whether a break is permitted during booting up is enabled or disabled. If it is set to yes, on, or 1, you can interrupt the automatic bootup 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 up. If it is set to no or 0, the bootloader attempts to automatically boot up the system. If it is set to anything else, you must manually boot up the switch from the bootloader mode.
Helper path-list	Displays a semicolon-separated list of loadable files to dynamically load during the bootloader initialization. Helper files extend or patch the functionality of the bootloader.
Auto upgrade	<p>Displays whether the switch stack is set to automatically copy its software version to an incompatible switch so that it can join the stack.</p> <p>A switch in version-mismatch mode is a switch that has a different stack protocol version than the version on the stack. Switches in version-mismatch mode cannot join the stack. If the stack has an image that can be copied to a switch in version-mismatch mode, and if the boot auto-copy-sw feature is enabled, the stack automatically copies the image from another stack member to the switch in version-mismatch mode. The switch then exits version-mismatch mode, reboots, and joins the stack.</p>
NVRAM/Config file buffer size	Displays the buffer size that Cisco IOS uses to hold a copy of the configuration file in memory. The configuration file cannot be larger than the buffer size allocation.

show cable-diagnostics prbs

To display the pseudo-random binary sequence (PRBS) test results, use the **show cable-diagnostics prbs** command in privileged EXEC mode.

show cable-diagnostics prbs interface *interface-id*

Syntax Description

interface-id The interface on which PRBS is run.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

PRBS is only supported on 10-Gigabit Ethernet ports. It is not supported on 10/100/100 copper Ethernet ports and small form-factor pluggable (SFP) module ports.

This example shows the output from the **show cable-diagnostics prbs interface** *interface-id* command on a device:

```
Switch# show cable-diagnostics prbs interface gigabitethernet1/0/23
prbs test last run on: March 01 00:04:08
Interface  Speed  Local pair  Pair length          Remote pair  Pair status
-----
Gi1/0/23  1000M  Pair A     1 +/- 1 meters      Pair A      Normal
           Pair B     1 +/- 1 meters      Pair B      Normal
           Pair C     1 +/- 1 meters      Pair C      Normal
           Pair D     1 +/- 1 meters      Pair D      Normal
```

Table 38: Field Descriptions for the show cable-diagnostics prbs Command Output

Field	Description
Interface	Interface on which PRBS is run.
Speed	Speed of connection.
Local pair	The name of the pair of wires that PRBS is testing on the local interface.
Pair length	The location of the problem on the cable, with respect to your device. PRBS can only find the location in one of these cases: <ul style="list-style-type: none"> • The cable is properly connected, the link is up, and the interface speed is 10-Gps. • The cable is open. • The cable has a short.

Field	Description
Remote pair	The name of the pair of wires to which the local pair is connected. PRBS can learn about the remote pair only when the cable is properly connected and the link is up.
Pair status	The status of the pair of wires on which PRBS is running: <ul style="list-style-type: none"> • Normal—The pair of wires is properly connected. • Not completed—The test is running and is not completed. • Not supported—The interface does not support PRBS. • Open—The pair of wires is open. • Shorted—The pair of wires is shorted. • ImpedanceMis—The impedance is mismatched. • Short/Impedance Mismatched—The impedance mismatched or the cable is short. • InProgress—The diagnostic test is in progress.

This example shows the output from the **show interface** *interface-id* command when PRBS is running:

```
Switch# show interface gigabitethernet1/0/2
gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

This example shows the output from the **show cable-diagnostics prbs interface** *interface-id* command when PRBS is not running:

```
Switch# show cable-diagnostics PRBS interface gigabitethernet1/0/2
% PRBS test was never issued on Gi1/0/2
```

If an interface does not support PRBS, this message appears:

```
% PRBS test is not supported on device 1
```

show cable-diagnostics tdr

To display the Time Domain Reflector (TDR) results, use the **show cable-diagnostics tdr** command in privileged EXEC mode.

show cable-diagnostics tdr interface *interface-id*

Syntax Description	<i>interface-id</i> Specifies the interface on which TDR is run.
---------------------------	--

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines	TDR is supported only on 10/100/100 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports and small form-factor pluggable (SFP) module ports.
-------------------------	---

Examples

This example shows the output from the **show cable-diagnostics tdr interface** *interface-id* command on a device:

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/23
TDR test last run on: March 01 00:04:08
Interface  Speed  Local pair  Pair length      Remote pair  Pair status
-----
Gi1/0/23  1000M  Pair A     1 +/- 1 meters  Pair A      Normal
          Pair B     1 +/- 1 meters  Pair B      Normal
          Pair C     1 +/- 1 meters  Pair C      Normal
          Pair D     1 +/- 1 meters  Pair D      Normal
```

Table 39: Field Descriptions for the show cable-diagnostics tdr Command Output

Field	Description
Interface	The interface on which TDR is run.
Speed	The speed of connection.
Local pair	The name of the pair of wires that TDR is testing on the local interface.

Field	Description
Pair length	The location of the problem on the cable, with respect to your device. TDR can only find the location in one of these cases: <ul style="list-style-type: none"> • The cable is properly connected, the link is up, and the interface speed is 1000 Mb/s. • The cable is open. • The cable has a short.
Remote pair	The name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up.
Pair status	The status of the pair of wires on which TDR is running: <ul style="list-style-type: none"> • Normal—The pair of wires is properly connected. • Not completed—The test is running and is not completed. • Not supported—The interface does not support TDR. • Open—The pair of wires is open. • Shorted—The pair of wires is shorted. • ImpedanceMis—The impedance is mismatched. • Short/Impedance Mismatched—The impedance mismatched or the cable is short. • InProgress—The diagnostic test is in progress.

This example shows the output from the **show interface** *interface-id* command when TDR is running:

```
Device# show interface gigabitethernet1/0/2
gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

This example shows the output from the **show cable-diagnostics tdr interface** *interface-id* command when TDR is not running:

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/2
% TDR test was never issued on gigabitethernet1/0/2
```

If an interface does not support TDR, this message appears:

```
% TDR test is not supported on device 1
```

show cluster

To display the cluster status and a summary of the cluster to which the switch belongs, use the **show cluster EXEC** command. This command can be entered on the cluster command switch and cluster member switches.

show cluster

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

If you enter this command on a switch that is not a cluster member, the following error message appears:

```
Not a management cluster member.
```

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 stack or 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.

Example

This example shows the output from the **show cluster** command entered on the 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 example shows the output from the **show cluster** command 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 example shows the output from the **show cluster** command entered on a cluster member 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 example shows the output from the **show cluster** command 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
```

show cluster candidates

To display a list of candidate switches, use the **show cluster candidates EXEC** command.

show cluster candidates [**detail** | **mac-address** *H.H.H*]

Syntax Description	detail	(Optional) Displays detailed information for all candidates.
	mac-address <i>H.H.H</i>	(Optional) Specifies the MAC address of the cluster candidate.

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines This command is available only on the cluster command switch stack or cluster command switch.



Note This feature is supported only on the LAN Base image.

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 located from the cluster command switch.

Example

This example shows the output from the **show cluster candidates** command:

```
Switch# show cluster candidates
MAC Address      Name           Device Type   PortIf  FEC Hops  SN  PortIf  FEC
00d0.7961.c4c0  StLouis-2     WS-C2960-12T Gi0/1    2    1    1    Fa0/11
00d0.bbf5.e900  ldf-dist-128 WS-C3524-XL   Fa0/7    1    0    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    0    Fa0/3
00e0.1e9f.8c00  Surfers-12-2  WS-C2912-XL   Fa0/4    1    0    0    Fa0/7
00e0.1e9f.8c40  Surfers-12-1  WS-C2912-XL   Fa0/1    1    0    0    Fa0/9
```

This example shows the output from the **show cluster candidates** 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-C2960-12T
```

```

Upstream MAC address: 00d0.796d.2f00 (Cluster Member 0)
Local port:          Gi6/0/1 FEC number:
Upstream port:      GI6/0/11 FEC Number:
Hops from cluster edge: 1
Hops from command device: 1

```

This example shows the output from the **show cluster candidates** that uses the MAC address of a cluster member switch that is 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 example shows the 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

```

show cluster members

To display information about cluster members, use the **show cluster members** privileged EXEC command.

show cluster members [*n* | **detail**]

Syntax Description	
<i>n</i>	(Optional) Number that identifies a cluster member. The range is 0 to 15.
detail	(Optional) Displays detailed information for all cluster members.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXC	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines This command is available only on the cluster command switch stack or cluster command switch.



Note This feature is supported only on the LAN Base image.

If the cluster has no members, this command displays an empty line at the prompt.

Example

This example shows the 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
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 example shows the 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-C2960
MAC address:          0002.4b29.4400
Upstream MAC address: 0030.946c.d740 (Cluster member 1)
Local port:           Gi6/0/1   FEC number:
Upstream port:        GI6/0/11  FEC Number:
Hops from command device: 2
```

This example shows the output from the **show cluster members detail** command:

```
Switch# show cluster members detail
Device 'StLouis1' with member number 0 (Command Switch)
Device type:          cisco WS-C2960
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-C2960
MAC address:         0002.4b29.4400
Upstream MAC address: 0030.946c.d740 (Cluster member 1)
Local port:         Gi6/0/1  FEC number:
Upstream port:     Fa6/0/11 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:         Gi2/1    FEC number:
Upstream port:     Gi0/7    FEC Number:
Hops from command device: 1
```

show ip name-server

To display all the name server IP addresses that have been maintained, enter the **show ip name-server** command.

show ip name-server

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Example

```
Device# show ip name-server
192.0.2.1
192.0.2.2
2001:DB8::1
```

show license right-to-use

To display information related to the right-to-use licenses on the device, use the **show license right-to-use** command in the privileged EXEC mode.

show license right-to-use [**default** | **detail** | **eula** | **summary** | **usage**]

Syntax Description	default	Displays the default license information.
	detail	Displays detailed information of all the licenses in the switch stack.
	eula	Displays the end user license agreement.
	summary	Displays a summary of the license information on the entire switch stack.
	usage	Displays detailed information about usage for all licenses in the switch stack.
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.2(6)E1	This command was introduced.

This example shows how to display the default license information:

```
Device# show license right-to-use default
slot      License Name      Type
-----
0         lanlite           Permanent
0         lanbase           Permanent
```

This example shows how to display detailed information of all the licenses in the switch stack:

```
Device# show license right-to-use detail
Index 1
License Name      : lanlite
Period left       : 0 minute 0 second
License Type: Permanent
License State: Inactive
Index 2
License Name      : lanbase
Period left       : 0 minute 0 second
License Type: Permanent
License State: Active, In use
Index 3
```

```

License Name      : dna-essentials
Period left      : CSSM Managed
License Type     : Subscription
License State    : Active, In use

```

Index 4

```

License Name      : dna-advantage
Period left      : CSSM Managed
License Type     : Subscription
License State    : Not Activated

```

This example shows how to display summary of the license information on the entire switch stack:

```

Device# show license right-to-use summary
License Name      Type      Period left
-----
lanlite           Permanent  0 minute 0 second
lanbase           Permanent  0 minute 0 second
dna-essentials    Subscription CSSM Managed
-----

```

```

License Level In Use: lanbase  addon: dna-essentials
License Level on Reboot: lanbase  addon: dna-essentials

```

This example shows how to display detailed information about usage for all licenses in the switch stack:

```

Device# show license right-to-use usage
slot      License Name      Type      In-use  EULA
-----
0         lanlite           Permanent  yes     yes
0         lanbase           Permanent  yes     yes
         dna-essentials    Subscription yes     yes

```

This example shows how to display the end user license agreement:

```

Device# show license right-to-use eula subscription
Feature name      EULA Accepted
-----
dna-essentials    yes
PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE,
AND OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE ?SOFTWARE?),
USING SUCH SOFTWARE, AND/OR ACTIVATION OF THE SOFTWARE COMMAND LINE INTERFACE
CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING TERMS.YOU MUST NOT PROCEED
FURTHER IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

```

```

Your use of the Software is subject to the Cisco End User License Agreement (EULA)
and any relevant supplemental terms (SEULA) found at
http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.
You hereby acknowledge and agree that certain Software and/or features are licensed
for a particular term, that the license to such Software and/or features is valid only
for the applicable term and that such Software and/or features may be shut down or
otherwise terminated by Cisco after expiration of the applicable license term (e.g.,
90-day trial period). Cisco reserves the right to terminate any such Software feature
electronically or by any other means available. While Cisco may provide alerts, it is
your sole responsibility to monitor your usage of any such term Software feature to

```

ensure that your systems and networks are prepared for a shutdown of the Software feature. To memorialize your acceptance of these terms and activate your license to use the Software, please execute the command "license accept end user agreement force".

show logging onboard

Display the on-board failure logging (OBFL) information using the **show logging onboard** privileged EXEC command.

```
show logging onboard [module [switch number]] {{clilog | environment | message | poe |
temperature | uptime | voltage}} [continuous | detail | summary] [start hh:mm:ss day month
year] [end hh:mm:ss day month year] }
```

Syntax Description

module [<i>switch number</i>]	(Optional) Displays OBFL information about the specified switches. Uses the <i>switch number</i> parameter to specify the switch number, which is the stack member number. If the switch is a standalone switch, the switch number is 1. If the switch is in a stack, the range is 1 to 8, depending on the switch member numbers in the stack. For more information about this parameter, see the “Usage Guidelines” section for this command.
clilog	Displays the OBFL CLI commands that were entered on the standalone switch or specified stack members.
environment	Displays the unique device identifier (UDI) information for the standalone switch or specified stack members. For all the connected FRU devices, it displays the product identification (PID), the version identification (VID), and the serial number.
message	Displays the hardware-related system messages generated by the standalone switch or specified stack members.
poe	Displays the power consumption of PoE ports on the standalone switch or specified stack members.
temperature	Displays the temperature of the standalone switch or specified stack members.
uptime	Displays the time when the standalone switch or specified stack members start, the reason the standalone switch or specified members restart, and the length of time the standalone switch or specified stack members have been running since they last restarted.
voltage	Displays the system voltages of the standalone switch or the specified switch stack members.
continuous	(Optional) Displays the data in the <i>continuous</i> file.
detail	(Optional) Displays both the continuous and summary data.
summary	(Optional) Displays the data in the <i>summary</i> file.
start <i>hh:mm:ss day month year</i>	(Optional) Displays the data from the specified time and date. For more information, see the “Usage Guidelines” section.
end <i>hh:mm:ss day month year</i>	(Optional) Displays the data from the specified time and date. For more information, see the “Usage Guidelines” section.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines When OBFL is enabled, the switch records OBFL data in a continuous file that contains all of the data. The continuous file is circular. When the continuous file is full, the switch combines the data into a summary file, which is also known as a historical file.

Creating the summary file frees up space in the continuous file so that the switch can write newer data to it.

If you enter the **module** keyword, but do not enter the switch number, the switch displays OBFL information about the stack members that support OBFL.

Use the **start** and **end** keywords to display data collected only during a particular time period. When specifying the start and end times, follow these guidelines:

- *hh:mm:ss*—Enter the time as a two-digit number for a 24-hour clock. Make sure to use the colons (:).
For example, enter **13:32:45**.
- *day*—Enter the day of the month. The range is from 1 to 31.
- *month*—Enter the month in uppercase or lowercase letters. You can enter the full name of the month, such as **January** or **august**, or the first three letters of the month, such as **jan** or **Aug**.
- *year*—Enter the year as a 4-digit number, such as 2008. The range is from 1993 to 2035.



Note This feature is supported only on the LAN Base image.

Example

This example shows the output from the **show logging onboard clilog continuous** command:

```
Switch# show logging onboard clilog continuous
-----
CLI LOGGING CONTINUOUS INFORMATION
-----
MM/DD/YYYY HH:MM:SS COMMAND
-----
05/12/2006 15:33:17 show logging onboard temperature detail
05/12/2006 15:33:21 show logging onboard voltage detail
05/12/2006 15:33:32 show logging onboard poe detail
05/12/2006 16:14:09 show logging onboard temperature summary
...
<output truncated>
....
05/16/2006 13:07:53 no hw-module module logging onboard message level
05/16/2006 13:16:13 show logging onboard uptime continuous
05/16/2006 13:39:18 show logging onboard uptime summary
05/16/2006 13:45:57 show logging onboard clilog summary
-----
```

This example shows the output from the **show logging onboard poe continuous end 01:01:00 jan 2000** command on a switch:

```
Switch# show logging onboard message poe continuous end 01:01:00 jan 2000
POE CONTINUOUS INFORMATION
-----
Sensor                | ID |
-----
Gi1/0/1                1
Gi1/0/2                2
Gi1/0/3                3
Gi1/0/4                4
...
<output truncated>
...
Gi1/0/21               21
Gi1/0/22               22
Gi1/0/23               23
Gi1/0/24               24
-----
Time Stamp            |Sensor Watts
MM/DD/YYYY HH:MM:SS | Gi1/0/1 Gi1/0/2 Gi1/0/3 Gi1/0/4 Gi1/0/5 Gi1/0/6 Gi1/0/7 Gi1/0/8 Gi1/0/9
Gi1/0/10 Gi1/0/11 Gi1/0/12 Gi1/0/13 Gi1/0/14 Gi1/0/15 Gi1/0/16 Gi1/0/17 Gi1/0/18 Gi1/0/19
Gi1/0/20 Gi1/0/21
Gi1/0/22 Gi1/0/23 Gi1/0/24
-----
03/01/1993 00:04:03  0.000  0.000  0.000  0.000  0.000  0.000  0.0  00  0.000  0.000
0.000  0.000  0.000  0.000 0.000  0.000  0.000  0.000  0.000  0.000  0.000  0.000
0.000  0.000  0.000
03/01/1993 00:05:03  0.000 1.862  0.000  1.862  0.000  0.000  0.000  0.000  0.000  0.000
0.000  0.000  0.000  0.000 0.000  0.000  0.000  0.000  0.000  0.000  0.000
0.000  0.000
-----
```

This example shows the output from the **show logging onboard status** command:

```
Switch# show logging onboard status
Devices registered with infra
      Slot no.: 0 Subslot no.: 0, Device obf10:
Application name cliiog :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
Application name environment :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
Application name errmsg :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
Application name poe :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
Application name temperature :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
Application name uptime :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
Application name voltage :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
```


This example shows the output from the **show logging onboard temperature continuous** command:

```
Switch# show logging onboard temperature continuous
-----
TEMPERATURE CONTINUOUS INFORMATION
-----
Sensor                               | ID |
-----
Board temperature                     | 1  |
-----
      Time Stamp   |Sensor Temperature 0C
MM/DD/YYYY HH:MM:SS | 1  2  3  4  5  6  7  8  9 10 11 12
-----
05/12/2006 15:33:20 35 -- -- -- -- -- -- -- -- -- -- --
05/12/2006 16:31:21 35 -- -- -- -- -- -- -- -- -- -- --
05/12/2006 17:31:21 35 -- -- -- -- -- -- -- -- -- -- --
05/12/2006 18:31:21 35 -- -- -- -- -- -- -- -- -- -- --
05/12/2006 19:31:21 35 -- -- -- -- -- -- -- -- -- -- --
05/12/2006 20:31:21 35 -- -- -- -- -- -- -- -- -- -- --
05/12/2006 21:29:22 35 -- -- -- -- -- -- -- -- -- -- --
05/12/2006 22:29:22 35 -- -- -- -- -- -- -- -- -- -- --
05/12/2006 23:29:22 35 -- -- -- -- -- -- -- -- -- -- --
05/13/2006 00:29:22 35 -- -- -- -- -- -- -- -- -- -- --
05/13/2006 01:29:22 35 -- -- -- -- -- -- -- -- -- -- --
05/13/2006 02:27:23 35 -- -- -- -- -- -- -- -- -- -- --
05/13/2006 03:27:23 35 -- -- -- -- -- -- -- -- -- -- --
05/13/2006 04:27:23 35 -- -- -- -- -- -- -- -- -- -- --
05/13/2006 05:27:23 35 -- -- -- -- -- -- -- -- -- -- --
05/13/2006 06:27:23 35 -- -- -- -- -- -- -- -- -- -- --
05/13/2006 07:25:24 36 -- -- -- -- -- -- -- -- -- -- --
05/13/2006 08:25:24 35 -- -- -- -- -- -- -- -- -- -- --
<output truncated>
```

This example shows the output from the **show logging onboard uptime summary** command:

```
Switch# show logging onboard uptime summary
-----
UPTIME SUMMARY INFORMATION
-----
First customer power on : 03/01/1993 00:03:50
Total uptime           : 0 years 0 weeks 3 days 21 hours 55 minutes
Total downtime        : 0 years 0 weeks 0 days 0 hours 0 minutes
Number of resets      : 2
Number of slot changes : 1
Current reset reason   : 0x0
Current reset timestamp : 03/01/1993 00:03:28
Current slot          : 1
Current uptime        : 0 years 0 weeks 0 days 0 hours 55 minutes
-----
Reset |      |
Reason | Count |
-----
No historical data to display
-----
```

This example shows the output from the **show logging onboard voltage summary** command:

```
Switch# show logging onboard voltage summary
-----
VOLTAGE SUMMARY INFORMATION
-----
Number of sensors      : 8
Sampling frequency     : 60 seconds
Maximum time of storage : 3600 minutes
-----
```

show logging onboard

```
Sensor                | ID | Maximum Voltage
-----|-----|-----
12.00V                | 0  | 12.567
5.00V                 | 1  | 5.198
3.30V                 | 2  | 3.439
2.50V                 | 3  | 2.594
1.50V                 | 4  | 1.556
1.20V                 | 5  | 1.239
1.00V                 | 6  | 0.980
0.75V                 | 7  | 0.768
-----|-----|-----
Nominal Range         |     | Sensor ID
-----|-----|-----
No historical data to display
-----|-----|-----
```

show mac address-table

To display a specific MAC address table entry, use the **show mac address-table** command in EXEC mode.

show mac-address-table

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines



Note This feature is supported only on the LAN Base image.

This command can display static and dynamic entries or the MAC address table static and dynamic entries on a specific interface or VLAN.

Example

This example shows the 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
```

show mac address-table address

To display MAC address table information for a specified MAC address, use the **show mac address-table address** command in EXEC mode.

show mac address-table address *mac-address* [**interface** *interface-id*] [**vlan** *vlan-id*]

Syntax Description

<i>mac-address</i>	The 48-bit MAC address; valid format is H.H.H.
interface <i>interface-id</i>	(Optional) Displays information for a specific interface. Valid interfaces include physical ports and port channels.
vlan <i>vlan-id</i>	(Optional) Displays entries for the specific VLAN only. The range is 1 to 4094.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Example

This example shows the 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
```

show mac address-table aging-time

To display the aging time of address table entries, use the **show mac address-table aging-time** command in EXEC mode.

show mac address-table aging-time [**vlan** *vlan-id*]

Syntax Description	vlan (Optional) Displays aging time information for a specific VLAN. The range is 1 to 4094. <i>vlan-id</i>
---------------------------	---

Command Modes	User EXEC Privileged EXEC
----------------------	------------------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines	If no VLAN number is specified, the aging time for all VLANs appears. This command displays 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.
-------------------------	--

Example

This example shows the output from the **show mac address-table aging-time** command:

```
Switch# show mac address-table aging-time
```

```
Vlan    Aging Time
----    -
1       300
```

This example shows the 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
```

show mac address-table count

To display the number of addresses present in all VLANs or the specified VLAN, use the **show mac address-table count** command in EXEC mode.

show mac address-table count [**vlan** *vlan-id*]

Syntax Description	vlan (Optional) Displays the number of addresses for a specific VLAN. The range is 1 to 4094. <i>vlan-id</i>				
Command Modes	User EXEC Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.				
Usage Guidelines	If no VLAN number is specified, the address count for all VLANs appears.				

Example

This example shows the 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
```

show mac address-table dynamic

To display only dynamic MAC address table entries, use the **show mac address-table dynamic** command in EXEC mode.

```
show mac address-table dynamic [address mac-address] [interface interface-id] [vlan vlan-id]
```

Syntax Description	
address <i>mac-address</i>	(Optional) Specifies a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
interface <i>interface-id</i>	(Optional) Specifies an interface to match; valid interfaces include physical ports and port channels.
vlan <i>vlan-id</i>	(Optional) Displays entries for a specific VLAN; the range is 1 to 4094.

Command Modes	
	User EXEC
	Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Example

This example shows the 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
```

show mac address-table interface

To display the MAC address table information for a specified interface on a specified VLAN, use the **show mac address-table interface** EXEC command.

show mac address-table interface *interface-id* [**vlan** *vlan-id*]

Syntax Description

interface-id The interface type; valid interfaces include physical ports and port channels.

vlan (Optional) Displays entries for a specific VLAN; the range is 1 to 4094.
vlan-id

Command Modes

User EXEC

Privileged EXEC

Command History

Release

Modification

Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E This command was introduced.

Example

This example shows the 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

```


show mac address-table learning

To display the status of MAC address learning for all VLANs or a specified VLAN, use the **show mac address-table learning** command in EXEC mode.

show mac address-table learning [**vlan** *vlan-id*]

Syntax Description	vlan (Optional) Displays information for a specific VLAN. The range is 1 to 4094. <i>vlan-id</i>
---------------------------	--

Command Modes	User EXEC Privileged EXEC
----------------------	------------------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines	Use the show mac address-table learning command without any keywords to display configured VLANs and whether MAC address learning is enabled or disabled on them. The default is that MAC address learning is enabled on all VLANs. Use the command with a specific VLAN ID to display the learning status on an individual VLAN.
-------------------------	---



Note	This command is supported only on the LAN Base image.
-------------	---

Example

This example shows the output from the **show mac address-table learning** command showing that MAC address learning is disabled on VLAN 200:

```
Switch# show mac address-table learning
```

```
VLAN      Learning Status
----      -
1         yes
100      yes
200      no
```

show mac address-table move update

To display the MAC address-table move update information on the device, use the **show mac address-table move update** command in EXEC mode.

show mac address-table move update

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Example

This example shows the output from the **show mac address-table move update** command:

```
Device# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

show mac address-table multicast

To display information about the multicast MAC address table, use the **show mac-address-table multicast** command.

```
show mac-address-table multicast [count | {igmp-snooping [count]} | {user [count]} |
{vlan vlan_num}]
```

Syntax Description

count	(Optional) Displays the number of multicast entries.
igmp-snooping	(Optional) Displays only the addresses learned by IGMP snooping.
user	(Optional) Displays only the user-entered static addresses.
vlan <i>vlan_num</i>	(Optional) Displays information for a specific VLAN only; valid values are from 1 to 4094.

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

For the MAC address table entries that are used by the routed ports, the routed port name is displayed in the "vlan" column, not the internal VLAN number.

Example

This example shows how to display multicast MAC address table information for a specific VLAN:

```
Switch# show mac-address-table multicast vlan 1
```

```
Multicast Entries
vlan  mac address      type    ports
-----+-----+-----+-----
  1    ffff.ffff.ffff    system  Switch,Fa6/15
Switch#
```

This example shows how to display the number of multicast MAC entries for all VLANs:

```
Switch# show mac-address-table multicast count
```

```
MAC Entries for all vlans:
Multicast MAC Address Count:          141
Total Multicast MAC Addresses Available: 16384
Switch#
```

show mac address-table notification

To display the MAC address notification settings for all interfaces or the specified interface, use the **show mac address-table notification** command in EXEC mode.

```
show mac address-table notification {change [interface[interface-id]] | mac-move | threshold}
```

Syntax Description		
change		The MAC change notification feature parameters and history table.
interface		(Optional) Displays information for all interfaces. Valid interfaces include physical ports and port channels.
interface-id		(Optional) The specified interface. Valid interfaces include physical ports and port channels.
mac-move		Displays status for MAC address move notifications.
threshold		Displays status for MAC address-table threshold monitoring.

Command Default

By default, the MAC address notification, MAC move, and MAC threshold monitoring are disabled.

The default MAC utilization threshold is 50 percent.

The default time between MAC threshold notifications is 120 seconds.

Command Modes

User EXEC

Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Use the **show mac address-table notification change** command without keywords to see if the MAC address change notification feature is enabled or disabled, the number of seconds in the MAC notification interval, the maximum number of entries allowed in the history table, and the history table contents.

Use the **interface** keyword to display the notifications for all interfaces. If the interface ID is included, only the flags for that interface appear.

Example

This example shows the output from the **show mac address-table notification change** command:

```
Switch# show mac address-table notification change
```

```
MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 60 secs
Number of MAC Addresses Added : 4
Number of MAC Addresses Removed : 4
Number of Notifications sent to NMS : 3
```

```
Maximum Number of entries configured in History Table : 100
Current History Table Length : 3
MAC Notification Traps are Enabled

History Table contents
-----
History Index 0, Entry Timestamp 1032254, Despatch Timestamp 1032254
MAC Changed Message :
Operation: Added Vlan: 2 MAC Addr: 0000.0000.0001 Module: 0 Port: 1

History Index 1, Entry Timestamp 1038254, Despatch Timestamp 1038254
MAC Changed Message :
Operation: Added Vlan: 2 MAC Addr: 0000.0000.0000 Module: 0 Port: 1
Operation: Added Vlan: 2 MAC Addr: 0000.0000.0002 Module: 0 Port: 1
Operation: Added Vlan: 2 MAC Addr: 0000.0000.0003 Module: 0 Port: 1

History Index 2, Entry Timestamp 1074254, Despatch Timestamp 1074254
MAC Changed Message :
Operation: Deleted Vlan: 2 MAC Addr: 0000.0000.0001 Module: 0 Port: 1
Operation: Deleted Vlan: 2 MAC Addr: 0000.0000.0002 Module: 0 Port: 1
Operation: Deleted Vlan: 2 MAC Addr: 0000.0000.0003 Module: 0 Port: 1
```

show mac address-table secure

To display only secure MAC address table entries, use the **show mac address-table secure** command in EXEC mode.

show mac address-table secure [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Syntax Description	address <i>mac-address</i>	(Optional) Specifies a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
	interface <i>interface-id</i>	(Optional) Specifies an interface to match; valid interfaces include physical ports and port channels.
	vlan <i>vlan-id</i>	(Optional) Displays entries for a specific VLAN; the range is 1 to 4094.
Command Modes	User EXEC Privileged EXEC	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Example

This example shows the output from the **show mac address-table secure** command:

```
Switch# show mac address-table secure

                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
```

show mac address-table static

To display only static MAC address table entries, use the **show mac address-table static** command in EXEC mode.

```
show mac address-table static [address mac-address] [interface interface-id] [vlan vlan-id]
```

Syntax Description	Parameter	Description
	address <i>mac-address</i>	(Optional) Specifies a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
	interface <i>interface-id</i>	(Optional) Specifies an interface to match; valid interfaces include physical ports and port channels.
	vlan <i>vlan-id</i>	(Optional) Specifies the address for a specific VLAN. The range is from 1 to 4094.

Command Modes	Mode
	User EXEC
	Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Example

This example shows the 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
```

show mac address-table vlan

To display the MAC address table information for a specified VLAN, use the **show mac address-table vlan** command in EXEC mode.

show mac address-table vlan *vlan-id*

Syntax Description	<i>vlan-id</i> The address for a specific VLAN. The range is 1 to 4094.
---------------------------	---

Command Modes	User EXEC Privileged EXEC
----------------------	------------------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Example

This example shows the 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

```


show nmosp

To display the Network Mobility Services Protocol (NMSP) configuration settings, use the **show nmosp** command.

```
show nmosp {attachment | {suppress interfaces} | capability | notification interval | statistics
{connection | summary} | status | subscription detail [ip-addr ] | summary}
```

Syntax Description		
attachment suppress interfaces		Displays attachment suppress interfaces.
capability		Displays NMSP capabilities.
notification interval		Displays the NMSP notification interval.
statistics connection		Displays all connection-specific counters.
statistics summary		Displays the NMSP counters.
status		Displays status of active NMSP connections.
subscription detail ip-addr		The details are only for the NMSP services subscribed to by a specific IP address.
subscription summary		Displays details for all of the NMSP services to which the controller is subscribed. The details are only for the NMSP services subscribed to by a specific IP address.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

The following is sample output from the **show nmosp notification interval** command:

```
Device# show nmosp notification interval
NMSP Notification Intervals
-----

RSSI Interval:
  Client           : 2 sec
  RFID             : 2 sec
  Rogue AP         : 2 sec
  Rogue Client     : 2 sec
Attachment Interval : 30 sec
Location Interval  : 30 sec
```

show onboard switch

To display OBFL information use the **show onboard switch** privileged EXEC command.

show onboard switch *switch-number*{**clilog** | **environment** | **message** | **counter** | **temperature** | **uptime** | **voltage** | **status**}

Syntax Description

<i>switch-number</i>	Specifies the switch or stack member numbers.
clilog	Displays the OBFL CLI commands that were entered on a standalone switch or the specified stack members.
environment	Displays the UDI information for a standalone switch or the specified stack members. For all the connected FRU devices, it displays the PID, the VID, and the serial number.
message	Displays the hardware-related messages generated by a standalone switch or the specified stack members.
counter	Displays the counter information on a standalone switch or the specified stack members.
temperature	Displays the temperature of a standalone switch or the specified switch stack members.
uptime	Displays the time when a standalone switch or the specified stack members start, the reason the standalone switch or specified stack members restart, and the length of time that the standalone switch or specified stack members have been running since they last restarted.
voltage	Displays the system voltages of a standalone switch or the specified stack members.
status	Displays the status of a standalone switch or the specified stack members.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Example

The following example displays the OBFL CLI commands entered on a standalone switch or the specified stack member:

```
Switch# show onboard switch 1 clilog
```

The following example displays the UDI information for a standalone switch or the specified stack members. For all the connected FRU devices, it displays the PID, the VID, and the serial number.

```
Switch# show onboard switch 1 environment
```

The following example displays the hardware-related messages generated by a standalone switch or the specified stack members.

```
Switch# show onboard switch 1 message
```

The following example displays the counter information on a standalone switch or the specified stack members.

```
Switch# show onboard switch 1 counter
```

The following example displays the temperature of a standalone switch or the specified stack members.

```
Switch# show onboard switch 1 temperature
```

The following example displays the time when a standalone switch or the specified stack members start, the reason the standalone switch or the specified stack members restart, and the length of time that the standalone switch or the specified stack members have been running since they last restarted.

```
Switch# show onboard switch 1 uptime
```

The following example displays the system voltages of a standalone switch or the specified stack members.

```
Switch# show onboard switch 1 voltage
```

The following example displays the status of a standalone switch or the specified stack members.

```
Switch# show onboard switch 1 status
```

shutdown

To shut down VLAN switching, use the **shutdown** command in global configuration mode. To disable the configuration set, use the **no** form of this command.

```
shutdown [ vlan vlan-id ]
no shutdown
```

Syntax Description	vlan <i>vlan-id</i>	VLAN ID of VLAN to shutdown.
Command Default	No default behavior or values.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Examples

This example shows how to shutdown a VLAN:

```
Device(config)# vlan open1
Device(config-wlan)# shutdown
```

This example shows that the access point is not shut down:

```
Device# configure terminal
Device(config)# ap name 3602a no shutdown
```

test cable-diagnostics prbs

To run the pseudo-random binary sequence (PRBS) feature on an interface, use the **test cable-diagnostics prbs** command in privileged EXEC mode.

```
test cable-diagnostics prbs interface interface-id
```

Syntax Description

interface-id The interface on which to run PRBS.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

PRBS is supported only on 10-Gigabit Ethernet ports. It is not supported on 10/100/100 copper Ethernet ports and small form-factor pluggable (SFP) module ports.

After you run PRBS by using the **test cable-diagnostics prbs interface interface-id** command, use the **show cable-diagnostics prbs interface interface-id** privileged EXEC command to display the results.

Example

This example shows how to run PRBS on an interface:

```
Switch# test cable-diagnostics prbs interface gigabitethernet1/0/2
PRBS test started on interface Gi1/0/2
A PRBS test can take a few seconds to run on an interface
Use 'show cable-diagnostics prbs' to read the TDR results
```

test cable-diagnostics tdr

To run the Time Domain Reflector (TDR) feature on an interface, use the **test cable-diagnostics tdr** command in privileged EXEC mode.

test cable-diagnostics tdr interface *interface-id*

Syntax Description

interface-id The interface on which to run TDR.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

TDR is supported only on 10/100/100 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports or small form-factor pluggable (SFP) module ports.

After you run TDR by using the **test cable-diagnostics tdr interface** *interface-id* command, use the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command to display the results.

This example shows how to run TDR on an interface:

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results
```

If you enter the **test cable-diagnostics tdr interface** *interface-id* command on an interface that has a link up status and a speed of 10 or 100 Mb/s, these messages appear:

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/3
TDR test on Gi1/0/9 will affect link state and traffic
TDR test started on interface Gi1/0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command in privileged EXEC mode.

```
traceroute mac [interface interface-id] source-mac-address [interface interface-id]
destination-mac-address [vlan vlan-id] [detail]
```

Syntax Description

interface <i>interface-id</i>	(Optional) Specifies an interface on the source or destination device.
<i>source-mac-address</i>	The MAC address of the source device in hexadecimal format.
<i>destination-mac-address</i>	The MAC address of the destination device in hexadecimal format.
vlan <i>vlan-id</i>	(Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source device to the destination device. Valid VLAN IDs are 1 to 4094.
detail	(Optional) Specifies that detailed information appears.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E
	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all of the devices in the network. Do not disable CDP.

When the device detects a device in the Layer 2 path that does not support Layer 2 traceroute, the device 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:

```
Device# tracert mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5      ) :   Gi0/0/3 => Gi0/0/1
con1          (2.2.1.1      ) :   Gi0/0/1 => Gi0/0/2
con2          (2.2.2.2      ) :   Gi0/0/2 => Gi0/0/1
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:

```
Device# tracert mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 / WS-C3750E-24PD / 2.2.6.6 :
      Gi0/0/2 [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 interfaces on the source and destination devices:

```
Device# tracert mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5      ) :   Gi0/0/3 => Gi0/0/1
con1          (2.2.1.1      ) :   Gi0/0/1 => Gi0/0/2
con2          (2.2.2.2      ) :   Gi0/0/2 => Gi0/0/1
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 device is not connected to the source device:

```
Device# tracert mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source ....
Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
con5 / WS-C3750E-24TD / 2.2.5.5 :
      Gi0/0/1 [auto, auto] => Gi0/0/3 [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 device cannot find the destination port for the source MAC address:

```
Device# 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:

```
Device# 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:

```
Device# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

This example shows the Layer 2 path when source and destination devices belong to multiple VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

tracroute mac ip

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, use the **tracroute mac ip** command in privileged EXEC mode.

tracroute mac ip {*source-ip-address source-hostname*} {*destination-ip-address destination-hostname*} [**detail**]

Syntax Description

<i>source-ip-address</i>	The IP address of the source device as a 32-bit quantity in dotted-decimal format.
<i>source-hostname</i>	The IP hostname of the source device.
<i>destination-ip-address</i>	The IP address of the destination device as a 32-bit quantity in dotted-decimal format.
<i>destination-hostname</i>	The IP hostname of the destination device.
detail	(Optional) Specifies that detailed information appears.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on each device in the network. Do not disable CDP.

When the device detects a device in the Layer 2 path that does not support Layer 2 traceroute, the device continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **tracroute 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 device 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 device uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the device 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:

```
Device# 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:

```
Device# 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:

```
Device# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

type

To display the contents of one or more files, use the **type** command in boot loader mode.

type *filesystem:/file-url...*

Syntax Description

filesystem: Alias for a file system. Use **flash:** for the system board flash device; use **usbflash0:** for USB memory sticks.

/file-url... Path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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 appear sequentially.

Examples

This example shows how to display the contents of a file:

```
Device: type flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

unset

To reset one or more environment variables, use the **unset** command in boot loader mode.

unset *variable*...

Syntax Description

variable

Use one of these keywords for *variable*:

MANUAL_BOOT—Specifies whether the device 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—Specifies 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—Identifies the 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—Specifies the 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.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release

Modification

Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

Under typical 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.

Example

This example shows how to unset the SWITCH_PRIORITY environment variable:

```
Device: unset SWITCH_PRIORITY
```

version

To display the boot loader version, use the **version** command in boot loader mode.

version

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Boot loader

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Examples

This example shows how to display the boot loader version on a device:

```
Device: version  
C2960X Boot Loader (C2960X-HBOOT-M) Version 15.0(2r)EX, RELEASE SOFTWARE (fcl)  
Compiled Wed 15-May-13 21:39 by rel
```




PART **X**

VLANs

- [VLAN](#), on page 705



VLAN

- [client vlan, on page 706](#)
- [clear vmps statistics, on page 707](#)
- [clear vtp counters, on page 708](#)
- [debug platform vlan, on page 709](#)
- [debug sw-vlan, on page 710](#)
- [debug sw-vlan ifs, on page 712](#)
- [debug sw-vlan notification, on page 713](#)
- [debug sw-vlan vtp, on page 715](#)
- [interface vlan, on page 717](#)
- [show platform vlan, on page 719](#)
- [show vlan, on page 720](#)
- [show vmps, on page 723](#)
- [show vtp, on page 725](#)
- [switchport priority extend, on page 731](#)
- [switchport trunk, on page 732](#)
- [switchport voice vlan, on page 735](#)
- [vlan, on page 738](#)
- [vmps reconfirm \(global configuration\), on page 744](#)
- [vmps reconfirm \(privileged EXEC\), on page 745](#)
- [vmps retry, on page 746](#)
- [vmps server, on page 747](#)
- [vtp \(global configuration\), on page 749](#)
- [vtp \(interface configuration\), on page 754](#)
- [vtp primary, on page 755](#)

client vlan

To configure a WLAN interface or an interface group, use the **client vlan** command. To disable the WLAN interface, use the **no** form of this command.

client vlan *interface-id-name-or-group-name*
no client vlan

Syntax Description

interface-id-name-or-group-name Interface ID, name, or VLAN group name. The interface ID can also be in digits too.

Command Default

The default interface is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable a client VLAN on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client vlan client-vlan1
Device(config-wlan)# end
```

This example shows how to disable a client VLAN on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no client vlan
Device(config-wlan)# end
```

clear vmps statistics

To clear the VLAN Membership Policy Server (VMPS) statistics maintained by the VLAN Query Protocol (VQP) client, use the **clear vmps statistics** command in privileged EXEC mode.

clear vmps statistics

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

This example shows how to clear VLAN Membership Policy Server (VMPS) statistics:

```
Device# clear vmps statistics
```

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

Related Topics

[show vmps](#), on page 723

clear vtp counters

To clear the VLAN Trunking Protocol (VTP) and pruning counters, use the **clear vtp counters** command in privileged EXEC mode.

clear vtp counters

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E	This command was introduced.

This example shows how to clear the VTP counters:

```
Device# clear vtp counters
```

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

Related Topics

[show vtp](#), on page 725

debug platform vlan

To enable debugging of the VLAN manager software, use the **debug platform vlan** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug platform vlan {error | mvid | rpc}
no debug platform vlan {error | mvid | rpc}
```

Syntax Description

error Displays VLAN error debug messages.

mvid Displays mapped VLAN ID allocations and free debug messages.

rpc Displays remote procedure call (RPC) debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

The **undebug platform vlan** command is the same as the **no debug platform vlan** command.

When you enable debugging on a switch stack, it is enabled only on the stack's active switch. To enable debugging on a stack member, start a session from the stack's active switch using the **session** *switch-number* EXEC command, and then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number* *LINE* EXEC command on the stack's active switch to enable debugging on a member switch without first starting a session.

This example shows how to display VLAN error debug messages:

```
Device# debug platform vlan error
```

debug sw-vlan

To enable debugging of VLAN manager activities, use the **debug sw-vlan** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | mapping | notification | packets | redundancy | registries | vtp}
no debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | mapping | notification | packets | redundancy | registries | vtp}

Syntax Description

badpmcookies	Displays debug messages for VLAN manager incidents of bad port manager cookies.
cfg-vlan	Displays VLAN configuration debug messages.
bootup	Displays messages when the switch is booting up.
cli	Displays messages when the command-line interface (CLI) is in VLAN configuration mode.
events	Displays debug messages for VLAN manager events.
ifs	Displays debug messages for the VLAN manager IOS file system (IFS). See debug sw-vlan ifs, on page 712 for more information.
mapping	Displays debug messages for VLAN mapping.
notification	Displays debug messages for VLAN manager notifications. See debug sw-vlan notification, on page 713 for more information.
packets	Displays debug messages for packet handling and encapsulation processes.
redundancy	Displays debug messages for VTP VLAN redundancy.
registries	Displays debug messages for VLAN manager registries.
vtp	Displays debug messages for the VLAN Trunking Protocol (VTP) code. See debug sw-vlan vtp, on page 715 for more information.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

The **undebug sw-vlan** command is the same as the **no debug sw-vlan** command.

When you enable debugging on a switch stack, it is enabled only on the stack's active switch. To debug a specific stack member, you can start a CLI session from the stack's active switch by using the **session switch-number** privileged EXEC command. You also can use the **remote command** *stack-member-number*

LINE EXEC command on the stack's active switch to enable debugging on a member switch without first starting a session.

This example shows how to display debug messages for VLAN manager events:

```
Device# debug sw-vlan events
```

Related Topics

[debug sw-vlan ifs](#), on page 712

[debug sw-vlan notification](#), on page 713

[debug sw-vlan vtp](#), on page 715

[show vlan](#), on page 720

[show vtp](#), on page 725

debug sw-vlan ifs

To enable debugging of the VLAN manager IOS file system (IFS) error tests, use the **debug sw-vlan ifs** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
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	Displays VLAN manager IFS file-read operation debug messages.
open write	Displays VLAN manager IFS file-write operation debug messages.
read	Displays file-read operation debug messages for the specified error test (1 , 2 , 3 , or 4).
write	Displays file-write operation debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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.

When you enable debugging on a switch stack, it is enabled only on the stack's active switch. To debug a specific stack member, you can start a CLI session from the stack's active switch by using the **session switch-number** privileged EXEC command. You also can use the **remote command stack-member-number LINE** EXEC command on the active switch to enable debugging on a member switch without first starting a session.

This example shows how to display file-write operation debug messages:

```
Device# debug sw-vlan ifs write
```

Related Topics

[show vlan](#), on page 720

debug sw-vlan notification

To enable debugging of VLAN manager notifications, use the **debug sw-vlan notification** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan notification {**accfwdchange** | **allowedvlanfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}

no debug sw-vlan notification {**accfwdchange** | **allowedvlanfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}

Syntax Description

accfwdchange	Displays debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
allowedvlanfgchange	Displays debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
fwdchange	Displays debug messages for VLAN manager notification of spanning-tree forwarding changes.
linkchange	Displays debug messages for VLAN manager notification of interface link-state changes.
modechange	Displays debug messages for VLAN manager notification of interface mode changes.
pruningcfgchange	Displays debug messages for VLAN manager notification of changes to the pruning configuration.
statechange	Displays debug messages for VLAN manager notification of interface state changes.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

The **undebg sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

When you enable debugging on a switch stack, it is enabled only on the stack's active switch. To debug a specific stack member, you can start a CLI session from the stack's active switch by using the **session switch-number** privileged EXEC command. You also can use the **remote command stack-member-number LINE** EXEC command on the active switch to enable debugging on a member switch without first starting a session.

This example shows how to display debug messages for VLAN manager notification of interface mode changes:

```
Device# debug sw-vlan notification
```

Related Topics

[show vlan](#), on page 720

debug sw-vlan vtp

To enable debugging of the VLAN Trunking Protocol (VTP) code, use the **debug sw-vlan vtp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug sw-vlan vtp {events | packets | pruning [{packets | xmit}] | redundancy | xmit}
no debug sw-vlan vtp {events | packets | pruning | redundancy | xmit}
```

Syntax Description		
	events	Displays debug messages for general-purpose logic flow and detailed VTP messages generated by the VTP_LOG_RUNTIME macro in the VTP code.
	packets	Displays debug messages for the contents of all incoming VTP packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer, except for pruning packets.
	pruning	Displays debug messages generated by the pruning segment of the VTP code.
	packets	(Optional) Displays debug messages for the contents of all incoming VTP pruning packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer.
	xmit	(Optional) Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send.
	redundancy	Displays debug messages for VTP redundancy.
	xmit	Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send, except for pruning packets.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E 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 additional 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.

When you enable debugging on a switch stack, it is enabled only on the stack's active switch. To debug a specific stack member, you can start a CLI session from the stack's active switch by using the **session switch-number** privileged EXEC command. You also can use the **remote command switch-member-number**

LINE EXEC command on the stack's active switch to enable debugging on a member switch without first starting a session.

This example shows how to display debug messages for VTP redundancy:

```
Device# debug sw-vlan vtp redundancy
```

Related Topics

[show vtp](#), on page 725

interface vlan

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

interface vlan *vlan-id*
no interface vlan *vlan-id*

Syntax Description	<i>vlan-id</i> VLAN number. The range is 1 to 4094.				
Command Default	The default VLAN interface is VLAN 1.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.				
Usage Guidelines	SVIs are created the first time you enter the interface vlan <i>vlan-id</i> command for a particular VLAN. The <i>vlan-id</i> 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 using the **no interface vlan** *vlan-id* command, it is no longer visible in the output from the **show interfaces** privileged EXEC command.



Note You cannot delete the VLAN 1 interface.

You can reinstate 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 or a switch stack 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.

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

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

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

Related Topics

[show interfaces](#), on page 87

show platform vlan

To display platform-dependent VLAN information, use the **show platform vlan** privileged EXEC command.

```
show platform vlan {misc | mvid | prune | refcount | rpc {receive | transmit}}
```

Syntax Description

misc	Displays miscellaneous VLAN module information.
mvid	Displays the mapped VLAN ID (MVID) allocation information.
prune	Displays the stack or platform-maintained pruning database.
refcount	Displays the VLAN lock module-wise reference counts.
rpc	Displays remote procedure call (RPC) messages.
receive	Displays received information.
transmit	Displays sent information.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

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.

This example shows how to display remote procedure call (RPC) messages:

```
Device# show platform vlan rpc
```

show vlan

To display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch, use the **show vlan** command in user EXEC mode.

show vlan [{**brief** | **group** | **id** *vlan-id* | **mtu** | **name** *vlan-name* | **remote-span** | **summary**}]

Syntax Description		
brief		(Optional) Displays one line for each VLAN with the VLAN name, status, and its ports.
group		(Optional) Displays information about VLAN groups.
id <i>vlan-id</i>		(Optional) Displays information about a single VLAN identified by the VLAN ID number. For <i>vlan-id</i> , the range is 1 to 4094.
mtu		(Optional) Displays a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.
name <i>vlan-name</i>		(Optional) Displays information about a single VLAN identified by the VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
remote-span		(Optional) Displays information about Remote SPAN (RSPAN) VLANs.
summary		(Optional) Displays VLAN summary information.



Note The **ifindex** keyword is not supported, even though it is visible in the command-line help string.

Command Default None

Command Modes User EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E 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 the 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 ports with the MinMTU and the MaxMTU appear.

This is an example of output from the **show vlan** command. See the table that follows for descriptions of the fields in the display.

```

Device> show vlan
VLAN Name                               Status      Ports
-----
1    default                               active     Gi1/0/2, Gi1/0/3, Gi1/0/4
                                           Gi1/0/5, Gi1/0/6, Gi1/0/7
                                           Gi1/0/8, Gi1/0/9, Gi1/0/10
                                           Gi1/0/11, Gi1/0/12, Gi1/0/13
                                           Gi1/0/14, Gi1/0/15, Gi1/0/16
                                           Gi1/0/17, Gi1/0/18, Gi1/0/19
                                           Gi1/0/20, Gi1/0/21, Gi1/0/22
                                           Gi1/0/23, Gi1/0/24, Gi1/0/25
                                           Gi1/0/26, Gi1/0/27, Gi1/0/28
                                           Gi1/0/29, Gi1/0/30, Gi1/0/31
                                           Gi1/0/32, Gi1/0/33, Gi1/0/34
                                           Gi1/0/35, Gi1/0/36, Gi1/0/37
                                           Gi1/0/38, Gi1/0/39, Gi1/0/40
                                           Gi1/0/41, Gi1/0/42, Gi1/0/43
                                           Gi1/0/44, Gi1/0/45, Gi1/0/46
                                           Gi1/0/47, Gi1/0/48

2    VLAN0002                               active
40   vlan-40                                 active
300  VLAN0300                               active
1002 fddi-default                           act/unsup
1003 token-ring-default                   act/unsup
1004 fddinet-default                       act/unsup
1005 trnet-default                         act/unsup

VLAN Type  SAID      MTU   Parent RingNo BridgeNo  Stp  BrdgMode  Trans1  Trans2
-----
1    enet  100001    1500 -     -     -     -     -     0      0
2    enet  100002    1500 -     -     -     -     -     0      0
40   enet  100040    1500 -     -     -     -     -     0      0
300  enet  100300    1500 -     -     -     -     -     0      0
1002 fddi  101002    1500 -     -     -     -     -     0      0
1003 tr   101003    1500 -     -     -     -     -     0      0
1004 fdnet 101004    1500 -     -     -     -     -     0      0
1005 trnet 101005    1500 -     -     -     -     -     0      0
2000 enet  102000    1500 -     -     -     -     -     0      0
3000 enet  103000    1500 -     -     -     -     -     0      0

Remote SPAN VLANs
-----
2000,3000

Primary Secondary Type          Ports
-----

```

Table 40: 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.

Field	Description
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 summary** command:

```
Device> 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:

```
Device# show vlan id 2
VLAN Name                Status    Ports
-----
2    VLAN0200                active    Gi1/0/7, Gi1/0/8
2    VLAN0200                active    Gi2/0/1, Gi2/0/2

VLAN Type  SAID      MTU   Parent  RingNo BridgeNo  Stp   BrdgMode Trans1 Trans2
-----
2    enet    100002   1500   -       -        -     -        0      0

Remote SPAN VLANs
-----
Disabled
```

Related Topics

[switchport mode
vlan](#), on page 738

show vmps

To display the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, and the current and primary servers, use the **show vmps** command in EXEC mode.

show vmps [**statistics**]

Syntax Description	statistics (Optional) Displays VQP client-side statistics and counters.				
Command Default	None				
Command Modes	User EXEC Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)E</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.				

Examples

This is an example of output from the **show vmps** command:

```
Device> show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status
-----
VMPS Action:          other
```

This is an example of output from the **show vmps statistics** command. The table that follows describes each field in the display.

```
Device> show vmps statistics
VMPS Client Statistics
-----
VQP Queries:          0
VQP Responses:        0
VMPS Changes:         0
VQP Shutdowns:        0
VQP Denied:           0
VQP Wrong Domain:     0
VQP Wrong Version:    0
VQP Insufficient Resource: 0
```

Table 41: show vmps statistics Field Descriptions

Field	Description
VQP Queries	Number of queries sent by the client to the VMPS.
VQP Responses	Number of responses sent to the client from the VMPS.
VMPS Changes	Number of times that the VMPS changed from one server to another.
VQP Shutdowns	Number of times the VMPS sent a response to shut down the port. The client disables the port and removes all dynamic addresses on this port from the address table. You must administratively reenable the port to restore connectivity.
VQP Denied	Number of times the VMPS denied the client request for security reasons. When the VMPS response denies an address, no frame is forwarded to or from the workstation with that address (broadcast or multicast frames are delivered to the workstation if the port has been assigned to a VLAN). The client keeps the denied address in the address table as a blocked address to prevent more queries from being sent to the VMPS for each new packet received from this workstation. The client ages the address if no new packets are received from this workstation on this port within the aging time period.
VQP Wrong Domain	Number of times the management domain in the request does not match the one for the VMPS. Any previous VLAN assignments of the port are not changed. This response means that the server and the client have not been configured with the same VTP management domain.
VQP Wrong Version	Number of times the version field in the query packet contains a value that is higher than the version supported by the VMPS. The VLAN assignment of the port is not changed. The switches send only VMPS Version 1 requests.
VQP Insufficient Resource	Number of times the VMPS is unable to answer the request because of a resource availability problem. If the retry limit has not yet been reached, the client repeats the request with the same server or with the next alternate server, depending on whether the per-server retry count has been reached.

Related Topics

[clear vmps statistics](#), on page 707

[vmps reconfirm \(global configuration\)](#), on page 744

[vmps retry](#), on page 746

[vmps server](#), on page 747

show vtp

To display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters, use the **show vtp** command in EXEC mode.

show vtp {**counters** | **devices** [**conflicts**] | **interface** [*interface-id*] | **password** | **status**}

Syntax Description		
counters		Displays the VTP statistics for the device.
devices		Displays information about all VTP version 3 devices in the domain. This keyword applies only if the device is not running VTP version 3.
conflicts		(Optional) Displays information about VTP version 3 devices that have conflicting primary servers. This command is ignored when the device is in VTP transparent or VTP off mode.
interface		Displays VTP status and configuration for all interfaces or the specified interface.
<i>interface-id</i>		(Optional) Interface for which to display VTP status and configuration. This can be a physical interface or a port channel.
password		Displays the configured VTP password (available in privileged EXEC mode only).
status		Displays general information about the VTP management domain status.

Command Default None

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines When you enter the **show vtp password** command when the device is running VTP version 3, the display follows these rules:

- If the **password** *password* global configuration command did not specify the **hidden** keyword and encryption is not enabled on the device, the password appears in clear text.
- If the **password** *password* command did not specify the **hidden** keyword and encryption is enabled on the device, the encrypted password appears.
- If the **password** *password* command is included the **hidden** keyword, the hexadecimal secret key is displayed.

This is an example of output from the **show vtp devices** command. A **Yes** in the **Conflict** column indicates that the responding server is in conflict with the local server for the feature; that is, when two devices in the same domain do not have the same primary server for a database.

```
Device# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf device ID      Primary Server Revision  System Name
-----
VLAN      Yes  00b0.8e50.d000 000c.0412.6300 12354      main.cisco.com
MST       No   00b0.8e50.d000 0004.AB45.6000 24         main.cisco.com
VLAN      Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com
```

This is an example of output from the **show vtp counters** command. The table that follows describes each field in the display.

```
Device> 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
-----
Gi1/0/47       0                 0                 0
Gi1/0/48       0                 0                 0
Gi2/0/1        0                 0                 0
Gi3/0/2        0                 0                 0
```

Table 42: show vtp counters Field Descriptions

Field	Description
Summary advertisements received	Number of summary advertisements received by this device 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 device 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 device on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.

Field	Description
Summary advertisements transmitted	Number of summary advertisements sent by this device 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 device 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 device 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	<p>Number of revision errors.</p> <p>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 device increments.</p> <p>Revision errors increment whenever the device receives an advertisement whose revision number matches the revision number of the device, but the MD5 digest values do not match. This error means that the VTP password in the two devices is different or that the devices have different configurations.</p> <p>These errors indicate that the device is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>
Number of configuration digest errors	<p>Number of MD5 digest errors.</p> <p>Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the device do not match. This error usually means that the VTP password in the two devices is different. To solve this problem, make sure the VTP password on all devices is the same.</p> <p>These errors indicate that the device is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>

Field	Description
Number of V1 summary errors	Number of Version 1 errors. Version 1 summary errors increment whenever a device in VTP V2 mode receives a VTP Version 1 frame. These errors indicate that at least one neighboring device is either running VTP Version 1 or VTP Version 2 with V2-mode disabled. To solve this problem, change the configuration of the devices 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. The table that follows describes each field in the display.

```
Device> show vtp status
VTP Version capable           : 1 to 3
VTP version running          : 1
VTP Domain Name               :
VTP Pruning Mode              : Disabled
VTP Traps Generation          : Disabled
Device ID                     : 2037.06ce.3580
Configuration last modified by 192.168.1.1 at 10-10-12 04:34:02
Local updater ID is 192.168.1.1 on interface LIIN0 (first layer3 interface found)

Feature VLAN:
-----
VTP Operating Mode            : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs      : 7
Configuration Revision        : 2
MD5 digest                   : 0xA0 0xA1 0xFE 0x4E 0x7E 0x5D 0x97 0x41
                               0x89 0xB9 0x9B 0x70 0x03 0x61 0xE9 0x27
```

Table 43: show vtp status Field Descriptions

Field	Description
VTP Version capable	Displays the VTP versions that are capable of operating on the device.
VTP Version running	Displays the VTP version operating on the device. By default, the device implements Version 1 but can be set to Version 2.
VTP Domain Name	Name that identifies the administrative domain for the device.

Field	Description
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 Traps Generation	Displays whether VTP traps are sent to a network management station.
Device ID	Displays the MAC address of the local device.
Configuration last modified	Displays the date and time of the last configuration modification. Displays the IP address of the device that caused the configuration change to the database.
VTP Operating Mode	<p>Displays the VTP operating mode, which can be server, client, or transparent.</p> <p>Server—A device in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The device guarantees that it can recover all the VLAN information in the current VTP database from NVRAM after reboot. By default, every device is a VTP server.</p> <p>Note The device 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.</p> <p>Client—A device 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.</p> <p>Transparent—A device 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 device receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.</p>
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.

Field	Description
Configuration Revision	Current configuration revision number on this device.
MD5 Digest	A 16-byte checksum of the VTP configuration.

This is an example of output from the **show vtp status** command for a device running VTP version 3:

```
Device# show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 3
VTP Domain Name         : Cisco
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : 0cd9.9624.dd80
```

Feature VLAN:

```
-----
VTP Operating Mode      : Off
Number of existing VLANs : 11
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 1005
```

Feature MST:

```
-----
VTP Operating Mode      : Transparent
```

Feature UNKNOWN:

```
-----
VTP Operating Mode      : Transparent
```

Related Topics

[clear vtp counters](#), on page 708

switchport priority extend

To set a port priority for the incoming untagged frames or the priority of frames received by the IP phone connected to the specified port, use the **switchport priority extend** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

switchport priority extend {*cos value* | **trust**}
no switchport priority extend

Syntax Description	cos value	trust
	Sets the IP phone port to override the IEEE 802.1p priority received from the PC or the attached device with the specified class of service (CoS) value. The range is 0 to 7. Seven is the highest priority. The default is 0.	Sets the IP phone port to trust the IEEE 802.1p priority received from the PC or the attached device.

Command Default The default port priority is set to a CoS value of 0 for untagged frames received on the port.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines When voice VLAN is enabled, you can configure the device to send the Cisco Discovery Protocol (CDP) packets to instruct the IP phone how to send data packets from the device attached to the access port on the Cisco IP Phone. You must enable CDP on the device port connected to the Cisco IP Phone to send the configuration to the Cisco IP Phone. (CDP is enabled by default globally and on all device interfaces.)

You should configure voice VLAN on device access ports.

Before you enable voice VLAN, we recommend that you enable quality of service (QoS) on the device by entering the **mls qos** global configuration command and configure the port trust state to trust by entering the **mls qos trust cos** interface configuration command.

This example shows how to configure the IP phone connected to the specified port to trust the received IEEE 802.1p priority:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport priority extend trust
```

You can verify your settings by entering the **show interfaces interface-id switchport** privileged EXEC command.

switchport trunk

To set the trunk characteristics when the interface is in trunking mode, use the **switchport trunk** command in interface configuration mode. To reset a trunking characteristic to the default, use the **no** form of this command.

```
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 <i>vlan-list</i>	Sets the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the Usage Guidelines for the <i>vlan-list</i> choices.
native vlan <i>vlan-id</i>	Sets 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 <i>vlan-list</i>	Sets the list of VLANs that are eligible for VTP pruning when in trunking mode. See the Usage Guidelines for the <i>vlan-list</i> choices.

Command Default

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
Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

The *vlan-list* format is **all** | **none** | [**add** | **remove** | **except**] *vlan-atom* [,*vlan-atom*...]:

- **all** specifies all VLANs from 1 to 4094. This is the default. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** specifies 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.

- **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.

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.

This example shows how to configure VLAN 3 as the default for the port to send all untagged traffic:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk native vlan 3
```

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Device(config)# interface gigabitethernet1/0/2
Device(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:

```
Device(config)# interface gigabitethernet1/0/2
Device(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 Topics

[show interfaces](#), on page 87

[switchport mode](#)

switchport voice vlan

To configure voice VLAN on the port, use the **switchport voice vlan** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
switchport voice vlan {vlan-id | dot1p | none | untagged | name vlan_name}
no switchport voice vlan
```

Syntax Description		
<i>vlan-id</i>		The VLAN to be used for voice traffic. The range is 1 to 4094. By default, the IP phone forwards the voice traffic with an IEEE 802.1Q priority of 5.
dot1p		Configures the telephone to use IEEE 802.1p priority tagging and uses VLAN 0 (the native VLAN). By default, the Cisco IP phone forwards the voice traffic with an IEEE 802.1p priority of 5.
none		Does not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.
untagged		Configures the telephone to send untagged voice traffic. This is the default for the telephone.
name <i>vlan_name</i>	(Optional)	Specifies the VLAN name to be used for voice traffic. You can enter up to 128 characters.

Command Default The default is not to automatically configure the telephone (**none**).
The telephone default is not to tag frames.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E	This command was introduced.
		Option to specify a VLAN name for voice VLAN. The ' name ' keyword was added.

Usage Guidelines You should configure voice VLAN on Layer 2 access ports.

You must enable Cisco Discovery Protocol (CDP) on the switch port connected to the Cisco IP phone for the device to send configuration information to the phone. CDP is enabled by default globally and on the interface.

Before you enable voice VLAN, we recommend that you enable quality of service (QoS) on the switch by entering the **mls qos** global configuration command and configure the port trust state to trust by entering the **mls qos trust cos** interface configuration command.

When you enter a VLAN ID, the IP phone forwards voice traffic in IEEE 802.1Q frames, tagged with the specified VLAN ID. The device puts IEEE 802.1Q voice traffic in the voice VLAN.

When you select **dot1p**, **none**, or **untagged**, the device puts the indicated voice traffic in the access VLAN.

In all configurations, the voice traffic carries a Layer 2 IP precedence value. The default is 5 for voice traffic.

When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to 2. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but not on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.

If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN.

You cannot configure static secure MAC addresses in the voice VLAN.

The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

This example show how to first populate the VLAN database by associating a VLAN ID with a VLAN name, and then configure the VLAN (using the name) on an interface, in the access mode: You can also verify your configuration by entering the **show interfaces interface-id switchport** in privileged EXEC command and examining information in the Voice VLAN: row.

Part 1 - Making the entry in the VLAN database:

```
Device# configure terminal
Device(config)# vlan 55
Device(config-vlan)# name test
Device(config-vlan)# end
Device#
```

Part 2 - Checking the VLAN database:

```
Device# show vlan id 55
VLAN Name Status Ports
-----
55 test active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
55 enet 100055 1500 - - - - - 0 0
Remote SPAN VLAN
-----
Disabled
Primary Secondary Type Ports
-----
```

Part 3- Assigning VLAN to the interface by using the name of the VLAN:

```
Device# configure terminal
Device(config)# interface gigabitethernet3/1/1
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan name test
Device(config-if)# end
Device#
```

Part 4 - Verifying configuration:

```
Device# show running-config
interface gigabitethernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
```

```
switchport voice vlan 55
switchport mode access
Switch#
```

Part 5 - Also can be verified in interface switchport:

```
Device# show interface GigabitEthernet3/1/1 switchport
Name: Gi3/1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 55 (test)
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
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Device#
```

Related Topics

[show interfaces](#), on page 87

[switchport priority extend](#), on page 731

vlan

To add a VLAN and to enter the VLAN configuration mode, use the **vlan** command in global configuration mode. To delete the VLAN, use the **no** form of this command.

vlan *vlan-id*
no vlan *vlan-id*

Syntax Description	<i>vlan-id</i> ID of the VLAN to be added and configured. 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.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines	Up to 1000 VLANs are supported when the is running the LAN Base image with the LAN Base default template, and up to 64 VLANs are supported when the is running the LAN Lite image.
-------------------------	--

You can use the **vlan** *vlan-id* global configuration command to add normal-range VLANs (VLAN IDs 1 to 1005) or extended-range VLANs (VLAN IDs 1006 to 4094). Configuration information for normal-range VLANs is always saved in the VLAN database, and you can display this information by entering the **show vlan** privileged EXEC command. With VTP version 1 and 2, extended-range VLANs are not recognized by VTP and are not added to the VLAN database. With VTP version 1 and version 2, before adding extended-range VLANs, you must use the **vtp transparent** global configuration command to put the device in VTP transparent mode. 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 device startup configuration file.

VTP version 3 supports propagation of extended-range VLANs and you can create them in VTP server or client mode. VTP versions 1 and 2 propagate only VLANs 1 to 1005.

When you save the VLAN and VTP configurations in the startup configuration file and reboot the device, the configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and 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 or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

With VTP version 1 and version 2, if you try to create an extended-range VLAN when the device 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 VLAN configuration mode.

Entering the **vlan** command with a VLAN ID enables VLAN configuration 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 VLAN configuration mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.



Note Although all commands are visible, the only VLAN configuration commands that are supported on extended-range VLANs are **mtu** *mtu-size* and **remote-span**. For extended-range VLANs, all other characteristics must remain at the default state.

These configuration commands are available in VLAN configuration mode. The **no** form of each command returns the characteristic to its 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 that have 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 VLAN configuration mode.
- **media**—Defines the VLAN media type and is one of these:



Note The device supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other devices. These VLANs are locally suspended.

- **ethernet**—Ethernet media type (the default).
- **fd-net**—FDDI network entity title (NET) media type.
- **fdi**—FDDI media type.
- **tokenring**—Token Ring media type if the VTP v2 mode is disabled, or TrCRF if the VTP Version 2 (v) mode is enabled.
- **tr-net**—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.

See the table that follows for valid commands and syntax for different media types.

- **mtu** *mtu-size*—Specifies the maximum transmission unit (MTU) (packet size in bytes). The range is 576 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**—Configures 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.



Note The RSPAN feature is supported only on switches running the LAN Base image.

- **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 VLAN configuration 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**—IEEE Ethernet STP running source-route transparent (SRT) bridging.
 - **ibm**—IBM STP running source-route bridging (SRB).
 - **auto**—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 44: Valid Commands and Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	name <i>vlan-name</i> , media ethernet , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , remote-span , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
FDDI	name <i>vlan-name</i> , media fddi , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
FDDI-NET	name <i>vlan-name</i> , media fd-net , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type {ieee ibm auto}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i> If VTP v2 mode is disabled, do not set the stp type to auto .
Token Ring	VTP v1 mode is enabled. name <i>vlan-name</i> , media tokenring , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. name <i>vlan-name</i> , media tokenring , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , bridge type {srb srt}, are <i>are-number</i> , ste <i>ste-number</i> , backupcrf {enable disable}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
Token Ring-NET	VTP v1 mode is enabled. name <i>vlan-name</i> , media tr-net , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type {ieee ibm}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. name <i>vlan-name</i> , media tr-net , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type {ieee ibm auto}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>

The following table describes the rules for configuring VLANs:

Table 45: 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.
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).

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of VLAN *xxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default media is ethernet; the state is active. The default *said-value* is 100000 plus the VLAN ID; the *mtu-size* variable is 1500; the *stp-type* is ieee. When you enter the **exit** 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 VLAN configuration mode:


```
Device(config)# vlan 200  
Device(config-vlan)# exit  
Device(config)#
```

This example shows how to create a new extended-range VLAN with all the default characteristics, to enter VLAN configuration mode, and to save the new VLAN in the device startup configuration file:

```
Device(config)# vtp mode transparent  
Device(config)# vlan 2000  
Device(config-vlan)# end  
Device# copy running-config startup config
```

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

Related Topics

[show vlan](#), on page 720

vmps reconfirm (global configuration)

To change the reconfirmation interval for the VLAN Query Protocol (VQP) client, use the **vmps reconfirm** global configuration command. To return to the default setting, use the **no** form of this command.

vmps reconfirm *interval*
no vmps reconfirm

Syntax Description	<i>interval</i> Reconfirmation interval for VQP client queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments. The range is 1 to 120 minutes.
---------------------------	--

Command Default	The default reconfirmation interval is 60 minutes.
------------------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines	You can verify your setting by entering the show vmps privileged EXEC command and examining information in the Reconfirm Interval row.
-------------------------	---

Examples	This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:
-----------------	--

```
Device(config)# vmps reconfirm 20
```

Related Topics

[show vmps](#), on page 723

[vmps reconfirm \(privileged EXEC\)](#), on page 745

vmpls reconfirm (privileged EXEC)

To immediately send VLAN Query Protocol (VQP) queries to reconfirm all dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS), use the **vmpls reconfirm** privileged EXEC command.

vmpls reconfirm

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines You can verify your setting by entering the **show vmpls** privileged EXEC command and examining the VMPS Action row of the Reconfirmation Status section. The **show vmpls** command shows the result of the last time the assignments were reconfirmed either because the reconfirmation timer expired or because the **vmpls reconfirm** command was entered.

Examples This example shows how to immediately send VQP queries to the VMPS:

```
Device# vmpls reconfirm
```

Related Topics

[show vmpls](#), on page 723

[vmpls reconfirm \(global configuration\)](#), on page 744

vmps retry

To configure the per-server retry count for the VLAN Query Protocol (VQP) client, use the **vmps retry** command in global configuration mode. Use the **no** form of this command to return to the default setting.

vmps retry *count*

no vmps retry

Syntax Description	<i>count</i> Number of attempts to contact the VLAN Membership Policy Server (VMPS) by the client before querying the next server in the list. The range is 1 to 10.				
Command Default	The default retry count is 3.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.0(2)EX</td> <td>Cisco IOS Release 15.2(5)E This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.
Release	Modification				
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.				

This example shows how to set the retry count to 7:

```
Device(config)# vmps retry 7
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the Server Retry Count row.

Related Topics

[show vmps](#), on page 723

vmpls server

To configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers, use the **vmpls server** command in global configuration mode. Use the **no** form of this command to remove a VMPS server.

```
vmpls server {hostnameip address} [primary]
no vmpls server {hostnameip address} [primary]
```

Syntax Description	<i>hostname</i>	Hostname of the primary or secondary VMPS servers. If you specify a hostname, the Domain Name System (DNS) server must be configured.
	<i>ip address</i>	IP address of the primary or secondary VMPS servers.
	primary	(Optional) Decides whether primary or secondary VMPS servers are being configured.
Command Default	No primary or secondary VMPS servers are defined.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E This command was introduced.	

Usage Guidelines The first server entered is automatically selected as the primary server whether or not primary is entered. The first server address can be overridden by using primary in a subsequent command.

If a member device in a cluster configuration does not have an IP address, the cluster does not use the VMPS server configured for that member device. Instead, the cluster uses the VMPS server on the command device, and the command device proxies the VMPS requests. The VMPS server treats the cluster as a single device and uses the IP address of the command device to respond to requests.

When using the **no** form without specifying the IP address, all configured servers are deleted. If you delete all servers when dynamic access ports are present, the device cannot forward packets from new sources on these ports because it cannot query the VMPS.

This example shows how to configure the server with IP address 191.10.49.20 as the primary VMPS server. The servers with IP addresses 191.10.49.21 and 191.10.49.22 are configured as secondary servers:

```
Device(config)# vmpls server 191.10.49.20 primary
Device(config)# vmpls server 191.10.49.21
Device(config)# vmpls server 191.10.49.22
```

This example shows how to delete the server with IP address 191.10.49.21:

```
Device(config)# no vmpls server 191.10.49.21
```

You can verify your setting by entering the **show vmpls** privileged EXEC command and examining information in the VMPS Domain Server row.

Related Topics

[show vmps](#), on page 723

vtp (global configuration)

To set or modify the VLAN Trunking Protocol (VTP) configuration characteristics, use the **vtp** command in global configuration mode. To remove the settings or to return to the default settings, use the **no** form of this command.

vtp {**domain** *domain-name* | **file** *filename* | **interface** *interface-name* [**only**] | **mode** {**client** | **off** | **server** | **transparent**} [{**mst** | **unknown** | **vlan**}] | **password** *password* [{**hidden** | **secret**}] | **pruning** | **version** *number*}

no vtp {**file** | **interface** | **mode** [{**client** | **off** | **server** | **transparent**}] [{**mst** | **unknown** | **vlan**}] | **password** | **pruning** | **version**}

Syntax Description	
domain <i>domain-name</i>	Specifies the VTP domain name, an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the device. The domain name is case sensitive.
file <i>filename</i>	Specifies the Cisco IOS file system file where the VTP VLAN configuration is stored.
interface <i>interface-name</i>	Specifies the name of the interface providing the VTP ID updated for this device.
only	(Optional) Uses only the IP address of this interface as the VTP IP updater.
mode	Specifies the VTP device mode as client, server, or transparent.
client	Places the device in VTP client mode. A device 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 a VTP client. VLANs are configured on another device in the domain that is in server mode. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
off	Places the device in VTP off mode. A device in VTP off mode functions the same as a VTP transparent device except that it does not forward VTP advertisements on trunk ports.
server	Places the device in VTP server mode. A device in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the device. The device can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	Places the device in VTP transparent mode. A device 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 device 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 device running configuration file, and you can save them in the device startup configuration file by entering the copy running-config startup config privileged EXEC command.
mst	(Optional) Sets the mode for the multiple spanning tree (MST) VTP database (only VTP Version 3).

unknown	(Optional) Sets the mode for unknown VTP databases (only VTP Version 3).
vlan	(Optional) Sets the mode for VLAN VTP databases. This is the default (only VTP Version 3).
password <i>password</i>	Sets 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.
hidden	(Optional) Specifies that the key generated from the password string is saved in the VLAN database file. When the hidden keyword is not specified, the password string is saved in clear text. When the hidden password is entered, you need to reenter the password to issue a command in the domain. This keyword is supported only in VTP Version 3.
secret	(Optional) Allows the user to directly configure the password secret key (only VTP Version 3).
pruning	Enables VTP pruning on the device.
version <i>number</i>	Sets the VTP Version to Version 1, Version 2, or Version 3.

Command Default

The default filename is *flash:vlan.dat*.

The default mode is server mode and the default database is VLAN.

In VTP Version 3, for the MST database, the default mode is transparent.

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
Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines

VTP Version 3 is supported only when the switch is running the LAN Base image.

When you save VTP mode, domain name, and VLAN configurations in the device startup configuration file and reboot the device, the VTP and VLAN configurations are selected by these conditions:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and 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 or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

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 device is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the device does not send any VTP advertisements even if changes occur to the local VLAN configuration. The device 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 device receives its domain from a summary packet, it resets its configuration revision number to 0. After the device leaves the no-management-domain state, it cannot 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 only reassign it to a different domain.

Follow these guidelines when setting VTP mode:

- The **no vtp mode** command returns the device 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 device is not in client or transparent mode.
- If the receiving device is in client mode, the client device changes its configuration to duplicate the configuration of the server. If you have devices in client mode, be sure to make all VTP or VLAN configuration changes on a device in server mode, as it has a higher VTP configuration revision number. If the receiving device is in server mode or transparent mode, the device configuration is not changed.
- A device in transparent mode does not participate in VTP. If you make VTP or VLAN configuration changes on a device in transparent mode, the changes are not propagated to other devices in the network.
- If you change the VTP or VLAN configuration on a device that is in server mode, that change is propagated to all the devices in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the device.
- In VTP Versions 1 and 2, 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. VTP supports extended-range VLANs in client and server mode and saves them in the VLAN database.
- With VTP Versions 1 and 2, if extended-range VLANs are configured on the device and you attempt to set the VTP mode to server or client, you receive an error message, and the configuration is not allowed. Changing VTP mode is allowed with extended VLANs in VTP Version 3.
- 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.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.
- The **vtp mode off** command sets the device to off. The **no vtp mode off** command resets the device to the VTP server mode.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all devices in the same domain.

- When you use the **no vtp password** form of the command, the device returns to the no-password state.
- The **hidden** and **secret** keywords are supported only in VTP Version 3. If you convert from VTP Version 2 to VTP Version 3, you must remove the hidden or secret keyword before the conversion.

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 device automatically detects the capabilities of all the other VTP devices. To use Version 2, all VTP devices in the network must support Version 2; otherwise, you must configure them to operate in VTP Version 1 mode.
- If all devices in a domain are VTP Version 2-capable, you only need to configure Version 2 on one device; the version number is then propagated to the other Version-2 capable devices 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.
- In VTP Version 3, all database VTP information is propagated across the VTP domain, not only VLAN database information.
- Two VTP Version 3 regions can only communicate over a VTP Version 1 or VTP Version 2 region in transparent mode.

You cannot save password, pruning, and version configurations in the device configuration file.

This example shows how to rename the filename for VTP configuration storage to vtpfilename:

```
Device(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Device(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:

```
Device(config)# vtp interface gigabitethernet
```

This example shows how to set the administrative domain for the device:

```
Device(config)# vtp domain OurDomainName
```

This example shows how to place the device in VTP transparent mode:

```
Device(config)# vtp mode transparent
```

This example shows how to configure the VTP domain password:

```
Device(config)# vtp password ThisIsOurDomainsPassword
```

This example shows how to enable pruning in the VLAN database:

```
Device(config)# vtp pruning  
Pruning switched ON
```

This example shows how to enable Version 2 mode in the VLAN database:

```
Device(config)# vtp version 2
```

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

Related Topics

[show vtp](#), on page 725

[vtp \(interface configuration\)](#), on page 754

vtp (interface configuration)

To enable the VLAN Trunking Protocol (VTP) on a per-port basis, use the **vtp** command in interface configuration mode. To disable VTP on the interface, use the **no** form of this command.

vtp
no vtp

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS Release 15.0(2)EX	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines Enter this command only on interfaces that are in trunking mode.
This command is supported only when the device is running the LAN Base image and VTP Version 3.

This example shows how to enable VTP on an interface:

```
Device(config-if)# vtp
```

This example shows how to disable VTP on an interface:

```
Device(config-if)# no vtp
```

Related Topics

[switchport trunk](#), on page 732

[vtp \(global configuration\)](#), on page 749

vtp primary

To configure a device as the VLAN Trunking Protocol (VTP) primary server, use the **vtp primary** command in privileged EXEC mode.

```
vtp primary [{mst | vlan}] [force]
```

Syntax Description	Parameter	Description
	mst	(Optional) Configures the device as the primary VTP server for the multiple spanning tree (MST) feature.
	vlan	(Optional) Configures the device as the primary VTP server for VLANs.
	force	(Optional) Configures the device to not check for conflicting devices when configuring the primary server.

Command Default The device is a VTP secondary server.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS Release 15.0(2)E	Cisco IOS Release 15.2(5)E This command was introduced.

Usage Guidelines A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up the updated VTP configurations received from the primary server to NVRAM.

By default, all devices come up as secondary servers. Primary server status is needed only for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers.

Primary server status is lost if the device reloads or domain parameters change.



Note This command is supported only when the device is running VTP Version 3.

This example shows how to configure the device as the primary VTP server for VLANs:

```
Device# vtp primary vlan
Setting device to VTP TRANSPARENT mode.
```

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

Related Topics

[show vtp](#), on page 725

[vtp \(global configuration\)](#), on page 749

